Washington and Lee Law Review

Volume 79
Issue 3 *Summer*

Article 10

Summer 2022

The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet

William Chaskes
Washington and Lee University School of Law, chaskes.w23@law.wlu.edu

The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet

William Chaskes*

Abstract

Criticism of the Chinese Communist Party (CCP) runs a wide gamut. Accusations of human rights abuses, intellectual property theft, authoritarian domestic policies, disrespecting sovereign borders, and propaganda campaigns all have one common factor: the CCP's desire to control information. Controlling information means controlling data. Lurking beneath the People's Republic of China's (PRC) tumultuous relationship with the rest of the world is the fight between nations to control their citizens' data while also keeping it out of the hands of adversaries. The CCP's Three Laws are its newest weapon in this data war.

One byproduct of the CCP's emphasis on controlling the narrative is that analyzing the PRC's laws and policies requires reading between the lines—in the dark, by candlelight. Even the most informed analysis requires assumptions. The Three Laws are no different. Their broad language, drastic penalties, and sweeping scope rule out the traditional tools of statutory interpretation. Ordinary meaning, canons of construction, and legislative history are useless. In the PRC, the law means what the CCP says it means. To understand the Three Laws and

* J.D. Candidate, Washington and Lee University School of Law; M.S., B.A., Florida State University. Thank you, Professor Joshua A.T. Fairfield, for serving as my Note Advisor and to the members of the *W&L Law Review*. I am grateful to my parents for their unwavering support, advice, and guidance. Special thanks to Jerry Sussman, a great business partner and mentor, who taught me about the power of data and how to break things.

predict the associated regulatory risks, lawyers, economists, and politicians alike must think and reason by analogy.

This Note offers analyses, case studies, and recommendations that provide practitioners a solid framework to assess a company's regulatory risk under the Three Laws. First, this Note outlines the guiding tenets of the CCP to understand the motivations behind the Three Laws. Next, it provides case studies of different companies' relationships with the CCP. Realizing how the CCP has dealt with some of the largest companies in the world—Ant Group, Didi Chuxing, Apple, Tesla—is crucial to understanding the threat of future capricious CCP action.

This Note then analyzes alleged CCP hacking campaigns and global influence building so the reader may better understand the types of actions that the CCP undertakes—and fears being done to it by others. Finally, this Note provides recommendations for companies with different levels of exposure to the CCP and its ability to enforce its laws. Ultimately, this Note provides the reader with a primer on an important geopolitical issue: the shadowy battle between the world's great powers to control their citizens' information, procure their adversaries' data, and the ways that the law is being used to further these goals.

Table of Contents

INTRODUCTION

The rise of Xi Jinping, the paramount leader for life of the People's Republic of China (PRC) and the Chinese Communist Party (CCP),[1] has been accompanied by the rise of "wolf warrior diplomacy."[2] This assertive attitude is named after a 2015 patriotic film and has steadily become a nigh-default tactic for PRC officials seeking to "defend China's national interests, often in confrontational ways."[3] This emboldened approach to international relations has crept into PRC domestic regulations with extraterritorial effect. The wolf warrior philosophy is central to the PRC's new privacy and cybersecurity laws.

The CCP views controlling cyberspace as a national priority.[4] In furtherance of this prerogative, the PRC has passed three laws that together comprise a framework for PRC

---

1. *See* Eleanor Albert et al., *The Chinese Communist Party*, COUNCIL ON FOREIGN RELS., https://perma.cc/5LV9-2EKH (last updated June 23, 2021, 3:00 PM) ("The Chinese Communist Party (CCP) is the founding and ruling political party of modern China, officially known as the People's Republic of China. The CCP has maintained a political monopoly since its founding a century ago . . . .").

2. *See* Joanna Nawrotkiewicz & Peter Martin, *Understanding Chinese "Wolf Warrior Diplomacy"*, NAT'L BUREAU ASIAN RSCH. (Oct. 22, 2021), https://perma.cc/3X7L-QK88

> Wolf Warrior diplomacy has become the shorthand expression for a new, assertive brand of Chinese diplomacy. In the past, Chinese diplomats tended to keep a lower profile and to be quite cautious and moderate in the way that they interacted with the outside world. Recently, however, they have become far more strident and assertive—exhibiting behavior that ranges from storming out of an international meeting to shouting at foreign counterparts and even insulting foreign leaders.

3. Zhiqun Zhu, *Interpreting China's 'Wolf-Warrior Diplomacy'*, THE DIPLOMAT (May 15, 2020), https://perma.cc/YEZ4-ABQH. *But see* Zhanna Malekos Smith, *New Tail for China's 'Wolf Warrior' Diplomats*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 13, 2021), https://perma.cc/S3VQ-GSLM (analyzing recent speeches by Xi Jinping that may signal a lessening of the "wolf warrior" phenomenon).

4. *See A Rising "Cyber China"*, TURKISH POL'Y Q. (Dec. 7, 2021), https://perma.cc/J76A-M8TN ("When Bill Clinton famously compared China's efforts to suppress free online discussion as 'trying to nail Jell-O to the wall,' he underestimated the [CCP]'s determination to adopt an internet that both facilitates China's development and preserves the Party's governing power.").

cybersecurity and privacy issues.[5] These three laws (the "Three Laws") are: (i) the Cyber Security Law (CSL);[6] (ii) the Personal Information Protection Law (PIPL);[7] and (iii) the Data Security Law (DSL).[8] The Three Laws create the bedrock legal infrastructure for achieving the PRC's cyberspace and geopolitical ambitions.[9] This legal foundation relies on categorizing data that the CCP values and, conversely, views as a threat if such data were accessible by PRC adversaries.

This Note will attempt to answer the question "what kind of data types and activities would draw the ire of PRC regulators?" Given the broad, vague language of the Three Laws, PRC authorities clearly have ample flexibility to apply any of the Three Laws to further national strategic objectives.[10] These laws are interrelated and must be read together—but even that does not provide enough clarity to assess regulatory risk. The ambiguity of how the PRC makes and enforces laws

5. *See* Clarice Yu et al., *Are You Ready? PRC Data Security Law Was Passed and Will Come into Effect on 1 September 2021!*, BIRD & BIRD (June 17, 2021), https://perma.cc/7NJM-VLV9 ("The CSL, the DSL and the PIPL will represent three pillars of the Chinese data legislation system and together form an overarching framework governing the data processing and cybersecurity issues.").

6. *See* Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, STAN. UNIV. DIGICHINA CYBER POL'Y CTR. (June 29, 2018), https://perma.cc/CMB8-ZAQ2.

7. *See* Rogier Creemers & Graham Webster, *Translation: Personal Information Protection Law of the People's Republic of China—Effective Nov. 1, 2021*, STAN. UNIV. DIGICHINA CYBER POL'Y CTR. (Aug. 20, 2021) [hereinafter *PIPL*], https://perma.cc/2NRV-7CDN (last updated Sept. 7, 2021).

8. *See Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, STAN. UNIV. DIGICHINA CYBER POL'Y CTR. (June 29, 2021) [hereinafter *DSL*], https://perma.cc/RAB4-SMC2.

9. *See* Xiang Wang et al., *China's New Data Security Law: What International Companies Need to Know*, ORRICK (Sept. 23, 2021), https://perma.cc/EQ6U-LS8G ("This triad of new data laws represents an increasingly comprehensive legal framework for privacy and data security in the [world's] second largest economy.").

10. *See* Karry Lai, *PRIMER: China's Data Security Law*, INT'L FIN. L. REV. (Nov. 11, 2021), https://perma.cc/5RZR-3KJM ("Data protection experts said that there are a number of areas that remain murky in the new [DSL] . . . .").

and regulations creates difficulties for companies trying to predict government action.[11] To prepare for the future ramifications of the Three Laws, companies and governments must understand the CCP's guiding philosophies, how the PRC has dealt with data collection and use up to this point, and how the Three Laws thrust data regulation headlong into the realms of politics, diplomacy, and power.

This Note will first discuss and analyze the pertinent language of the Three Laws.[12] Next, it will orient the reader to the guiding principles and philosophies that motivate the CCP to impose such wide-reaching legislation.[13] This Note then provides case studies of CCP actions through a data-focused lens.[14] Finally, this Note analyzes the potential enforceability and therefore overall regulatory risk of the Three Laws to companies across the globe.[15]

I. THE THREE LAWS

A. The Cyber Security Law

The CSL came into force on June 1, 2017.[16] This expansive law prescribes a sweeping list of requirements with particular focus on controlling whether data is stored in the PRC (data localization) and what data is allowed to leave the PRC's borders (cross-border transactions).[17] As the first of the Three Laws to

11. *See* REEDSMITH LLP, CHINA'S CYBERSECURITY LAW 1 [hereinafter CHINA'S CYBERSECURITY LAW], https://perma.cc/4RVN-6HXS (PDF) ("The Chinese legislative and enforcement style creates confusion and misunderstandings, and sometimes false hopes, for Western companies.").

12. *See infra* Part I.

13. *See infra* Part II.

14. *See infra* Part III–VI.

15. *See infra* Parts VII–VIII.

16. CHINA'S CYBERSECURITY LAW, *supra* note 11, at 1.

17. *See* Samuel Yang, *The Privacy, Data Protection and Cybersecurity Law Review: China*, THE L. REVS. (Nov. 5, 2021), https://perma.cc/84DG-27VW (PDF)

> Among other things, the CSL covers the following aspects: personal information protection; general network protection obligations of the network operators and the multi-level protection scheme (MLPS); enhanced

be enacted, the CSL's language is vague and broad, giving the CSL an "over-reaching scope."[18] As a result, the CSL cannot be understood in a vacuum. Achieving any clarity as to how companies might rankle the CCP requires an examination of the rest of the Three Laws as well as how the CSL is enforced.

B. The Personal Information Protection Law

The PIPL came into force on November 1, 2021.[19] The law states its rationale as "protect[ing] personal information rights and interests, standardiz[ing] personal information handling activities, and promot[ing] the rational use of personal information."[20] Analogous to the European Union's (EU) Global Data Protection Regulation (GDPR),[21] the PIPL increases compliance costs, restricts what data can be stored, where data can be stored, and how data is authorized to leave the PRC's borders.[22] Enforced by the newly-created Cyberspace Administration of China (CAC), the PIPL imposes harsh financial penalties of up to fifty million CNY (approximately $7.8 million USD) or five percent of the offending company's revenue from the previous year.[23] The PIPL's extraterritorial reach is triggered "(1) [w]here the purpose is to provide products

---

protection for the critical information infrastructure (CII); data localization and security assessment for the cross-border transfer of personal information and important data; and security review of the network products and services.

18. *See* CHINA'S CYBERSECURITY LAW, *supra* note 11, at 1 ("The path to CSL compliance is not straightforward . . . . Despite this environment of uncertainty and change, the Chinese authority has already begun initiating enforcement actions for CSL violations.").

19. *See PIPL*, *supra* note 7.

20. *Id.* art. 1.

21. Regulation 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, and Repealing Directive 95/46/EC, art. 9, 2016 O.J. (L 119) 1 (EU).

22. *See* Paul McKenzie, *Top-5 Operational Impacts of China's PIPL: Part 1—Scope, Key Definitions and Lawful Handling of Personal Information*, INT'L. ASS'N PRIV. PROS. (Feb. 10, 2022), https://perma.cc/7UBS-NM7B.

23. *See PIPL*, *supra* note 7, art. 66.

or services to natural persons inside the [PRC]; (2) [w]here analyzing or assessing activities of natural persons inside the borders; [or] (3) [o]ther circumstances provided in laws or administrative regulations."[24] This extraterritoriality provision is broadly worded but centers around the concept of "sensitive personal information"[25] and, therefore, understanding what the PRC considers "sensitive personal information" is key to assessing a company's regulatory risk under the PIPL.

Article 28 of the PIPL explicitly defines "sensitive personal information" as "personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security [sic]."[26] The PIPL provides a non-exclusive list of "sensitive personal information," including "information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14."[27] While the PIPL adds additional clarity, the language is still so broad that the law could be selectively enforced.[28] Like the rest of the Three Laws, the PIPL provides the CCP wide latitude to enforce the Three Laws arbitrarily to further CCP objectives.

C. The Data Security Law

On September 1, 2021, the PRC enacted the DSL.[29] In pertinent part, the DSL prescribes monetary sanctions for expansive situations including "[w]hen data handling activities outside the mainland territory of the PRC harm the national

---

24. *See id.* art. 3.

25. *See id.* art. 28 (explaining the PIPL's focus on sensitive personal information and providing a non-exhaustive list of examples).

26. *Id.*

27. *Id.*

28. *See id.* (prescribing that "only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures, may personal information handlers handle sensitive personal information," without defining any of the key terms further).

29. *DSL*, *supra* note 8.

security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC."[30] Keeping to the general tenor of broad and expansive regulations, none of these three categories are defined further in the text of the law.[31] Absent statutory definitions, CCP philosophies and past regulatory actions provide the only indication as to what data the PRC views as potentially harming these nebulous categories of "the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC."[32] Optimism that future regulations would provide definitive guidance was misplaced, as subsequent regulations later expanded the scope of the Three Laws.

D. Draft Regulations

On November 14, 2021, the CAC published draft regulations for public comment designed to implement portions of the Three Laws.[33] These draft regulations drastically expand the scope of the Three Laws.[34] It was expected that the Three Laws would apply to data activities within the PRC, but these regulations would alarmingly apply to any data processing whose purpose is to "monitor and evaluate the activities of individuals and organizations in China; process 'important data' located in China; or comply with any conditions under other Chinese law and regulation."[35] The Three Laws have already

30. *Id.*

31. *Id.*

32. *Id.*

33. *See Regulations on the Management of Online Data Security (Draft for Solicitation of Comments)*, CHINA L. TRANSLATE (Nov. 14, 2021), https://perma.cc/WD9J-XC7U (providing a crowdsourced translation of the draft regulations); *see also China Releases Draft Regulations on Network Data Security Management*, HUNTON ANDREWS KURTH LLP (Jan. 26, 2022) [hereinafter *China Releases Draft Regulations*], https://perma.cc/MU5K-E8GA (analyzing the draft regulations).

34. *See China Releases Draft Regulations*, *supra* note 33 ("The exterritorial scope under the Draft Regulations is much broader than that under the Three Laws.").

35. *Id.*

been used to order the removal of hundreds of Chinese apps from PRC app stores for violations of any or all of the laws.[36] The broad language of the Three Laws and their attendant regulations requires practitioners to holistically consider the PRC's cyberspace and geopolitical ambitions when interpreting these statutes and regulations.[37]

II. BACKGROUND

Analyzing anything CCP-related involves dealing with ambiguity and unfamiliarity—even for those well-versed on the PRC and its affairs. To best comprehend the motivations behind the Three Laws, it is necessary to understand how the CCP regulates, what its motivations and guiding principles are, and how the value of data affects governmental and business objectives.

A. Arbitrary CCP Action at Home and Abroad

CCP action can impact foreign companies either through outright regulation or less obvious gamesmanship favoring PRC actors. Foreign companies have long been concerned about arbitrary CCP action that would entrench or bolster PRC economic competitors.[38] YUM! Brands and Uber divested themselves of their PRC operations in the face of greater market competition, management difficulties, and increased CCP

36. *See* Josh Ye & Coco Feng, *China Internet Crackdown: Beijing Orders App Stores to Remove Douban and 105 Other Apps*, S. CHINA MORNING POST (Dec. 9, 2021, 7:59 PM), https://perma.cc/6HCJ-GB29.

37. *See* Lai, *supra* note 10 ("[D]ata classification is a key challenge. For instance, Article 21 of the [DSL] stipulates that important data and national core data require significantly higher protection; however, as of now, the authorities have not provided guidelines on how to define and identify important data and national core data." (internal quotation omitted)).

38. *See China Travel Advisory*, U.S. DEP'T STATE, (July 5, 2022), https://perma.cc/Q6M7-PPLK (warning of the arbitrary experiences of businesspersons, journalists, and others "subjected to prolonged interrogations and extended detention without due process of law" in the PRC); *see also* Eric Li, *China and the Rule of Law*, J. AM. AFFS. (2019), https://perma.cc/HP2K-CHLB ("Businesses and individuals cannot operate with predictability, nor even basic security of property and liberty.").

regulatory oversight.[39] These divestitures by American companies are a purposeful absence in one of the world's largest markets.[40] Whether these companies were concerned about competing with PRC companies in the face of potential PRC regulation, supply problems, or difficulties managing PRC operations from afar, they reached the decision that divesting their PRC operations made better business sense than remaining exposed to the whims of the CCP and other threats endemic to doing business in the PRC.[41] At a certain point the risks of operating in the PRC were not worth the reward.

In evaluating such risks, companies must understand the doctrines that undergird CCP actions. Most importantly, the CCP's cyber sovereignty and information domination philosophies mandate a new datafocused analytical framework for evaluating the risks of doing business with the PRC—especially for companies that heavily rely on data. If data control is the PRC's goal, then foreign firms and governments risk being caught flatfooted if they do not meticulously analyze the informational advantage that private sector data control provides governments—particularly the PRC.

---

39. *See* Stephanie Strom et al., *Yum Brands to Split China Business into Separate Company*, N.Y. TIMES (Oct. 20, 2015), https://perma.cc/KD2L-HXR4 (reporting on the YUM! divestiture and its potential motivations being food safety issues, changing customer tastes, and local and international competition); Alyssa Abkowitz & Rick Carew, *Uber Sells China Operations to Didi Chuxing*, WALL ST. J. (Aug. 1, 2016, 1:06 PM), https://perma.cc/N2ZG-JQQ9 (reporting on the Uber divestiture and remarking on the long history of competition between Uber and the PRC company, Didi Chuxing).

40. *See One Year Later, Yum China Thrives After Its Spin-off*, THE MOTLEY FOOL (Oct. 18, 2017, 4:42 PM), https://perma.cc/4H7S-3SBC (analyzing the YUM! divestiture a year later and evaluating the supply chain, competition, and regulatory motivations for the deal).

41. *See* William C. Kirby, *The Real Reason Uber is Giving Up in China*, HARV. BUS. REV. (Aug. 2, 2016), https://perma.cc/PS57-AE2L ("Uber is leaving China not because of interference from its rivals but because of interference from the state.").

B. Cyber Sovereignty and Information Domination

Internet security and control is a PRC national priority cloaked under the mantra of cyber sovereignty.[42] This concept of "cyber sovereignty" is nebulously defined but presents itself most acutely in censorship and strict controls on not allowing access to PRC data to any but the CCP.[43] To fully grasp this concept and its ramifications, a key consideration is the PRC model of central control and the lack of any theoretical barriers between the public and private sectors.[44] As the head of the United Kingdom's MI5 remarked in a joint press conference with the head of the FBI, "The CCP adopts a whole-of-state approach in which businesses and individuals are forced by law to co-operate with the Party."[45] With no lines between the public and private sectors, this cyber sovereignty approach has ramifications on censorship and regulation of PRC and foreign citizens and companies behind the Golden Shield Project, colloquially known as the Great Firewall, which isolates the PRC from the rest of the global internet.[46] Additionally, the

42. *See China Internet: Xi Jinping Calls for 'Cyber Sovereignty'*, BBC (Dec. 16, 2015), https://perma.cc/CKC8-JPLY (reporting Xi's comments emphasizing "cyber sovereignty" as a "clear sign" of PRC national priorities).

43. *See* Elliot Zaagman, *Cyber Sovereignty and the PRC's Vision for Global Internet Governance*, THE JAMESTOWN FOUND. (June 5, 2018, 7:00 PM), https://perma.cc/2YFL-BAME (remarking that PRC cyber sovereignty, at its core, concerns "sophisticated, systematic censorship through a well-developed 'Great Firewall,' and strict requirements for local data storage imposed upon all firms operating within its borders").

44. *See* Stephen Olson, *Are Private Chinese Companies Really Private?*, THE DIPLOMAT (Sept. 30, 2020), https://perma.cc/8KNZ-UPFC (analyzing the PRC Central Committee "Opinion on Strengthening the United Front Work of the Private Economy in the New Era," which "tells us in no uncertain terms that Chinese private companies will be increasingly called upon to conduct their operations in tight coordination with governmental policy objectives and ideologies"); SCOTT LIVINGSTON, THE CHINESE COMMUNIST PARTY TARGETS THE PRIVATE SECTOR (Oct. 2020), https://perma.cc/Q36Z-MWQH (PDF).

45. Ken McCallum, Dir. Gen., MI5 & Chris Wray, Dir., FBI, Joint Address by MI5 and FBI Heads (July 6, 2022), https://perma.cc/A5YM-7BMZ.

46. *See* Marty Hu, *The Great Firewall: A Technical Perspective*, TORFOX: A STAN. PROJECT (May 30, 2011), https://perma.cc/M6PB-S9Z2 (explaining the basic technical features of the Great Firewall including internet protocol blocking, address misdirection, and—most pertinent to our analysis—data

cyber sovereignty philosophy has veiled effects on companies whose operations involve PRC-controlled infrastructure or markets.[47] Subsumed within the cyber sovereignty philosophy is another dictum that guides PRC regulatory decision-making—the quest for information domination.

The CCP values informational superiority as a prerogative for maintaining domestic control and achieving its international ambitions. In 2003, the PRC promulgated the "Three Warfares" strategic concept.[48] This stratagem, in all its facets, requires informational superiority.[49] Colloquially, information domination involves leveraging technology to disrupt or direct the narrative surrounding the PRC's security interests.[50] As a former FBI director testified to Congress, "Ultimately, China doesn't hesitate to use smoke, mirrors, and misdirection to influence Americans."[51] CCP strategy for maintaining control of the PRC revolves around "creat[ing] an environment of anonymity, ambiguity, and the confusion and dilemma of ethical retaliation that Chinese have traditionally dominated."[52] The

---

filtering); *see also* Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED (June 1, 1997, 12:00 PM), https://perma.cc/3N92-LLRT; *see generally* JAMES GRIFFITHS, THE GREAT FIREWALL OF CHINA: HOW TO BUILD AND CONTROL AN ALTERNATIVE VERSION OF THE INTERNET (2021).

47. *See* Justin Sherman, *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?*, COUNCIL ON FOREIGN RELS. (Oct. 30, 2019, 4:00 PM), https://perma.cc/4SBX-ZHJM.

48. *See* STEFAN HALPER, CHINA: THE THREE WARFARES 28 (2013), https://perma.cc/AVC5-G2RG (PDF) (describing the "Three Warfares" as comprising psychological, media, and legal warfare).

49. *See id.* (outlining the myriad ways China uses information and misinformation to achieve its political objectives).

50. *See generally* CHRISTOPHER WHYTE & BRIAN MAZANEC, UNDERSTANDING CYBER WARFARE: POLITICS, POLICY AND STRATEGY (2018).

51. Olivia Solon & Ken Dilanian, *China's Influence Operations Offer a Glimpse into the Future of Information Warfare*, NBC NEWS (Oct. 21, 2020, 5:00 AM), https://perma.cc/M65M-8N7Z.

52. Vincent Wei-Cheng Wang, *Asymmetric War? Implications for China's Information Warfare Strategies*, 20 AM. ASIAN REV. 167, 197 (2002), https://perma.cc/MW97-RQBS (PDF) (commenting on the traditional Thirty-Six Strategies: The Secret Art of War and its influence on modern PRC strategic thinking).

PRC has expansive regulatory ambitions and these legal upheavals resist easy classification into public and private sector efforts. However, information is data aggregated. So, if information is the objective, data are bricks in the artifice.

C. The PRC's Rapacious Thirst for Data

The CCP has fenced off the PRC from the rest of the global internet and fanatically protects access to its markets, networks, and data. Essentially, the PRC population is an intentionally designed black box for anyone other than the CCP. The CCP has greater insight into the PRC population than other nations can achieve—due in large part to purposeful PRC infrastructure and network priorities.[53] One of the largest differences inherent to the PRC approach is the blurring of lines between data available to private-sector companies and data available to government actors.[54] In the post-Snowden age, all must assume that governments have access to their respective nation's private-sector data, especially in the PRC.[55] In evaluating technology both inside and outside the PRC, nations should not lose sight of the PRC's focus on what data these technologies and companies collect, maintain, and store.[56] The tension between the PRC approach to control and western traditions of openness is paramount to understanding the greater context of any transaction dealing with citizen data and PRC access to such data.[57]

---

53. *See* Matt Sheehan, *Much Ado About Data: How America and China Stack Up*, MACRO POLO (July 16, 2019), https://perma.cc/2X8Y-L3JM.

54. *See* Lindsay Gorman, *China's Data Ambitions: Strategy, Emerging Technologies, and Implications for Democracies*, NAT'L BUREAU ASIAN OF RSCH. (Aug. 14, 2021), https://perma.cc/HE2V-GSKL ("To achieve these goals, the [PRC] has combined national policy planning and aggressive data-retention policies with an outgoing effort to export data-based technologies.").

55. *See generally* FRED H. CATE & JAMES X. DEMPSEY, BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (2017).

56. *See* Gorman, *supra* note 54 ("China's data ambitions risk normalizing concepts of state access to citizen data absent independent legal due process.").

57. *See* Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUD. COMPAR. INT'L DEV. 45, 45 (2021) ("Chinese tech companies, therefore, confront a 'deep versus broad' dilemma: deep ties with the Chinese

The PRC wants to collect all possible data from its adversaries while denying anyone but the CCP access to data behind the Great Firewall.[58] The PRC is collecting rivals' data at an increasing—almost exponential—rate.[59] Some PRC-influenced news publications try to differentiate the PRC approach as defensive in contrast to other countries that also collect troves of data as part of their information warfare strategy.[60] Propagandic characterizations aside, the data is still collected, stored, and capable of being used in any possible fashion.[61] If you have the bricks, you can make whatever kind of house you desire. The overarching philosophy behind PRC data collection is to further its goal of becoming the supreme world power.[62] Warehousing data allows flexibility to adapt strategy to new circumstances, so the PRC's collection of data must be a

government help promote their domestic business but jeopardize their international expansion.").

58. *See* Samantha Hoffman, *The U.S.-China Data Fight Is Only Getting Started*, FOREIGN POL'Y (July 22, 2021, 12:40 PM), https://perma.cc/D4AG-NAPX ("[W]hat is exceptional is the way the Chinese Communist Party-state has used such laws—and other tools—to give it ultimate influence over digital technologies and the flow of data.").

59. *See* Cate Cadell, *China Harvests Masses of Data on Western Targets, Documents Show*, WASH. POST (Dec. 31, 2021, 5:13 PM), https://perma.cc/J5JB-WYUW ("China is turning a major part of its internal Internet-data surveillance network outward, mining Western social media, including Facebook and Twitter, to equip its government agencies, military and police with information on foreign targets.").

60. *See* Alex Lo, *Why Chinese Information Warfare Is Different from Those of the US and Russia*, S. CHINA MORNING POST (Feb. 7, 2022, 9:00 PM), https://perma.cc/ZCF6-RJ4K ("Chinese state propaganda is primarily defensive in nature and aims at pushing the country's preferred viewpoints and narratives about itself. Comparable operations by Russia and the United States are generally offensive as they aim at regime change, political delegitimisation, and societal and economic destabilisation in the targeted country.").

61. *See* Solon & Dilanian, *supra* note 51 (quoting the Director General of MI5 as saying "Russia [is] like bad weather but China [is] a far greater challenge in the long-term and more like climate change").

62. *See id.* ("The goal, experts said, is to develop more influence overseas, particularly among America's political and military allies in Southeast Asia, who have been alienated by President Donald Trump, and to ultimately replace the U.S. as the dominant world power.").

primary concern.[63] However, not all data is created equal and comprehending the values of different datatypes is pivotal to understanding the PRC's data obsession.

D. Differing Values of Data

Some data is more valuable than others.[64] Certain datatypes are worth more because they are more easily monetized.[65] Other datatypes provide valuable metrics that allow advertisers, businesses, and intelligence organizations to glean insights into individuals or groups.[66] While these two broad categories overlap, there is dissonance between the datatypes most valuable to cybercriminals and the datatypes most useful to governments and businesses. Credit card numbers, bank account information, and other traditional identity theft data are decidedly in the first category.[67] This information is taken without consent and its primary uses sound in fraud and theft. On the other hand, the datatypes most valuable to companies and governments are those that are used to build analytical, predictive models of individuals and groups.[68] Insight into their customers' or citizens' behavior promotes greater control.[69] This control is useful to a company wishing to grow its revenue as well as a government seeking to

63. *See* Anthony J. Eastin & Patrick G. Franck, *Information Warfare on United States' Citizens: How China Weaponized COVID-19*, OVER THE HORIZON (Aug. 28, 2020), https://perma.cc/PCD9-WZVE (explaining that the COVID-19 pandemic caused a shift in PRC information warfare operations).

64. *See* Ravi Sen, *Here's How Much Your Personal Information Is Worth to Cybercriminals—and What They Do with It*, PBS (May 14, 2021, 12:04 PM), https://perma.cc/9LHP-NFAE.

65. *See Valuing Data Is Hard*, SILICON VALLEY DATA SCI. (Nov. 10, 2015), https://perma.cc/DM7N-BEWF.

66. *See generally* DELOITTE, DATA VALUATION: UNDERSTANDING THE VALUE OF YOUR DATA ASSETS (2020), https://perma.cc/H63C-Y35U (PDF).

67. *See Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST. (2021), https://perma.cc/P8JZ-FKBA.

68. *See* Elaine Bennett, *Types of Data Every Business Should Collect*, DISRUPT MAG. (2020), https://perma.cc/82LS-YYK4.

69. *See* Steven Feldstein, *We Need to Get Smart About How Governments Use AI*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Jan. 22, 2019), https://perma.cc/59Y8-QEH8.

control either its citizens or the citizens of another country.[70] Cost of collection and the quality of analysis that a given datatype yields are two of the biggest determinants for why one datatype is more valuable than another.[71] Viewing past PRC actions from a data perspective allows better understanding of what priorities the CCP views as critical to its national security and policy objectives. Because companies and governments both covet these types of data, the Three Laws should be of paramount concern for international, private-sector companies that collect, manage, or store data valuable to their business purposes that is also strategically important to the PRC.

III. FINANCIAL DATA CASE STUDY: ANT GROUP'S IPO

On November 3, 2020, the CCP halted the initial public offering (IPO) of Jack Ma's Ant Group days before the financial technology behemoth was scheduled to list on the Shanghai and Hong Kong stock exchanges.[72] Regulators were not forthcoming about the specific rationale for halting an IPO of one of the PRC's largest companies.[73] Rumors abounded that Jack Ma, Ant Group's billionaire founder, had rankled the CCP with a speech criticizing the PRC's financial system and regulations.[74] While the speech might have been the straw that broke the camel's back, the true crux of this cataclysmic regulatory action is the

70. *See* Amanda Evans et al., *Four Ways Governments Can Use Data to Transform Outcomes*, EY (Mar. 25, 2021), https://perma.cc/3J4D-C6WC ("Unlike the private sector, though, governments have no similarly disruptive 'competitors' [data-centric service providers such as Netflix and Alibaba] to provide the spur for change.").

71. *See* Gillian MacPherson, *Location vs. Transactional Data: Is One Better?*, EPSILON (Apr. 30, 2019), https://perma.cc/B658-NMXH.

72. *See* Jing Yang & Serena Ng, *Ant's Record IPO Suspended in Shanghai and Hong Kong Stock Exchanges*, WALL ST. J., https://perma.cc/JB83-PLEJ (last updated Nov. 3, 2020).

73. *See id.* ("Regulators didn't go into detail about what led them to pull the plug on Ant's IPO.").

74. *See id.* ("We cannot regulate the future with yesterday's means. . . . There[] [are] no systemic financial risks in China because there's no financial system in China. The risks are a lack of systems.").

detailed data accumulated as a result of Ant Group's business model.

In April 2021, after months of financial technology companies encountering significant obstacles to listing publicly, China's Securities Regulatory Commission issued new guidelines for companies that wanted to list on PRC exchanges.[75] Rumors and guesses circulated as experts struggled to understand the PRC regulatory policy.[76] These theories ranged from assuming that the PRC was protecting its state-owned banks—giving the banks time to create their own competitive financial technology operations—to CCP paranoia about losing control to a bevy of billionaire technology entrepreneurs.[77] This abrupt intervention in a prestigious PRC private-sector economic achievement is perhaps best explained by future developments that might elucidate PRC fears of technology companies and the data these companies collect, analyze, and use. One of the plausible explanations for this regulatory shift is a PRC focus on protecting Chinese citizens' financial data.[78] Indeed, the overarching question becomes: "What made the PRC willing to cut one of its crown jewel private sector companies down at the knees?"

Article 28 of the PIPL provides examples of various types of information that fall within its ambit.[79] Financial account information is explicitly listed therein.[80] Even assuming the entire Ant Group crackdown was solely an attempt to weaken billionaire Jack Ma, the PRC has 625 other publicly-known

75. *See* Eustance Huang, *China's Fintech Giants Are Hitting Roadblocks in Planned Listings at Home*, CNBC (Apr. 23, 2021, 12:49 AM), https://perma.cc/Y5KL-NT6F.

76. *See* VIVIANA ZHU, INSTITUT MONTAIGNE, CHINA'S FINTECH: THE END OF THE WILD WEST 25–28 (Apr. 2021), https://perma.cc/A3Z7-G7GJ (PDF).

77. *See supra* notes 72–76 and accompanying text; *see also China's Regulators Vow 'Special' Oversight of Fintech Giants*, BLOOMBERG (Nov. 30, 2020, 8:37 AM), https://perma.cc/GW3C-QX5P (last updated Nov. 30, 2020 11:05 PM).

78. *See* Lingling Wei, *Chinese Regulators Try to Get Jack Ma's Ant Group to Share Customer Data*, WALL ST. J. (Jan. 5, 2021, 3:33 PM), https://perma.cc/8ECX-3HNN.

79. *See supra* Part I.B.

80. *See supra* Part I.B.

billionaires.[81] The context of the crackdown on Jack Ma and Ant Group sheds light on the PRC's desire to control the financial information of its citizens.[82] If Jack Ma's speech was in response to regulators wanting more control over the financial data inherent to Ant Group's business model, then the motivation for quashing the Ant Group IPO is truly a CCP desire for financial control. If so, then how is BlackRock, the first foreign firm to be allowed to offer mutual fund products to PRC citizens,[83] going to navigate the PRC's protectionism regarding its citizens' financial information?[84] Further, there are many companies that sell transaction data, cultivated either from their proprietary applications or as the terms for providing back-end software to financial institutions.[85] Will these companies be

81. *See* Giacomo Tognini, *The Countries with the Most Billionaires 2021*, FORBES (Apr. 6, 2021, 6:00 AM), https://perma.cc/8X9V-DHFE ("[N]early half of the individuals on *Forbes'* World's Billionaires list hail from the U.S. and China.").

82. *See* Eswar Prasad, *Jack Ma Taunted China. Then Came His Fall*, N.Y. TIMES (Apr. 28, 2021), https://perma.cc/8YPY-LAB8 ("Chinese regulators trying to assess financial risks on Ant's books had been brushed off by Mr. Ma. In an audacious speech, he criticized regulators as too cautious and pilloried state-owned banks for their 'pawnshop' mentality of providing loans only to borrowers who could post collateral.").

83. *See* Jing Yang & Dawn Lim, *BlackRock Raises $1 Billion for First Chinese Mutual Fund Run by Foreign Firm*, WALL ST. J. (Sept. 7, 2021), https://perma.cc/R9XB-VE8M ("BlackRock was the first firm given full approval to sell mutual funds of its own to Chinese individuals. It is so far the only foreign firm with that distinction."). *But see* George Soros, *BlackRock's China Blunder*, WALL ST. J. (Sept. 6, 2021, 11:42 AM), https://perma.cc/YVT4-Q6BP ("[BlackRock] appears to misunderstand President Xi Jinping's China.").

84. BlackRock's foray into the PRC market is a developing issue and would provide an excellent case study for further research and analysis, but is unfortunately out of scope for this Note due to the recency of their market entry.

85. *See, e.g.*, *Access Detailed Transaction History*, PLAID, https://perma.cc/P8RY-FYHG (advertising Plaid's transaction data services); *Transaction Data Enrichment, an Opportunity for Financial Wellness*, ENVESTNET YODLEE, https://perma.cc/J63U-3WTC (advertising transaction data access and data enrichment services, which would add datapoints to financial institutions' own customer databases, providing greater fidelity and insight).

subject to the broad and extraterritorial restrictions of the Three Laws even if they do not operate in the PRC?[86]

IV. LOCATION DATA

A. Didi Cybersecurity Review

On June 30, 2021, Didi-Chuxing ("Didi"), a PRC version of Uber, debuted on the New York Stock Exchange.[87] Days later, the CAC suspended new users from registering for the PRC's largest ride-sharing company.[88] Eventually, Didi's apps were removed from PRC app stores and the company was ordered to comply with a full cybersecurity review.[89] In response to this multi-billion-dollar tumult, the United States Securities and Exchange Commission temporarily halted approval of any future listings of PRC companies on United States exchanges.[90] Undoubtedly, the widespread investor frustration over CCP interference imploding the Didi IPO motivated this pause.[91] In the weeks after the Didi IPO, the CAC proposed new regulations requiring companies wanting to list overseas to pass a national security review regarding how user data is handled in advance.[92] Didi shares then further plummeted after rumors spread that PRC regulators were asking the firm to delist from the U.S. exchange.[93]

---

86. *See infra* Part VIII.

87. *See* Paul R. La Monica, *SEC Temporarily Halts Approvals of New Chinese IPOs After Didi Debacle*, CNN, https://perma.cc/8RUE-9EBU (last updated Aug. 2, 2021, 12:37 AM).

88. *See* Moira Ritter, *Didi Stock Tumbles After China Suspends Registration of New Users*, CNN, https://perma.cc/77C5-X9LD (last updated July 2, 2021, 10:58 AM).

89. *See* John Ruwitch, *China Removed Didi from App Stores, Accused the Company of Violating Security Rules*, NPR: ALL THINGS CONSIDERED (July 12, 2021, 4:20 PM), https://perma.cc/VB54-WSGW.

90. *See supra* notes 87–89 and accompanying text.

91. *See supra* notes 87–89 and accompanying text.

92. *See* Jane Li, *Meet the New Gatekeeper for Chinese Tech Firms Seeking to IPO in the US*, QUARTZ (July 15, 2021), https://perma.cc/JN3L-PFJL.

93. *See* Arjun Kharpal, *Didi Shares Sink on a Report that Chinese Regulators Have Asked It to Delist from U.S.*, CNBC, https://perma.cc/Z4BK-JK5D (last updated Nov. 26, 2021, 1:01 PM) ("The Cyberspace Administration

The Didi cybersecurity review and New York Stock Exchange delisting had deleterious effects on the company's business, including twenty percent of its employees being laid off, plummeting daily active users, and a two-thirds drop from its debut IPO share price.[94] In June of 2022, in what some commentators ascribed to a desire to spur economic activity in tough times, the CCP concluded the security audit and allowed Didi back onto app stores and new users to enroll.[95] Days later, Didi's delisting from the New York Stock Exchange was completed.[96] Subsequently, the CCP announced that the cybersecurity review was concluding, a $1 billion fine would be assessed, and Didi's apps would be allowed to continue to enroll new users.[97] In total, billions of dollars and thousands of jobs had evaporated, and yet it was still not completely clear what had rankled the CCP enough to kneecap one of its most valuable companies.[98] While the Ant Group brouhaha appeared to revolve around financial data, this calamitous CCP regulatory action centered on a company with some of the best possible location data on PRC citizens.[99] As manufacturers add technology to their vehicles every year, location data is not just limited to ride-sharing companies but all vehicles that rely on

---

of China has asked Didi to work out the details for a delisting which will be subject to government approval.").

94. *See* Coco Feng, *Didi Chuxing Starts Companywide Layoffs Amid Unresolved Cybersecurity Probe, Ongoing Delisting in New York*, S. CHINA MORNING POST (Feb. 15, 2022, 2:30 PM), https://perma.cc/MP7U-V5XY.

95. Keith Zhai & Liza Lin, *China to Conclude Didi Cybersecurity Probe, Lift Ban on New Users*, WALL ST. J. (June 6, 2022), https://perma.cc/5UCQ-QHEL.

96. Jing Yang & Dave Sebastian, *Didi Ends Tumultuous Run as a New York-Listed Company*, WALL ST. J. (June 10, 2022), https://perma.cc/JED2-SVSZ.

97. *See* Keith Zhai & Liza Lin, *Chinese Regulator to Fine Didi More Than $1 Billion over Data-Security Breaches*, WALL ST. J. (July 19, 2022), https://perma.cc/RGK7-8P4L.

98. *See supra* notes 90–93 and accompanying text.

99. *See* Heather Somerville, *The Answer to Uber's Profit Challenge? It May Lie in Its Trove of Data*, REUTERS (May 9, 2019, 4:07 AM), https://perma.cc/RV62-NWE6 (remarking on the value of the "treasure trove of trip data" in advance of Uber's IPO).

microprocessors, wireless signals, and connectivity—which is steadily becoming most modern automobiles.

B. Smart Vehicles

Modern vehicles are connected to the internet and collect data to function—electric and self-driving vehicles collect even more.[100] These types of vehicles function by persistently amassing varied, detailed data that reveals far more than simple location, including video, radar, and other specialized datatypes.[101] The PRC has significant security concerns over vehicle data leaving mainland China.[102] It banned officials from owning Tesla vehicles and the vehicles themselves from entering sensitive government areas.[103] In light of increased PRC regulatory attention, Tesla has undertaken several measures to appease the PRC and hopefully thereby maintain access to the lucrative market.

---

100. *See* Cara Bloom et al., *Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles*, USENIX (July 14, 2017), https://perma.cc/PS38-ZG75 (PDF); *see also Autonomous Car Data: Future Cars Run on Data, Not Gasoline*, SUMMA LINGUAE, https://perma.cc/43HX-QFT8 (last updated July 26, 2021).

101. *See* Andrew J. Hawkins, *Waymo Is Disclosing More Autonomous Vehicle Data for Research Purposes*, THE VERGE (Mar. 10, 2021, 10:00 AM), https://perma.cc/PUX3-7RFA (describing Google's self-driving vehicle subsidiary Waymo's dataset and its pertinent datatypes).

102. *See* Eamon Barrett, *Tesla Just Had Its Best Month Ever in China—But a New Data Law Looms Large*, FORTUNE (Oct. 12, 2021, 5:59 AM), https://perma.cc/66KY-9GM9 (reporting on the DSL prompting PRC regulators to assess the types of data smart vehicles collect and transfer overseas).

103. *See* Shunsuke Tabeta, *China Clamps Down on Auto Data Collection by Tesla and Others*, NIKKEI (May 13, 2021, 3:59 AM), https://perma.cc/NYC7-YV92.

Tesla initially enjoyed remarkable success in the PRC market.[104] However, Tesla soon encountered obstacles.[105] In 2021, state-run media airwaves broadcasted accusations of safety concerns leading to high-profile protests and eventually a "recall of almost all the cars Tesla has ever sold in the [PRC]—more than 285,000 in all—to address a software flaw."[106] The onslaught of protests, the lack of censorship on social media, and unfavorable treatment by state-run media prompted observers to suspect that the CCP was supportive of—if not involved in—Tesla's public relations kerfuffle.[107] Allegations of safety concerns, spurious or otherwise, and their rampant spread on social media could be cynically characterized as a CCP tactic to rein in a foreign corporation—a foreign corporation that jumpstarted the PRC electric vehicle market but was also jeopardizing the PRC data objective of keeping all PRC citizen data out of the clutches of foreign nations.[108] The CCP quickly enacted laws that would solidify its control over the detailed data collected by smart vehicles.

---

104. *See Tesla's Fall From Grace in China Shows Perils of Betting on Beijing*, BLOOMBERG BUSINESSWEEK, https://perma.cc/Z9H7-CG5H (last updated July 6, 2021, 5:01 AM) (reporting on Tesla's early success in the PRC, including "receiving red-carpet treatment from government officials, who granted Tesla the unprecedented concession of allowing it to wholly control its local subsidiary, . . . substantial assistance building its Shanghai facility and helping it reopen rapidly after the nationwide coronavirus shutdown").

105. *See id.* ("Until recently, the unspoken bargain between Musk and Beijing seemed relatively clear: in exchange for state support, the company would use its brand and high-tech expertise to attract Chinese consumers to electric vehicles, while pushing local manufacturers of EVs and components to up their game.").

106. *See id.* ("[Tesla's recent difficulties] . . . provide[] compelling evidence of how fraught operating in China can be, even for those who appear to enjoy every possible advantage.").

107. *See id.* ("But the [protestor]'s presence at the high-security ticketed event—and the fact that images of her circulated uncensored on social networks—prompted industry observers to wonder whether officials were quietly supportive of her actions.").

108. *See generally* SCOTT W. HERALD ET AL., CHINESE DISINFORMATION EFFORTS ON SOCIAL MEDIA (2021), https://perma.cc/52QP-Z9HG (PDF).

In April 2021, the PRC proposed regulations focused on automobile data storage.[109] Tesla sought to address the PRC's concerns by constructing a PRC data center so that any domestically-collected data would remain in the PRC and under CCP control.[110] Even with the data center constructed, the PRC remains concerned about the data Tesla vehicles collect.[111] Other foreign automobile manufacturers also have kept their user data inside the PRC, thus adversely affecting overseas technology development.[112] The CCP's data focus will remain a costly problem for vehicle manufacturers who want to access the world's largest automobile market.[113] Vehicle data provides analytical insights about their drivers and the CCP is equally concerned about companies collecting data about PRC citizens.

V. HEALTH DATA

Currently, health data is one of the most precious datatypes. Health data is immensely valuable, especially when compared to other datatypes, but privacy concerns and different

109. *See* Eamon Barrett, *Tesla Changes Its China Data Policy After Government Scrutiny*, FORTUNE (May 26, 2021, 6:18 AM), https://perma.cc/F3C7-XGZA (reporting on the automobile-specific regulations that "require[] automakers to store user data in China and obtain special permission to send any data abroad").

110. *See* Trefor Moss, *Tesla to Store China Data Locally in New Data Center*, WALL ST. J. (May 26, 2021, 3:43 AM), https://perma.cc/29ZT-5JNP.

111. *See China Develops Machines that Can Track Data Sent Abroad by Cars*, REUTERS (Sept. 14, 2021, 10:02 AM), https://perma.cc/5JFY-MWBX (reporting on technological efforts to curtail extraterritorial data transfers out of the PRC).

112. *See* Yilei Sun & Tony Munroe, *EXCLUSIVE As China Plans New Rules, Global Automakers Move to Store Car Data Locally*, REUTERS (May 27, 2021, 10:08 AM), https://perma.cc/M9TZ-AJFM ("BMW, Daimler and Ford have set up facilities in China to store data generated by their cars locally . . . as automakers come under growing pressure in the world's biggest car market over how they handle information from vehicles."); *see also* Shunsuke Tabeta, *China Data Rules to Squeeze Overseas Development of Self-Driving Tech*, NIKKEI (Aug. 22, 2021, 1:26 AM), https://perma.cc/2JHP-YLQ5 (predicting that PRC regulations mean "information generated in [the PRC] will mostly stay within the country").

113. *See* Anjani Trivedi, *China Targets the Troves of Data Collected by Electric Vehicles*, TAIPEI TIMES (July 25, 2021), https://perma.cc/QZY8-8T34.

nations' healthcare infrastructures make market valuations difficult.[114] One valuation method is to examine the prices that health data yields in cybercrime markets.[115] In addition to using cybercrime analogs, health data is valued by using efficiency gains and measuring improvements in analytical fidelity.[116] Regardless of valuation methodology, it is remarkable that a health record is often fifty times more valuable than a stolen credit card.[117] Recognizing the value of health data, some companies—like 23andMe—rely on such data almost exclusively in their business model.[118]

A. 23andMe

The genetic testing company 23andMe has faced persistent concerns over data security since 2013.[119] For years, privacy considerations were the biggest roadblock to 23andMe conducting a public offering.[120] Experts argue that 23andMe has

114. *See Life Sciences Industry*, EY, https://perma.cc/AUK2-44RR.

115. *See* Ellen Neveux, *Hackers, Breaches, and the Value of Healthcare Data*, SECURELINK (June 30, 2021), https://perma.cc/Q2XR-HDAB (last updated Oct. 1, 2021).

116. *See How Global Data Flows Can Unlock the Value of Health Data*, HEALTHCARE IT NEWS (June 21, 2021, 10:21 AM), https://perma.cc/PKN9-F75C (arguing that "enhanced patient care, more efficient health systems and advanced research models" drive the true value of healthcare data).

117. *See* Will Maddox, *Why Medical Data is 50 Times More Valuable Than a Credit Card*, D MAG. (Oct. 15, 2019, 11:09 PM), https://perma.cc/98YK-8D4Q.

118. *See* Marcy Darnovsky, *23andMe's Dangerous Business Model*, N.Y. TIMES, https://perma.cc/UG9E-G38C (last updated Mar. 2, 2015, 3:30 AM) ("[23andMe's] business model depends on packaging and reselling its customers' genetic data and other information.").

119. *See* Charles Seife, *23andMe Is Terrifying, but Not for the Reasons the FDA Thinks,* SCI. AM. (Nov. 27, 2013), https://perma.cc/QAQ3-8RLY; *see also* Kendra T, *23andMe: Losing at Digital Privacy*, HARV. BUS. SCH. (Feb. 11, 2020), https://perma.cc/4BBS-RE8U.

120. *See* Kari Paul, *Fears over DNA Privacy as 23andMe Plans to Go Public in Deal with Richard Branson*, THE GUARDIAN (Feb. 9, 2021, 4:54 PM), https://perma.cc/6U7L-ECCT.

two business models—one targeting consumers and the other aimed at selling customer data to researchers.[121]

When 23andMe finally went public, one of the company's investors presented a preliminary outline of the CEO's vision.[122] This vision depended on gaining a critical mass of users providing their genetic information, resulting in a database of DNA information.[123] In 2018, the company entered a $300 million deal with a drug manufacturer to use its DNA data for health and pharmaceutical research.[124] In so doing, 23andMe signaled its readiness to use its database for research and development, thereby tacitly acknowledging that its database purportedly yields insights into the health of its users and, in the aggregate, can inform scientific progress. 23andMe has PRC investors, but the CEO has stated that "Chinese investors have no access to the genetic information of the company's customers."[125] Curiously, the 23andMe CEO also stated that her biggest concern is the PRC "very publicly stating that they wanna [sic] win in the genetic information revolution."[126]

121. *See* Henri-Corto Stoeklé et al., *23andMe: A New Two-Sided Data-Banking Market Model*, BMC MED. ETHICS (2016), https://perma.cc/N3BY-N9QM (PDF) (highlighting the likelihood that 23andMe's business objectives are "two-fold: promoting itself within the market for predictive testing . . . at a low cost to consumers, and establishing a high-value database/biobank for research").

122. *See* Kristen V. Brown, *All Those 23andMe Spit Tests Were Part of a Bigger Plan*, BLOOMBERG BUSINESSWEEK (Nov. 4, 2021, 5:00 AM), https://perma.cc/JJM6-BWUN.

123. *See id.* ("[I]t wouldn't be crazy for the 8.8 million 23andMe customers who once absently checked a box saying yeah, sure, use my data for whatever, to feel like they've been bait-and-switched now that their genes are laying the groundwork for potential cancer cures.").

124. *See* Jamie Ducharme, *A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?*, TIME (July 26, 2018, 3:47 PM), https://perma.cc/F6NX-X7BG.

125. *See* Jon Wertheim, *Companies and Foreign Countries Vying for Your Data*, 60 MINUTES (Jan. 31, 2021), https://perma.cc/77CL-52VX (denying a data sharing agreement with Chinese investors but emphasizing "the Chinese threat to U.S. biotech is real").

126. *Id.*

Due to the PIPL's explicit proscription on biometric and health data,[127] the PRC's avowed goal to "win in the genetic information revolution," and privacy concerns in the U.S., any collection of genetic or health data will fall squarely within the "rights of PRC citizens" and almost certainly draw the ire of PRC regulators.[128] The Three Laws may force 23andMe to either comply with oppressive data regulations that de facto cede control over its data to the CCP or bar PRC citizens from purchasing its products. But DNA testing companies are not the only companies to offer products that collect users' health data.

B. Wearable Technology and Fitness Trackers

Wearable fitness trackers, such as Google's Fitbit products or an Apple Watch, collect biometric data on wearers.[129] The Chinese military has voiced concerns that wearables may pose a national security risk if worn by military personnel.[130] This data is not just managed by the device maker, but is often linked and shared with other companies, sometimes resulting in large-scale data breaches.[131] Fitness trackers collect a cornucopia of valuable data. Indeed, regulators' objections to

127. *See supra* Part I.B.

128. *See supra* Part I.

129. *See Do Fitness Trackers Put Your Privacy at Risk?*, KASPERSKY, https://perma.cc/3J6D-3VAH (providing a high-level overview of fitness tracker data collection and the datatypes wearables collect including "weight, blood pressure, what distances you run or walk, your heart or lung function, your menstrual cycle, your sleep patterns").

130. *See China Says Wearable Tech Could Leak Secrets*, CYBER SEC. INTEL. (May 20, 2015), https://perma.cc/U4X7-HSJ5 (reporting on the publication in the People's Liberation Army Daily of concerns that "[t]he moment a soldier puts on a device that can record high-definition audio and video, take photos, and process and transmit data, it's very possible for him or her to be tracked or to reveal military secrets").

131. *See* Heather Landi, *Fitbit, Apple User Data Exposed in Breach Impacting 61M Fitness Tracker Records*, FIERCE HEALTHCARE (Sept. 13, 2021, 4:21 PM), https://perma.cc/E8HR-EJ95 (reporting on a data breach of a third-party data aggregator that allows its users to sync across different fitness tracker platforms that could "make[] it much easier for bad actors to locate where people are living or staying, and can expose patterns of travel").

Google's acquisition of Fitbit demonstrate the value of this data to online advertising and other private sector industries.[132] One of the most popular wearables is the Apple Watch.[133] Apple's PRC presence provides excellent insight into how one of the world's largest companies navigates selling a product reliant on rich, arguably invasive, data collection in an oppressive regulatory environment.

"[J]ust as [current Apple CEO Tim] Cook figured out how to make China work for Apple, China is making Apple work for the Chinese government."[134] Apple is by far the most successful American company in the PRC, generating over $55 billion a year in revenue from the country and assembling nearly all of its products in Chinese factories.[135] The CCP has extracted many concessions from Apple as the company attempts to balance this critical relationship and avoid the ire of the CCP.[136] For instance, to comply with PRC law and maintain its lucrative and dominant PRC market share, all of Apple's PRC customer data is stored inside the PRC.[137]

Apple has ceded control to PRC authorities over managing its data center, what encryption is used in the PRC, and—in

132. *See* Argam Artashyan, *Google's Acquisition of Fitbit Transaction Raises Data Collection Concerns*, GIZCHINA (July 4, 2020), https://perma.cc/849A-U9GK (reporting on the EU and Australian regulatory concerns that "[b]uying Fitbit will allow Google to build an even more comprehensive set of user data, further cementing its position and raising barriers to entry to potential rivals").

133. *See* Nick Statt, *Apple Now Sells More Watches Than the Entire Swiss Watch Industry*, THE VERGE (Feb. 5, 2020, 7:39 PM), https://perma.cc/D5AY-C9RA.

134. Jack Nicas et al., *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (May 17, 2021), https://perma.cc/DNP3-QDLY (last updated June 17, 2021).

135. *See id.* (emphasizing Apple's "high profile and acute dependence on the [PRC]").

136. *See id*. (outlining Apple's compromises in the PRC including removing "Designed by Apple in California" from its iPhones, and other ways that Apple has "put the data of its Chinese customers at risk and has aided government censorship in the Chinese version of its App Store").

137. *See id.* ("Cook agreed to move the personal data of his Chinese customers to the servers of a Chinese state-owned company. That led to a project known inside Apple as 'Golden Gate.'").

violation of sound cybersecurity principles—it has made the encryption keys as easily accessible as possible.[138] To avoid U.S. laws prohibiting American companies from turning over data to PRC law enforcement, Apple does not even own its PRC customer data.[139] By allowing a PRC state-owned company to own Apple customer data, the PRC is able to request data from the PRC company and Apple can avoid running afoul of the U.S. laws that prohibit Apple from complying with these data requests themselves.[140] "[If] Chinese intelligence has physical control over your hardware—that's basically a threat level you can't let it get to."[141] Apple rebuts concerns about PRC authorities having physical control by emphasizing that its encryption makes illegitimate access impossible.[142] However, PRC law requires approval of any encryption standard and expert opinions say that housing the encryption keys inside the PRC—even worse, in the same building as the encrypted data—drastically increases the likelihood of the CCP accessing both

138. *See id.* ("Chinese state employees physically manage the computers. Apple abandoned the encryption technology it used elsewhere after China would not allow it. And the digital keys that unlock information on those computers are stored in the data centers they're meant to secure.").

139. *See id.* ("Apple has ceded legal ownership of its customers' data to Guizhou-Cloud Big Data, or GCBD, a company owned by the government of Guizhou province, and Apple's iCloud terms and conditions lists GCBD as 'service provider' and Apple as 'an additional party.'").

140. *See id.* ("Apple believes [Chinese authorities asking GCBD—not Apple—for Apple customers' data] gives it a legal shield from American law."); *see also* Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2523 (providing the statutory framework for international law enforcement data sharing); DOJ, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/33ZK-UPVA (PDF) (explaining the legislative intent and ramifications of the CLOUD Act).

141. Nicas, *supra* note 134 (quoting Matthew D. Green, a cryptography professor at Johns Hopkins University).

142. *See id.* (quoting Apple as saying that its iCloud security is designed "in such a way that only Apple has control of the encryption keys").

the encryption keys and the customer data those keys are supposed to protect.[143]

Apple also provides user data to law enforcement in the United States.[144] The higher number of instances in which Apple provides data to U.S. law enforcement may indicate that the PRC does not need to request the data from Apple because it already possesses the data as a result of the structure and ownership of Apple's data centers in the PRC.[145] A new compromise is on the horizon as the PRC wants Apple to store more of its user data inside the country, arguably making the data even more accessible to PRC authorities through extrajudicial means.[146]

Apple's compromises demonstrate that even the world's largest companies are not exempt from the PRC's ravenous data zealotry. Apple's concessions are concerning from privacy and human rights perspectives and are equally indicative of the economic barriers to entry that the PRC's data regulations create. Smaller, less successful companies who wish to operate in the PRC may lack Apple's budget to build localized data centers or the negotiating power of one of the world's largest companies, and would likely be completely beholden to the whims of the CCP if they wish to do business inside one of the world's largest markets. Apple's products collect mountains of various types of data that add up to greater than the sum of their parts, and the CCP focus on controlling this treasure trove demonstrates both the value of the aggregated data and the CCP's recognition thereof.

---

143. *See id.* (quoting Ross J. Anderson, University of Cambridge cybersecurity researcher, as saying, "I'm convinced that [the PRC] will have the ability to break into [Apple's] servers").

144. *See id.* ("[F]rom 2013 through June 2020, Apple said it turned over the contents of iCloud accounts to U.S. authorities in 10,781 separate cases [as compared to Apple providing] the contents of an undisclosed number of iCloud accounts to the [PRC] government in nine cases and challeng[ing] just three government requests.").

145. *See id.* ("[T]he [PRC] government has two avenues to [Apple] data[:] demand it—or take it without asking.").

146. *See* U.S. DEPT. OF STATE, 2022 INVESTMENT CLIENT STATEMENTS: CHINA (2022), https://perma.cc/NSX4-M39H (remarking that the Three Laws will increase the CCP's data localization campaign).

VI. AGGREGATED DATA

A solitary datapoint may provide some insights. By combining multiple datapoints, however, that insight can be honed and made increasingly prescient. Combining data from multiple sources is a tactic utilized by both the public and private sector to increase data's value and accuracy. Recent events indicate that the CCP assuredly understands this concept—and in fact is pursuing it as a national security priority.

A. Grindr and OPM

Combining different data sources and types can often result in greater utility than the sum of the individual data. Companies and governments are increasingly focused on the risks that such aggregated data presents. On September 30, 2021, the board of Five9, a cloud contact-center company, disapproved a merger with the PRC-linked teleconferencing company Zoom.[147] The Five9 board did so on the heels of reports that U.S. regulators were evaluating the national security implications of a merger involving Zoom due to its entrenched PRC links.[148] Zoom's relevance and prevalence during the COVID-19 pandemic were accompanied by warnings about the teleconferencing application's data privacy and usage.[149] Teleconferencing data—who calls whom, for how long, etc.—is obviously valuable data. This importance is exemplified by the

147. *See* Joe Williams, *Zoom's Contact-Center Future Is on Hold After the Five9 Fallout*, PROTOCOL (Oct. 1, 2021), https://perma.cc/3AL9-ZRKT.

148. *See* Jordan Novet, *U.S. Committee Is Reviewing Zoom's $14.7 Billion Deal for Five9 on National-Security Grounds*, CNBC (Sept. 21, 2021, 4:04 PM), https://perma.cc/C6E8-3FU2 ("USDOJ believes that such [national security] risk may be raised by the foreign participation (including the foreign relationships and ownership) associated with the application . . . .").

149. *See* Shannon Bond, *A Must for Millions, Zoom Has a Dark Side—and an FBI Warning*, NPR (Apr. 3, 2020, 5:00 AM), https://perma.cc/E7WR-QZXD (reporting on Zoom's privacy issues and how a former NSA analyst describes the software as "[t]hings you just would like to have in a chat and video application—strong encryption, strong privacy controls, strong security—just seem to be completely missing").

fact that wiretapping, which yields similar datapoints, has been illegal for years prior to the advent of the internet.[150] By only evaluating obviously valuable datatypes, however, nations would be shortsightedly attempting to stem the tide of PRC data chicanery.

For any given datatype, countries must evaluate how aggregated datasets add up to greater than the sum of their individual datapoints. In 2019, the Committee on Foreign Investment in the United States (CFIUS) ordered a PRC company to sell its ownership stake in Grindr, a dating application catering to the LGBTQ+ community.[151] Because the sensitive Grindr data would be available to PRC governmental entities, the opportunity for PRC malfeasance and blackmail is readily apparent. Comparing and aggregating datasets can astronomically increase the likelihood of exposure and deanonymization.

In 2015, reports surfaced that the United States Office of Personnel Management (OPM) had been hacked, exposing the records of nearly all civilian government employees—including any applications submitted for security clearances.[152] U.S. authorities attributed this breach to PRC-affiliated hackers.[153] The OPM hack yielded a wealth of data on nearly all former and current federal government employees, and this intelligence was squarely under PRC control.[154] Cumulatively, the OPM and

150. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523.

151. *See* Georgia Wells & Kate O'Keeffe, *U.S. Orders Chinese Firm to Sell Dating App Grindr over Blackmail Risk*, WALL ST. J. (Mar. 27, 2019, 6:43 PM), https://perma.cc/553J-G9SY (reporting on the forced sale amid "the risk that the personal data it collects could be exploited by Beijing to blackmail individuals with security clearances").

152. *See* Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, WIRED (Feb. 11, 2020, 2:58 PM), https://perma.cc/RGM3-RSHS ("Some of the biggest hacks of Americans' private data in the past decade had been the work of the Chinese government, resulting in massive, unparalleled espionage advantage[s].").

153. *See id.* ("Then-director of national security James Clapper named the [PRC] as the 'leading suspect.'").

154. *See id.* (quoting Attorney General Barr as saying that "this data has economic value, and these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages").

Grindr data combined to alert CFIUS and other U.S. government agencies tasked with protecting national security to a potential exposure threat.[155]

Historically, governments have considered many factors in granting security clearances, including sexual orientation, particularly if closeted.[156] Since Grindr has granular data over the messages, locations, sexual orientations, and even sexual health of its users, this Grindr database could augment the hacked OPM data. Combining the OPM and Grindr data would "create a database of the Social Security numbers, fingerprints and compromising photographs of thousands of gay U.S. government employees."[157] Regardless of one's stance on whether sexual preference increases the likelihood of blackmail, CFIUS's order for the PRC company to sell its Grindr stake reflects that data-constructed blackmail is likely a concern when evaluating PRC access to private sector and U.S. citizen data.[158] Unfortunately, the torrid pace of PRC data theft and collection has not slowed.

B. Equifax

In 2017, Equifax, one of the main U.S. credit reporting companies, disclosed that the personal information of 143 million Americans under its control had been breached, including Social Security numbers and granular information

155. *See* Carl O'Donnell et al., *Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, REUTERS (Mar. 27, 2019, 1:02 AM), https://perma.cc/SNJ5-97CU ("CFIUS' specific concerns and whether any attempt was made to mitigate them could not be learned. The United States has been increasingly scrutinizing app developers over the safety of personal data they handle, especially if some of it involves U.S. military or intelligence personnel.").

156. *See* Gregory B. Lewis, *Barriers to Security Clearances for Gay Men and Lesbians: Fear of Blackmail or Fear of Homosexuals?*, 11 J. PUB. ADMIN 539, 540–45 (2001).

157. Isaac Stone Fish, Opinion, *China Has Access to Grindr Activity. We Should All Be Worried*, WASH. POST (Apr. 9, 2019), https://perma.cc/8NSL-TU57.

158. *See supra* note 155 and accompanying text.

about their financial situations.[159] In 2020, the United States Department of Justice charged four PRC military personnel with perpetrating the hack.[160] The PRC expectedly denied involvement.[161] The Equifax data has significant value to foreign intelligence agencies wishing to identify people who are in dire financial straits and therefore susceptible to potential bribery.[162] Additionally, identifying people susceptible to bribery in the private sector could be an avenue for intellectual property theft.[163] Pairing the 147 million Equifax records with the 21.5 million OPM records would provide a fulsome list of people with security clearances and their financial status.[164] Bribery and blackmail are favorite tactics of intelligence agencies.[165] The PRC has paid scientists in the hopes of pilfering their knowledge

159. *See* Pete Schroeder, *Equifax to Pay up to $650 Million in Data Breach Settlement*, REUTERS (July 22, 2019), https://perma.cc/EVP5-Z494 ("'This company's ineptitude, negligence, and lax security standards endangered the identities of half the U.S. population,' New York Attorney General Letitia James said in a statement.").

160. *See U.S. Charges Four Chinese Military Hackers in 2017 Equifax Breach*, REUTERS (Feb. 10, 2020, 10:24 AM), https://perma.cc/A9AV-54ZD (quoting a former White House cybersecurity coordinator as saying that "the Equifax hack fits into a pattern of past Chinese cyberattacks . . . because the stolen data can support other spying efforts").

161. *See id.* ("Chinese foreign ministry spokesman Geng Shuang denied the allegations . . . and said China's government, military and their personnel 'never engage in cyber theft of trade secrets.'").

162. *See id.* ("[The Equifax data's] primary utility would be in developing potential targets for approach by intelligence operatives or feeding artificial intelligence [and] machine learning tools.").

163. *See* Josephine Wolff, *That Enormous Equifax Hack Looks a Lot More Bizarre Now*, SLATE (Feb. 11, 2020, 10:57 AM), https://perma.cc/P9RK-PWP4 (commenting on the uncertainty of "[w]hatever the Chinese government plans to do with this information—whether that's extortion, identifying people in precarious financial positions who might be susceptible to bribery, or simply putting together more comprehensive dossiers on people of interest to them").

164. *See id.*

165. *See* Jackie Northam, *Russian Spies' Go-To Tactics for Entangling People: Bribery and Blackmail*, NPR (Apr. 11, 2017, 2:06 PM), https://perma.cc/J856-XLA8 ("Loans, payments, sweetheart deals or other transactions are a tried and tested way that Russia's spy agencies get access to or control over people who interest them.").

and research.[166] The Equifax data identifies who would be the best target for such tactics, and the OPM data further identifies those with government secrets who would be susceptible to such bribery or blackmail.[167] The PRC continues in its quest to collect the best data possible to augment its already ample warehouse of detailed data on American citizens.

C. Other Alleged PRC Hacking Efforts

In February 2020, then-Attorney General William Barr publicly attributed some of the largest data breaches of U.S. companies to PRC efforts to collect personal data on Americans.[168] "China's hoovering of Americans' private data has long been one of the biggest open secrets of modern intelligence."[169] Hacks of Marriott hotel data and Anthem health insurance records have been attributed to PRC governmental entities.[170] With access to hotel data, one can surmise who is staying at what hotel and for how long—yielding powerful insights. For example, knowledge that a group of executives are frequently staying at hotels near the headquarters of another

166. *See* Nate Raymond, *Harvard Professor Convicted by U.S. Jury of Lying About China Ties*, REUTERS (Dec. 21, 2021, 8:33 PM), https://perma.cc/DZ7B-ZR4G ("[The Wuhan University] agreed to pay him up to $50,000 per month plus $158,000 in living expenses, and he was paid in cash and deposits to a Chinese bank account, prosecutors said.").

167. *See* Christy Cooney, *China Accused of Stealing Australian Students' Data to Blackmail Them*, N.Y. POST (June 7, 2019, 3:00 PM), https://perma.cc/B5YH-YDJV (reporting that the PRC allegedly collected banking, tax, and academic records to potentially blackmail victims into committing espionage); Angus Grigg, *White House: China's 'Digital Dossiers' to Blackmail and Intimidate*, FIN. REV. (Oct. 26, 2020, 12:00 AM), https://perma.cc/5EU2-NPG6 ("Assembling such 'dossiers' [has] always been part of Leninist regimes and their efforts to influence, humiliate, divide and blackmail opponents [and] this [has] become far easier in the digital age.").

168. *See* Graff, *supra* note 152 ("For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from [OPM], the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax.").

169. *Id.*

170. *Id.*

company could signal a potential merger or acquisition. Alternatively, hotel data coupled with the OPM data could identify holders of security clearances who are not staying at their own home, either for professional or personal reasons. Further, the Marriott hack also involved passport data, which presents significant privacy concerns for Americans.[171] Health insurer data can yield insights into the health of Americans. "By combining personnel data with travel records, health records, and credit information, Chinese intelligence has amassed in just five years a database more detailed than any nation has ever possessed about one of its adversaries."[172] The PRC values American data enough to perpetrate the largest hacks in history. The Three Laws are their attempt to prevent the same from being done to them.

VII. ARE THE THREE LAWS ENFORCEABLE? IF SO, HOW?

As the anecdotes above demonstrate, the Three Laws present monumental compliance tasks for companies. However, the compliance risks must be balanced against the likelihood that the Three Laws will be effectively enforced. Companies must (i) identify which of the Three Laws present the greatest risk, (ii) understand how courts outside the PRC might view an extraterritorial penalty, and (iii) understand that the extraterritorial nature of the Three Laws mandates a global analysis of PRC influence.

A. The DSL is the Wild Card; the PIPL is Just GDPR With Chinese Characteristics

If companies already comply with GDPR, they should find complying with the PIPL easily attainable. The PRC promulgated the PIPL as companion legislation to the DSL, and

171. *See* David E. Sanger et al., *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://perma.cc/GY4B-6UKF ("[P]assport information would be particularly valuable in tracking who is crossing borders and what they look like, among other key data.").

172. Graff, *supra* note 152.

the heavier fines and similarity to the EU's GDPR has occupied much of the media discussion on the new PRC data regulations.[173] This focus is misplaced. "If companies are compliant with Europe's GDPR, 'they are going to be fine complying with [the PIPL].'"[174] Companies cite the PRC's "increasingly challenging business and legal environment" as the key motivator to abandoning one of the world's largest economies.[175] These companies have not exited Europe, so they ostensibly comply with GDPR.[176] GDPR and the PIPL are analogous and impose similar compliance costs, so if the PIPL is not the "legal environment" that concerns them, then perhaps they are deterred by the PRC's differing views on data and privacy reflected in the rest of the Three Laws. Indeed, the DSL and its focus on national security would provide the best insight into the opaque regulatory framework undergirding the CCP's control of the PRC.

Any application of the DSL to inculpate a foreign company would also likely include allegations of PIPL impropriety. The broad language of both statutes makes selective and arbitrary enforcement possible and even likely.[177] However, the aspects of

---

173. *See generally* Eva Xiao, *China Passes One of the World's Strictest Data-Privacy Laws*, WALL ST. J., https://perma.cc/RGX5-BGDG (last updated Aug. 20, 2021, 4:55 AM); Catherine Zhu, *Is China's New Personal Information Privacy Law the New GDPR?*, BLOOMBERG L. (Sept. 17, 2021, 4:01 AM), https://perma.cc/CN9R-E3ZV; Matt Burgess, *Ignore China's New Data Privacy Law at Your Peril*, WIRED (Nov. 5, 2021, 7:00 AM), https://perma.cc/7Y94-9NSB.

174. Xiao, *supra* note 173.

175. *See, e.g.*, Nick Turner, *Yahoo Quits China in Wake of LinkedIn Exit as Media Hurdles Grow*, BLOOMBERG (Nov. 2, 2021, 9:50 PM), https://perma.cc/PSN9-3Y4K ("In recognition of the increasingly challenging business and legal environment in China, Yahoo's suite of services will no longer be accessible from mainland China as of Nov. 1.").

176. *See Learn More About the General Data Protection Regulation (GDPR)*, LINKEDIN, https://perma.cc/8NWY-M8XJ; *Data Processing Agreement*, YAHOO, https://perma.cc/U9N6-KVN6 (providing that Yahoo and its vendors must comply with GDPR); *see also* YAHOO FR., https://perma.cc/4W48-XGT4 (demonstrating that Yahoo is still available in the EU).

177. *See DSL*, *supra* note 8, art. 2 ("When data handling activities outside the mainland territory of the PRC harm the national security, the public

the PIPL that vary from the EU's GDPR are squarely within the ambit of the DSL—namely "national security." By understanding the PRC view as to what data falls within their national security interests, companies can attempt to predict what fickle regulatory risks they may potentially have to address to remain in the PRC market. If a company is not operating within the PRC, however, its regulatory risk is not obviated due to the Three Laws' extraterritorial provisions. The Three Laws reach across borders and would require recognition by a foreign court to be enforced.

B. U.S. Courts Will Likely Not Enforce a Three Laws Fine

How do U.S. courts treat foreign enforcement decisions in the internet context? The Three Laws have not yet been enforced in the United States, but it is highly unlikely that a U.S. court would ever enforce a Three Laws fine against an American company.

In *Yahoo v. La Ligue Contre Le Racisme Et L'Antisemitisme*,[178] the Ninth Circuit dealt with a foreign organization obtaining a French court penalty that would affect a U.S. internet service provider's content moderation.[179] La Ligue Contre Le Racisme Et L'Antisemitisme (LICRA) obtained an order from a French court that threatened significant financial penalties if Yahoo did not bar access to Nazi websites.[180] Peculiar to this case is the fact that Yahoo had already attempted to comply with the French court's order and limit access to Nazi websites within France.[181] Since the internet easily transcends borders, however, these websites were still accessible from France by users seeking out Yahoo's U.S.

---

interest, or the lawful rights and interests of citizens or organizations of the PRC, legal liability is to be pursued according to the law."); *supra* Part I.

178. 433 F.3d 1199 (9th Cir. 2006).

179. *See generally id.*

180. *See id.* at 1203–04.

181. *See id.* at 1205 ("However, after conducting its own Internet research on yahoo.com, the district court found that even after this policy change, Yahoo! 'appear[s]' not to have fully complied with the orders with respect to its auction site.").

services.[182] The Ninth Circuit initially focused on whether the district court possessed personal jurisdiction over the French parties when the lower court granted summary judgment in favor of Yahoo.[183] While the Ninth Circuit held that there were sufficient minimum contacts for personal jurisdiction over the French defendants, the court reversed and remanded based on its view that the appeal was not ripe for decision.[184] However, the *Yahoo* court squarely addressed the enforceability of foreign fines and penalties in the hypothetical.

In *Yahoo*, the Ninth Circuit analyzed the enforceability of foreign penalties in U.S. courts and found it "exceedingly unlikely that any court in California—or indeed elsewhere in the United States—would enforce" a foreign monetary penalty.[185] While *Yahoo* applied California law, U.S. federal and state courts are generally loath to enforce foreign fines or penalties as a settled common law rule.[186] "[T]he common law rule against the enforcement of penal judgments is venerable and widely-recognized."[187] Further, The Restatement (Third) of Foreign Relations Law emphasizes that U.S. courts are not required to recognize foreign fines or penalties.[188]

The background of *Yahoo* is key to understanding this case. There was no actual fine or enforcement from the French court,

182. *See id.* at 1202 ("Conversely, any user in France can type www.yahoo.com into his or her browser, or click the link to Yahoo.com on the Yahoo! France home page, and thereby reach yahoo.com.").

183. *See id.* at 1205–11.

184. *See id.* at 1223–24.

185. *Id.* at 1218.

186. *See id.* at 1219–20 (commenting that "California courts follow the generally-observed rule that, [u]nless required to do so by treaty, no [i.e. country] enforces the penal judgments of other states [i.e. countries] . . . [and a] number of states have adopted an identical version of California's Uniform Act" (alterations added and in original) (internal quotation omitted)).

187. *Id.* at 1219 (citing Huntington v. Attrill, 146 U.S. 657, 673–74 (1892)).

188. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 483 (AM. L. INST. 1987) ("Courts in the United States are not required to recognize or to enforce judgments for the collection of taxes, fines, or penalties rendered by the courts of other states.").

merely the prospect of such monetary penalty.[189] Yahoo brought this suit partially based on a concern that the "threat of a monetary penalty hangs like the sword of Damocles."[190] Even without an actual monetary penalty, the Ninth Circuit still analyzed and found that U.S. courts will generally not enforce foreign fines and penalties.[191] Using *Yahoo* as precedent, it is unlikely that a U.S. court would enforce a PRC judgment against a U.S. company predicated on the Three Laws.[192]

The internet's nebulous borders loomed heavily in *Yahoo*.[193] The PRC cordons off its cyberspace from the rest of the world's networks.[194] Any use of *Yahoo* as precedent to avoid a PRC penalty would need to address how the very mechanism of evading geographic controls on browsers is decidedly against PRC law, as well as the distinguishing fact that there are technical and societal controls in place to prevent PRC citizens from escaping the manicured network behind the Great

189. *See* Yahoo v. La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199, 1218 (9th Cir. 2006) ("[The French defendants] have represented that they have no intention of seeking a monetary penalty by the French court so long as Yahoo! does not revert to its 'old ways.'").

190. *Id.* at 1218.

191. *See id.* at 1218–21.

192. *See* 30 AM. JUR. 2D *Executions and Enforcement of Judgments* § 653 (2022) ("Courts in the United States will not recognize or enforce a penal judgment rendered in another nation.").

193. See *Yahoo*, 433 F.3d at 1202 ("In actual practice, however, national boundaries [on the internet] are highly permeable.").

194. *See* Yaqiu Wang, *In China, the 'Great Firewall' is Changing a Generation*, POLITICO (Sept. 1, 2020), https://perma.cc/H2E2-8RXM.

Firewall.[195] *Yahoo* nonetheless stands for the proposition that U.S. courts will not rubber-stamp foreign fines and penalties.[196]

Since *Yahoo* explicitly finds most foreign fines and penalties are unenforceable in the United States, a company's Three Laws risk will hinge on its exposure to PRC levers for enforcement. Operating inside the PRC is obviously the highest-risk scenario for a foreign corporation, since countries can most easily enforce fines and penalties within their jurisdiction, extrajudicial or otherwise.[197] Even though *Yahoo* blunts the efficacy of foreign penalties, there remains one scenario where the enforceability of the Three Laws is an undecided issue. If a U.S. corporation operates outside the PRC, but in a country where the PRC has significant influence, the PRC could likely use its relationship with the third country to enforce its regulatory goals. Accordingly, understanding potential liability under the Three Laws requires an examination of the PRC's soft power and influence.

---

195. *See id.*

> Gradually, the experience of being online in China changed. The list of banned words and images grew. Articles and posts that managed to be published got removed quickly. The government got savvier, and more aggressive, about using its own technology: AI-powered censors could scan images to determine whether they contained certain sensitive words or phrases. An increasing number of foreign websites were block [sic] by the Great Firewall. Twitter has long been inaccessible, and so have the *Times* and the *Journal*. It is still possible to use VPNs and other circumvention tools to scale the Great Firewall, but it is getting increasingly dangerous to do so. Some people went to jail for selling VPNs, and others were fined for merely using them.

196. *See* de Fontbrune v. Wofsy, 838 F.3d 992, 1006 (9th Cir. 2016) (analyzing *Yahoo* and finding that four factors made the French order penal and therefore unenforceable: (i) the French term translates to "penalty," (ii) the sanctions were imposed due to the French treating the conduct as a "crime," (iii) *Yahoo* dealt with a public dispute, and (iv) the penalty was payable to the government).

197. *See infra* Part VIII.A.

C. Soft Power Controls How Regulations Are Enforced Against Foreign Entities

Soft power is defined as "the use of a country's cultural or economic influence to persuade other countries to do something, rather than the use of military power."[198] Alternatively phrased, soft power is a country's ability to rely on tactics other than force to achieve its objectives. Soft power is not just effective on other countries, but also the people and organizations that comprise those countries.[199] How the Three Laws impact the globe will be driven by the efficacy and strength of the PRC's soft power influence. Understanding the enforceability of the Three Laws requires an examination of how the enforceability of analogous EU data regulations relies on the EU's soft power. Next, EU and PRC soft power must be compared to determine their present relative strengths and weaknesses. Finally, an analysis of whether PRC soft power is growing or shrinking provides a framework for predicting whether the Three Laws can be effectively enforced globally against foreign companies.

1. EU Data Regulations Have Teeth Because of the EU's Soft Power

In 2016, the EU passed the GDPR which came into force in May 2018.[200] Some believe that the GDPR is "the toughest privacy and security law in the world."[201] GDPR's chief focus was

198. *Soft Power*, CAMBRIDGE DICTIONARY, https://perma.cc/D9GS-HG85.

199. *See* Steve Thomson, *Soft Power: Why It Matters to Governments, People, and Brands*, BRAND FINANCE (Feb. 25, 2022), https://perma.cc/6AKW-23U5 ("Soft power has a significant impact on the decisions people, businesses, and governments make.").

200. *See* Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 13, 2021), https://perma.cc/YPV7-86RH ("The European Union's General Data Protection Regulation (GDPR) was adopted in 2016 and officially launched in May 2018 to govern the use of personal data by both EU and non-EU companies who collect, process, and store the data of EU citizens.").

201. Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://perma.cc/DK4Y-E9P5.

on increasing privacy rights for individuals.[202] Applying to all types of businesses, GDPR fines violators up to the greater of €20 million or four percent of their global revenue.[203] Since coming into effect in 2018, 854 fines have been issued totaling €1,297,257,954.[204] Astronomical numbers aside, GDPR's effectiveness and enforceability are directly tied to the EU's soft power.[205]

The enforcement of EU law on actors outside Brussels' direct control is tied to EU political and economic influence—key components of soft power.[206] Government regulations can have an outsized global effect if the government has sufficient soft power to make noncompliance either fiscally, logistically, or legally unfeasible.[207] One of the key drivers of soft power is

202. *See* Sarah Gordon & Aliya Ram, *Information Wars: How Europe Became the World's Data Police*, FIN. TIMES (May 20, 2018), https://perma.cc/W8TC-JDWD ("GDPR will harmonise data protection rules across the world's largest trading bloc, give greater rights to individuals over how their data is used, put in place significant protections for children and streamline regulators' ability to crack down on breaches.").

203. *See* Ben Wolford, *What Are the GDPR Fines?*, GDPR.EU, https://perma.cc/M8EW-DSVH (explaining the possible fines for violation of the GDPR).

204. *See GDPR Fines Tracker & Statistics*, PRIV. AFFS., https://perma.cc/HRY9-CFM9 (providing a dashboard of GDPR fines, the violator, and the issuing country amongst other data).

205. *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 771 (2019) ("[T]he EU has become the world's privacy cop, acting in a unilateral fashion and exercising de facto influence over other nations through its market power.").

206. *See* Steven Blockmans, *Why Europe Should Harden Its Soft Power to Lawfare*, CTR. FOR EUR. POL'Y STUD. (June 15, 2020), https://perma.cc/3ZQZ-4VKJ ("The so-called Brussels effect—the impact of EU law on its neighbours and global corporations operating in the single market, has been waning for years. Nowadays its effect is mostly felt in anti-trust law, or in the chemicals directive or the General Data Protection Regulation.").

207. *See* Anu Bradford, *The Brussels Effect*, 107 NW. L. REV. 1, 5 (2012) ("The following conditions are necessary for a jurisdiction to dictate rules for global commerce: the jurisdiction must have a large domestic market, significant regulatory capacity, and the propensity to enforce strict rules over inelastic targets (e.g., consumer markets) as opposed to elastic targets (e.g., capital).").

economic might.[208] Global companies need to find and exploit any opportunity to grow their business.[209] A market rich in opportunities gives the government that controls said market increased leverage over companies that desire access.[210] Accordingly, the more powerful the economy, the more power a government has to influence foreign companies under the allure of market access. Simply stated, a country will be more effective in regulating foreign companies if said companies cannot forego access to that country's market. Therefore, companies must consider the PRC's soft power in relation to the soft power that allows the EU to enforce the GDPR.

2. Comparing EU and PRC Soft Power

The PRC views building soft power as a national priority.[211] The PRC toolkit for achieving this goal can be categorized into three general areas: culture promotion and educational exchanges; media, social media, and political messaging; and the soft power aspects of economic cooperation.[212] The last category is most applicable to determining how a sovereign's regulations affect private-sector firm decisions in a given jurisdiction.

---

208. *See id.* at 11–12.

209. *See* Jan-Emile van Rossum, *5 Benefits of International Expansion*, THE BUS. J. (Dec. 18, 2017, 3:15 AM), https://perma.cc/73P4-BF3D ("[I]nternational expansion offers a chance to conquer new territories and reach more . . . consumers, thus increasing sales.").

210. *See* George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3, 3 ("With its power to prohibit or compel, to take or give money, the state can and does selectively help or hurt a vast number of industries.").

211. *See* Eleanor Albert, *China's Big Bet on Soft Power*, COUNCIL ON FOREIGN RELS., https://perma.cc/H543-PCQ4 (last updated Feb. 9, 2018, 7:00 AM) (quoting Xi Jinping in 2014 as saying that "[w]e should increase China's soft power, give a good Chinese narrative, and better communicate China's message to the world").

212. *See* EUROPEAN THINK-TANK NETWORK ON CHINA, CHINA'S SOFT POWER IN EUROPE: FALLING ON HARD TIMES 7–10 (Ties Dams et al. eds., 2021).

The largest obstacle to the PRC's influence objectives is the country's declining international reputation.[213] While the EU "has a romantic and touristic appeal, a (struggling) sense of supranational unity, and its far-reaching foreign policy of assistance[,] it is legitimate to ask whether China's 'charm offensive' is losing momentum."[214] The largest driver of PRC global influence is its economic might and the corresponding secondary effects.[215]

China's economic might is roughly analogous to the EU's. According to the World Bank, the PRC and the EU are the two closest competitors to the United States in terms of largest gross domestic product (GDP).[216] Similarly, the Fortune Global 500 is dominated by companies headquartered in these three jurisdictions.[217] As two of the largest economies in the world, both the EU and the PRC have formidable global influence. This economic influence is most effective when used against other, poorer countries—best evidenced by the PRC's economic development efforts abroad through the Belt and Road Initiative.[218]

---

213. *See* Daniele Carminati, *The State of China's Soft Power in 2020*, E-INTERNATIONAL RELS. (July 3, 2020), https://perma.cc/Q6YK-R8PE ("China's culture still has limited appeal, its values mostly fail to reflect the country's image and reputation abroad, and its foreign policy is seen with skepticism at best—and as hegemonic at worst.").

214. *Id.*

215. *See id.* ("[I]t is fair to say that China's soft power heavily relies on its economic clout.").

216. *See GDP (current US$)—European Union, United States, China*, WORLD BANK, https://perma.cc/R8C3-S2SG (providing statistics on EU ($15.292 trillion), PRC ($14.273 trillion), and US ($20.894 trillion) GDPs as of 2020).

217. *See generally Global 500*, FORTUNE, https://perma.cc/F824-GRFJ.

218. *See* Shan Saeed, *For Developing World, Belt and Road Initiative Is Best Deal Around*, NIKKEI ASIA (May 6, 2020), https://perma.cc/Z2PN-G8HZ ("China has been willing to invest in projects that Western funders reject, giving developing nations a chance to implement their highest priority investments.").

3. The Belt and Road Initiative

Characterized by some as "China's Marshall Plan," the Belt and Road Initiative (BRI) seeks to grow China's influence in pursuit of its national priorities.[219] As of December 2021, over 145 countries have participated in the BRI since it began in 2013.[220] A participating country receives PRC direct investment or contracts with PRC-affiliated companies often financed by PRC-sourced loans.[221] A large focus of the BRI is building PRC influence in developing economies in Asia, Africa, South America, and the Middle East.[222] The focus on developing and impoverished countries allows PRC investment to enjoy an outsized economic and influential effect in recipient countries, but not without criticism of PRC gamesmanship.[223] Critics of the BRI characterize the true motivation behind the initiative as "[t]he developing world . . . helping [to] fix China's problems."[224] One of the most frequent criticisms is the accusation that BRI

219. *See* SIMON SHEN & WILSON CHAN, A COMPARATIVE STUDY OF THE BELT AND ROAD INITIATIVE AND THE MARSHALL PLAN 2 (2018) (finding "five core similarities in the background and purposes" of the Marshall Plan and BRI, "namely (1) boosting exports, (2) exporting currency, (3) countering a rival, (4) fostering strategic division, and (5) siphon[ing] away diplomatic support").

220. *See* Cristoph Nidopil, *Countries of the Belt and Road Initiative (BRI)*, GREEN FIN. & DEV. CTR., https://perma.cc/K63L-RQ6P.

221. *See id.* (summarizing 2021 BRI projects as comprising "about US$13.9 billion . . . through investment, and US$45.6 billion through contracts (partly financed by Chinese loans)").

222. *See* SHEN & CHAN, *supra* note 219, at 9 (commenting on the growing trend of "engagement to African and Arab countries, as well as more construction in South America" in addition to "Asian countries continu[ing] to receive the largest share of Chinese BRI investments (about 35% in 2021)").

223. *See* James T. Areddy, *Hidden Debt Plagues China's Belt and Road Infrastructure Plan, Studies Find*, WALL ST. J. (Sept. 28, 2021), https://perma.cc/7DM7-BXZR (reporting on findings that BRI projects subject recipient countries to hidden debt and the projects themselves are troubled by corruption, labor violations, and environmental risks).

224. *See id.* ("Beijing has . . . consistently pursued three goals: turning the enormous haul of dollars earned by the nation's exporters into foreign loans; keeping its massive domestic construction and industrial sectors busy by pursuing building projects abroad; and securing commodities like oil and grain to plug domestic shortfalls.").

projects create "debt traps" for recipient countries.[225] This indebtedness creates perverse incentives for recipient countries: BRI participants must either kowtow to the PRC or face onerous terms that may threaten the sovereignty of recipient country resources.[226] BRI infrastructure projects also create opportunities for exporting PRC technology.

A key component of BRI is known as the Digital Silk Road (DSR).[227] While debate surrounds the primary motives for the DSR, it has spread PRC technology—with its accompanying security and human rights concerns and risks—to BRI countries.[228] Regardless of potentially malicious motives, the DSR is the PRC's attempt to increase its digital influence at the expense of the U.S.[229] With technology developing at a torrential

---

225. *See id.* ("China has appeared reluctant to write off its loans to foreign countries, which on average carr[y] interest rates four times higher than offered by other bilateral lenders and maturity periods of a third as long.").

226. *See* Dylan Gertsel, *It's a (Debt) Trap! Managing China-IMF Cooperation Across the Belt and Road*, CTR. FOR STRATEGIC & INT'L STUD., https://perma.cc/859Y-3QZ9 ("The IMF has scrutinized multiple aspects of the BRI, repeatedly warning of unsustainable debt levels, predatory lending, and the lack of project transparency."). *But see* Jessica C. Liao, *How BRI Debt Puts China at Risk*, THE DIPLOMAT (Oct. 27, 2021), https://perma.cc/4DG8-FR66 ("Whether Beijing seeks to use debt as a tool to expand its influence and leverage over other countries remains under debate.").

227. *See* Robert Greene & Paul Triolo, *Will China Control the Global Internet Via Its Digital Silk Road?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 8, 2020), https://perma.cc/Q2DY-RJWH ("Beijing wants Chinese companies to participate in building many more pieces of financial, information, and telecommunications networks globally, with the goal of increasing China's overall capacity to participate in international technology standards setting and governance norm bodies.").

228. *See id.*

> Another misperception of the DSR is that it is a masterplan by Beijing to deploy its "techno-authoritarian" model to countries along the BRI. Certainly, Chinese companies export facial recognition technology and privacy-invasive cyber infrastructure that is used in emerging market countries—yet deployment of these technologies in emerging markets is very much a demand-driven phenomenon.

229. *See* Elles Houweling, *How Huawei's Power Play Fits into China's Digital Silk Road*, VERDICT (Aug. 6, 2021), https://perma.cc/Z63F-T4VP ("At its core, the DSR is a solution that engenders a less US-centric and more Sino-centric global digital order.").

pace and touching more aspects of everyone's lives, this digital influence clearly expands the PRC's influence around the world.

The PRC has expanded its influence, both digital and economic, to hundreds of countries. The DSR component of the BRI and the nature of PRC "private-sector" companies have provoked suspicions and criticisms that these projects will allow the PRC to achieve its international objectives through underhanded means.[230] Nevertheless, the PRC already exerts tremendous influence, and predictions about its future growth or decline are useless to companies attempting to determine how to navigate the Three Laws now. Failing to do so will leave companies at the whim of the PRC's efforts to achieve its global objectives through "lawfare."

The PRC wholeheartedly embraces "lawfare" as a tactic for achieving its international goals.[231] Lawfare is "the use of law as a means of accomplishing what might otherwise require the application of traditional military force."[232] The Three Laws and their extraterritorial provisions are a powerful weapon in the PRC's growing lawfare arsenal. Combining the influence curried via BRI and the lawfare philosophy, the PRC will expand its influence even further. While companies used to only need worry about CCP laws while they were inside the PRC, the

230. *See* Lindsay Maizland & Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, COUNCIL ON FOREIGN RELS., https://perma.cc/5GPV-YXT2 (last updated Aug. 6, 2020, 8:00 AM) (providing a detailed overview of the security concerns revolving around China's flagship information technology company being used to "spy, sabotage, or take other actions on the [PRC government's] behalf").

231. *See* Bradley A. Thayer & Lianchao Han, *The Growing Threat of China's Lawfare*, THE HILL (Apr. 9, 2021), https://perma.cc/J8PL-J47F ("In practice, Xi increasingly uses law as a weapon to crack down on dissent to ensure regime security, while simultaneously employing it as a weapon in the CCP's quest for world hegemony."); Jonas Parello-Plesner, *With Denmark, China Tests the Reach of Its Lawfare into Democracies*, GERMAN MARSHALL FUND (2022), https://perma.cc/Q2FS-UMUV ("Today, the [CCP] is extending its long authoritarian arm and misusing legal principles, so-called lawfare, far beyond its borders and into democracies around the world.").

232. Charles J. Dunlap Jr., *Lawfare 101: A Primer*, 97 MIL. REV. 8, 9 (2017) ("[Lawfare] is something of an example of what Chinese strategist Sun Tzu might say is the 'supreme excellence' of war, which aims to subdue 'the enemy's resistance without fighting.'").

advancement of BRI, lawfare, and the PRC's overall global influence compels organizations to analyze their regulatory risk through a worldwide, geopolitical framework.

VIII. RECOMMENDATIONS

As described above, non-PRC companies must gauge their regulatory risk under the Three Laws based upon a holistic understanding of PRC objectives and interpretations of past regulatory actions.[233] Navigating the onerous requirements of the Three Laws and their ambiguity is an uphill battle.[234] From a data perspective, companies may gauge their risk by reviewing the types of PRC citizen data they collect, store, and process. Once companies analyze their risk from a data perspective, they must then analyze their operations in light of geography, influence, and prevailing international power dynamics. Companies would be well-advised to conduct this analysis through the lens of three different categories: operations within the PRC and behind the Great Firewall; operations with zero presence behind the Great Firewall; and operations in countries with significant PRC influence.

A. Companies Behind the Firewall

Companies operating within the PRC face the highest regulatory compliance requirements and risk.[235] As Ant Group,[236] Didi,[237] Tesla,[238] and Apple[239] demonstrate, the lure of

233. *See supra* Parts II–VII.

234. *See* Elizabeth Cole et al., *China Finalizes Data Security Law to Strengthen Regulation on Data Protection*, JONES DAY (June 2021), https://perma.cc/G4RL-8V2B ("The exact scope of these data categories are intentionally broad and vague to allow for flexible interpretation. This will add an additional level of uncertainty for businesses."); *see also supra* Part I.

235. *See* Monopoly (Hasbro, English ed. 2020) ("Do not pass Go; Do not collect $200.").

236. *See supra* Part III.

237. *See supra* Part IV.A.

238. *See supra* Part IV.B.

239. *See supra* Part V.B.

success in one of the world's most lucrative markets carries with it the probability of sudden, unwanted CCP attention and crackdowns. Companies operating inside the PRC must work assiduously to stay informed of regulatory developments and maintain compliance.[240] The carrot of more than a billion consumers inside the PRC allows the CCP to wield a big stick—the Three Laws' requirements and potential punishments. Companies operating in the PRC must evaluate the costs of compliance with the Three Laws and soberly consider the benefits. Optimism is foolish.[241] Companies with established revenue streams in the PRC, like Apple and Tesla, cannot rely on their prior success as a shield against future shifts in PRC actions.[242] Continued good luck does not good risk management make. Even the world's largest companies must still operate with both eyes open if they are within the PRC's borders. However, remaining outside the PRC does not negate the risk presented by the Three Laws.

B. Companies with No Presence in the PRC

Companies operating in jurisdictions completely removed from the PRC are relatively safe from the barriers and risks of the Three Laws, but technology companies reliant on data easily scale internationally and will thus likely not be confined to just one jurisdiction.[243] However, a majority of the world's largest

240. *See* CHINA'S CYBERSECURITY LAW, *supra* note 11 ("Companies operating in China should take swift actions now to assess their specific obligations under the CSL and other related regulations and adopt a comprehensive approach to mitigate the compliance risks.").

241. *See* Steve Saleen, *How Chinese Officials Hijacked My Company*, WALL ST. J. (July 31, 2020, 6:13 PM), https://perma.cc/DCZ7-PQRM ("The deal was a sham. It was a trap designed to secure my intellectual property, then use intimidation tactics and lies to nullify the agreement and seize control.").

242. *See* Barrett, *supra* note 104 ("Tesla's experience is 'a warning shot that they need to stay between the lines, and not be so flamboyant in their success . . . . You can't be so far up front that you become arrogant in the way you conduct yourself.'").

243. *See* Jim Molis, *Critical Considerations for Tech Companies Seeking to Grow Internationally*, THE BUS. J. (Jan. 31, 2020), https://perma.cc/XKL9-WAYQ ("Tech startups can reach international markets quickly because the world is increasingly connected.").

technology companies are headquartered in the United States.[244] Hypothetically, a U.S. company with an international presence—but not one in the PRC—would likely be shielded from the United States enforcing a PRC extraterritorial penalty against them.[245]

Recognition of PRC judgments by U.S. courts is an unsettled issue, the resolution of which may depend on whether the PRC judicial system ultimately values due process.[246] The number of U.S. courts recognizing a PRC judgment can be counted on one hand.[247] Further, as *Yahoo* demonstrates, U.S. courts will not enforce foreign fines and penalties on the foreign nation's behalf.[248] However, the Three Laws—and their international relations implications—introduce complex issues far beyond a business deal gone bad. A Three Laws fine on a U.S. company would introduce diplomatic and political considerations that would dramatically affect the likelihood that a company would have to pay an assessed penalty.

---

244. *See generally* THOMSON REUTERS, THE TOP 100 GLOBAL TECHNOLOGY LEADERS (2018), https://perma.cc/2BAP-LR39 (PDF).

245. *See supra* Part VII.B.

246. *See* Mark Moedritzer et al., *Judgments 'Made in China' But Enforceable in the United States?: Obtaining Recognition and Enforcement in the United States of Monetary Judgments Entered in China Against U.S. Companies Doing Business Abroad*, 44 INT'L LAW. 817, 835 (2010)

> [C]ases specifically addressing recognition of foreign judgments entered in China are still relatively few. Based on developments in the legal system in the People's Republic of China over the past two decades, it is increasingly likely that a U.S. court evaluating whether to recognize a judgment entered in China would conclude that the system of justice in China comports with traditional Western notions of due process, and thus that element would likely not be a bar to recognition in a U.S. court.

247. *See* Meng Yu, *U.S. Court Recognizes a Chinese Judgment for the Third Time*, CHINA JUST. OBSERVER (Feb. 4, 2020), https://perma.cc/YHV4-S2B5 ("It marks the third time for [a] U.S. court to recognize a Chinese judgment. Prior to this, two Chinese judgments were recognized respectively in the U.S. in 2009, and in 2016 [sic].").

248. *See supra* Part VII.B.

"During the past several years, the U.S.-China relationship has reached its lowest point in decades."[249] American recognition of a Three Laws fine against a U.S. company would signal either U.S. parity with or submission to the PRC.[250] The PRC would likely tout any such recognition as a significant victory in its quest to be considered the supreme world power.[251] Thus, the U.S. political and diplomatic establishment would likely do whatever possible to protect a U.S. company and avoid allowing the PRC to achieve such a significant international accomplishment. Additionally, companies like Alphabet, which still maintains a presence in the PRC despite having its services blocked by the Great Firewall, could be a prime target for the PRC.[252] Enforcing the Three Laws against a U.S. company would be a valuable tactic for achieving PRC international objectives and prompts an interesting, unsettled question. What if a PRC citizen in the United States registers for a U.S. company's services that ostensibly violate the Three Laws?

---

249. Isaac Chotiner, *The Fraying of U.S.-China Relations*, THE NEW YORKER (Nov. 20, 2021), https://perma.cc/NX8J-WSLN; *see also* Owen Churchill, *China–US Relations: Blinken Says Beijing is Bringing More Aggression to Competitive and Cooperative Ties*, S. CHINA MORNING POST (Jan. 25, 2022, 2:00 PM), https://perma.cc/X7VR-PERJ ("The US-China relationship is becoming increasingly adversarial, according to US Secretary of State Antony Blinken who on Monday criticized the Chinese government for being 'more assertive and aggressive' than in previous decades.").

250. *See* Ryan Hass, *How China Is Responding to Escalating Strategic Competition with the US*, BROOKINGS (Mar. 1, 2021), https://perma.cc/4E28-29AH ("To [achieve their national goals], China appears to be pursuing a three-pronged medium-term strategy: maintaining a non-hostile external environment in order to focus on domestic priorities; reducing dependence on America while increasing the rest of the world's dependence on China; and expanding the reach of Chinese influence overseas.").

251. *See* Chotiner, *supra* note 249 ("Xi Jinping is now stating that China's political system is demonstratively superior to Western democracies in its ability to deliver practical governance outcomes, and so the narrative is, 'Our system is better than yours, and Western democracy is a path to infighting, polarization, and institutional atrophy.'").

252. *See* William Yuen Yee, *Google Parent Company Alphabet Is Back in China (Because It Never Left)*, SUPCHINA (June 18, 2020), https://perma.cc/T62Y-YH6W ("While widely credited with 'having left China,' Google still operates a significant in-country presence and through its parent company, Alphabet, continues to launch new projects in China and invest into Chinese companies of all sizes.").

Before COVID-19 countermeasures blocked free travel, millions of PRC citizens escaped the confines of the Great Firewall and visited the United States.[253] These PRC tourists could enroll in services or purchase products that collect "sensitive personal information" or any of the gamut of classified datatypes that trigger Three Laws liability.[254] This vector of enforcement could present an opportunity for the PRC to achieve its desired strategic international achievement.[255] Companies should be aware that, given the vague and ambiguous statutory text, the Three Laws could be invoked by the innocuous action of a PRC citizen registering for an account or a company marketing its services to PRC citizens outside the PRC.[256] Methods for dealing with this possibility could present difficult U.S. constitutional questions of a company discriminating against customers based upon their national origin.[257] Disallowing PRC citizens from participating in data-collection products may seem like a simple solution to avoid Three Laws liability, but as with any complicated issue, solutions often create more problems. If the PRC desires to enforce the Three Laws extraterritorially but cannot achieve this strategic international objective in the United States, the

253. Agne Blazyte, *Number of Tourist Arrivals in the United States from China from 2005 to 2020*, STATISTA (Feb. 8, 2022), https://perma.cc/BN6D-YTPJ.

254. *See supra* Part I.

255. *See supra* notes 249–251 and accompanying text.

256. *See* McKenzie, *supra* note 22 ("It remains uncertain, for example, whether an online company based outside China will become subject to the PIPL merely because it allows a Chinese resident to register an account or when its services are actively marketed to Chinese residents.").

257. *See* Civil Rights Act of 1964, 42 U.S.C. § 2000d ("No person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance."); *see also* Press Release, Ctr. for Am. Progress, Tech Companies Supported by the Federal Government Should Share Profits With Workers, New CAP Proposal Says (Apr. 19, 2018) ("The federal government has been a major funder of research to advance innovation and technical understanding for approximately 80 years. The tech industry is heavily supported by Washington . . . .").

PRC could potentially seek other jurisdictions more amenable to assisting the PRC in its global ambitions—the vassals of its BRI.

C. Companies Operating in BRI Countries

Enforcement of the Three Laws against a U.S. company that operates in a BRI vassal country could cause a cataclysmic shift in international relations and law. For the company, a Three Laws enforcement could significantly influence the business decision to remain in the BRI vassal nation. Technology has had a positive effect on individual freedoms and rights in countries throwing off the yoke of dictatorship, arguably further motivating the CCP's cyber sovereignty policy in pursuit of avoiding similar results in the PRC.[258] A U.S. technology company abandoning a BRI vassal market could have a deleterious effect on the individual rights of the BRI vassal's citizens. Further, the withdrawal of a U.S. company could damage diplomatic relations between the United States, the BRI vassal state, and the PRC.[259] No matter what, enforcement of the Three Laws in BRI vassal states would provide a victory for the PRC on multiple fronts—raising international estimations of PRC power, lessening U.S. hegemony, and providing an economic demand vacuum that the PRC could fill with any of its similar companies. Unfortunately, the scope of this potential problem is beyond the ability of any

258. *See* Catherine O'Donnell, *New Study Quantifies Use of Social Media in Arab Spring*, UNIV. OF WASH. (Sept. 12, 2011), https://perma.cc/8G6H-XWAH ("[S]ocial media played a central role in shaping political debates in the Arab Spring. Conversations about revolution often preceded major events, and social media has carried inspiring stories of protest across international borders."). *But see* Haythem Guesmi, *The Social Media Myth About the Arab Spring*, AL JAZEERA (Jan. 27, 2021), https://perma.cc/LUG5-9PJ7 ("Social media networks did not trigger the Arab revolutions, but they did contribute to the counter-revolutions.").

259. *See* THOMAS L. FRIEDMAN, THE LEXUS AND THE OLIVE TREE 195 (1999) ("No two countries that both had McDonald's had fought a war against each other since each got its McDonald's."). *But see* Paul Musgrave, *The Beautiful, Dumb Dream of McDonald's Peace Theory*, FOREIGN POL'Y (Nov. 26, 2020, 3:58 PM), https://perma.cc/7VQ2-R6NJ (refuting Friedman's capitalist peace hypothesis in favor of a theory that "market development diminishes prospects of war between two countries but doesn't rule it out").

single company to manage. Governments and diplomacy are the most effective tools to insulate private-sector companies from the whims of global powers.[260] Unfortunately, the United States may lack legitimacy in the digital privacy arena due to its data collection practices.[261] The EU could build upon the philosophy that led to its enactment of the GDPR by leading the push to a diplomatic resolution of the problems created when geopolitics, technology, and lawfare collide. Regardless, the Three Laws represent one of the strongest indicators that the world may shift beneath our feet in the near future as global powers wage their disputes in an unprecedented manner.

The prospect of the PRC enforcing the Three Laws as a lawfare tactic raises serious questions about how international law currently treats lawfare and extraterritorial provisions in domestic laws. The PRC's preferred lawfare tactics should prompt a reevaluation of the international community's standards for recognizing foreign judgments, fines, and enforcement penalties. Permitting nations to reach across their borders and exert their own laws in other countries in which they have influence should be drastically limited. Were the PRC unable to enforce the Three Laws against a U.S. company in either the PRC (because the U.S. company has no presence in the PRC) or because the U.S. company is completely removed from the curtain of the Great Firewall, current international law

260. *See* Justin Sherman, *U.S. Diplomacy Is a Necessary Part of Countering China's Digital Authoritarianism*, LAWFARE (Mar. 17, 2020, 1:18 PM), https://perma.cc/JH3R-BDUN ("Digital diplomacy is important for trade; it's important for national security; and it's important for collaborating with other liberal democracies to establish and reinforce clear, democratic regulations and behavior around artificial intelligence and emerging surveillance issues.").

261. *See* Justin Sink & John Harney, *CIA Secretly Collected 'Bulk' Data on American Citizens, Senators Say*, BLOOMBERG (Feb. 11, 2022, 12:31 AM), https://perma.cc/Z54L-WARS (last updated Feb. 11, 2022, 7:13 AM) (reporting that the U.S. intelligence community collected hundreds of millions of American citizen's data); Jose Luis Magana, *Senator Calls for Review of U.S. Intelligence Gathering as Outcry Grows from Germany, Other Nations*, ASSOCIATED PRESS (Oct. 29, 2013, 1:40 AM), https://perma.cc/6NQ8-PU3Z (last updated Jan. 12, 2019, 5:40 AM) ("The NSA's program of spying on . . . foreign leaders was already damaging relations with some of the closest U.S. allies.").

structures encourage a type of forum shopping. By deciding a penalty and then seeking a forum that would enforce it, the PRC would wage its lawfare strategy on the battlefields of developing countries. While America's international reputation is battered, especially when it comes to individual privacy rights, the international community should recognize the problematic precedent that foreign enforcement of the Three Laws would present. Limiting the reach of powerful nations with audacious regulations should be a priority, if only to confine diplomacy and global power struggles to their traditional venues. Otherwise, much like war is now carried out in cyberspace, international squabbles will be conducted on new, uncertain battlefields. While many like to think of courtrooms as gladiatorial arenas, the fate of billions should not hang in the balance as one judge sits alone in whatever country a more powerful nation chooses.

CONCLUSION

The Three Laws are a calculated tool for the CCP to achieve its domestic and international objectives.[262] These laws allow the CCP to seek any geopolitical advantage at the expense of their rivals by using data's power to influence and shape people and events.[263] The Three Laws are the first phase of the CCP's evolving attempt to use data regulation to further its information warfare strategy. Considering their recent enactment, however, the global impact of the Three Laws is yet to be determined. But companies and governments must think and plan steps ahead to counter the Three Laws' potentially calamitous consequences. Understanding the CCP's motivations, strategies, and tools for controlling data helps one comprehend not just issues in cyberspace, but also the current tension in the business and geopolitical realms swirling around the PRC. Every battle is won before it is fought.[264]

---

262. *See supra* Part II.

263. *See supra* Part VI.

264. *See* Sun Tzu, *The Art of War*, *in* THE SEVEN MILITARY CLASSICS OF ANCIENT CHINA 157, 162 (Ralph D. Sawyer & Mei-Chün Sawyer trans., 1993) ("One who, fully prepared, awaits the unprepared will be victorious.").