Notes

An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts

Debevoise & Plimpton LLP Student Writing Prize in Comparative and International Law, Best Note

China's 2017 Cybersecurity Law (CSL), one of the first comprehensive cybersecurity laws by a major power, drew attention for its ambitious, all-encompassing approach to managing cybersecurity from the top down. The CSL also reflected China's efforts to respond to its citizens' demands for consumer protections, data privacy, and data security. However, when the CSL was implemented, ambiguity surrounded its interpretation and enforcement. This is the first detailed study of the Chinese judicial system's treatment of the CSL to date—by examining a sample of administrative, criminal, and civil cases, this Note showcases the on-the-ground realities of the CSL's implementation. These cases reveal that strengthened legal protections for consumers may come at the cost of eliminating anonymity. The CSL has increased the State's ability to monitor the citizenry and enforce the State's restrictive vision of "cybersecurity," with impacts on both individuals and businesses. Most significantly, the State is using the CSL to target politically sensitive and anti-government speech. This trend is particularly worrying as China's role as an exporter of technology and cyber policy continues to grow.

INTRODUCTION

In terms of sheer volume of internet users and its technical capabilities and aspirations, China's presence as a global cyber power cannot be ignored.[1] As of December 2020, China had 989 million internet users,[2] representing approximately 20% of the global total.[3] As recently as 2018, China failed to break the top ten in global studies assessing the world's cyber powers.[4] Cyber power, while defined differently by each of the studies, generally refers to a country's ability to defend itself from cyberattacks and the strength of its offensive cyber capabilities.[5] By 2020, however, China was recognized as second only to the United States ("U.S.") in cyber capabilities and "cyber intent."[6] While variations in methodology explain some differences in the indices,[7] the jump in ranking also reflects China's increased

1. Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 58 (2018). Throughout this Note, references to "China" or "Chinese" are references to the People's Republic of China, or PRC, and not to the broader cultural, ethnic, and linguistic group represented by Chinese people around the world.

2. Evelyn Cheng, *China Says It Now Has Nearly 1 Billion Internet Users*, CNBC (Feb. 4, 2021, 2:40 AM), https://www.cnbc.com/2021/02/04/china-says-it-now-has-nearly-1-billion-internet-users.html [https://perma.cc/68HU-NBFN].

3. Jacob Davidson, *Here's How Many Internet Users There Are (in 2020)*, MONEY (May 19, 2020, 1:48 PM), https://money.com/internet-users-worldwide [https://perma.cc/2WDZ-3ZQZ].

4. BOOZ ALLEN HAMILTON, CYBER POWER INDEX: FINDINGS AND METHODOLOGY 4–6 (2011) (ranking China 13th among the G20 in a report evaluating each country's "Legal and Regulatory Environment," "Economic and Social Context," "Technology Infrastructure," and "Industry Application"); INT'L TELECOMMS. UNION, GLOBAL CYBERSECURITY INDEX 2018, at 7–8, 58 (2018), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [https://perma.cc/67XM-VXXT] (ranking China 27th globally in an index measuring the legal, technical, organization, capacity building, and cooperation aspects of cybersecurity).

5. BOOZ ALLEN HAMILTON, *supra* note 4, at 2; JULIA VOO ET AL., NATIONAL CYBER POWER INDEX 2020 1–3 (2020), https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf [https://perma.cc/U4D6-SYWZ].

6. VOO ET AL., *supra* note 5, at 8–10. This study by the Harvard Kennedy School's Belfer Center for Science and International Affairs examined a country's stated objectives in cyberspace, its ability to pursue those objectives, and the overall number of objectives the country is pursuing. "Cyber intent" assesses "[e]ach country's track record in perpetrating cyber attacks," its "cyber military strategies to date," and its "participation in international cooperation agreements on cyberspace." *Id.*

7. *Id.* at 6–7 (noting the 2011 Booz Allen Hamilton report only focused on digital infrastructure, while the 2018 International Telecommunication Union's Global Cybersecurity Index focused on "domestic cyber resilience" and "d[id] not take into account offensive cyber capabilities").

investment in technology that has strengthened its technical capabilities and showcased its global ambitions.[8]

In furtherance of these global ambitions, the Chinese government has sought to establish a comprehensive legal framework for managing cyberspace.[9] Consistent with Xi Jinping's emphasis on the "rule of law,"[10] China has enacted national legislation, beginning with the National Security Law in 2015[11] and the Counter-Terrorism Law in 2016.[12] With the passage of the Cybersecurity Law ("CSL") (网络安全法) in 2017, China revealed 'its vision of cybersecurity,[13] which is a broad term generally referring to "technologies, processes, and practices designed to protect networks . . . from attack, damage, or unauthorized access."[14] Since the CSL came into effect, a constant stream of implementing regulations and guidelines have added detail to China's cybersecurity regime.[15] Additional laws released since the CSL include the Data Security Law[16] and the Personal Information

8. *Id.* at 40.

9. Samm Sacks, *China's Emerging Cyber Governance System*, CSIS, https://www.csis.org/chinas-emerging-cyber-governance-system [https://perma.cc/36LP-H8GP] .

10. 2 XI JINPING, *Promote Socialist Rule of Law*, *in* THE GOVERNANCE OF CHINA 119, 119 (2017); JAMIE P. HORSLEY, PARTY LEADERSHIP AND RULE OF LAW IN THE XI JINPING ERA 1 (2019), https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_legal_development_horsley.pdf [https://perma.cc/9EUZ-VME8].

11. *China Passes Tough New Intelligence Law*, REUTERS (June 28, 2017, 8:06 AM), https://www.reuters.com/article/us-china-security-lawmaking-idUSKBN19I1FW [https://perma.cc/96G9-9A3P].

12. Zunyou Zhou, *China's Comprehensive Counter-Terrorism Law*, THE DIPLOMAT (Jan. 23, 2016), https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/ [https://perma.cc/BKM7-7URM].

13. Sacks, *supra* note 9; *Cybersecurity Law: Reactions and Recent Enforcement*, CHINA DIGIT. TIMES (June 20, 2017), https://chinadigitaltimes.net/2017/06/chinas-new-cybersecurity-law-reactions-recent-enforcement/ [https://perma.cc/83XK-V83N].

14. Juliana De Groot, *What is Cyber Security? Definition, Best Practices & More*, DIGITAL GUARDIAN: DATA INSIDER (Oct. 5, 2020), https://digitalguardian.com/blog/what-cyber-security [https://perma.cc/7GNF-UCBD].

15. For examples of implementing regulations, see SAMM SACKS & MANYI KATHY LI, HOW CHINESE CYBERSECURITY STANDARDS IMPACT DOING BUSINESS IN CHINA (2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf [https://perma.cc/F5PQ-LYYX].

16. Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [PRC Data Security Law] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), *translated in* TRANSLATION: DATA SECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA, STANFORD DIGICHINA CYBER POLICY CENTER (June 29, 2021), https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china [https://perma.cc/A6E9-AN5J] [hereinafter Data Security Law].

Protection Law, both passed in 2021.[17] These two laws have expanded China's rules for the internet, with the Personal Information Protection Law resembling the EU's General Data Protection Regulation ("GDPR").[18]

As its domestic capabilities have grown, China's influence on global cybersecurity capabilities and policies has also become more prominent.[19] One example of this trend is China's Digital Silk Road, an extension of 'its Belt and Road Initiative, which invests in internet and communication technology (ICT) projects around the globe.[20] These investments have coincided with ever-increasing global demand for digital infrastructure.[21] China has contributed an estimated $79 billion U.S. dollars ("USD") to digital infrastructure globally, boosting Chinese companies' footprint and extending China's influence.[22] A

17. Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [PRC Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml [https://perma.cc/AD2Z-ZSGD] [hereinafter Personal Information Protection Law].

18. Natasha Lomas, *China Passes Data Protection Law*, TECH CRUNCH (Aug. 20, 2021, 6:35 AM), https://techcrunch.com/2021/08/20/china-passes-data-protection-law [https://perma.cc/8J48-38WG].

19. INT'L INST. FOR STRATEGIC STUD., *China's Cyber Power in a New Era*, *in* ASIA PACIFIC REGIONAL SECURITY ASSESSMENT 2019, at 77–90 (May 2019); JONATHAN WOETZEL ET AL., CHINA'S DIGITAL ECONOMY: A LEADING GLOBAL FORCE 1 (2017), https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/China/Chinas%20digital%20economy%20A%20leading%20global%20force/MGI-Chinas-digital-economy-A-leading-global-force.pdf [https://perma.cc/L8F7-VC8U].

20. Clayton Cheney, *China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism*, COUNCIL ON FOREIGN REL. (Sept. 26, 2019, 8:00 AM), https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political [https://perma.cc/2Z6C-8DLW].

21. Int'l Inst. for Strategic Stud., *supra* note 19; Jude Blanchette & Jonathan E. Hillman, *China's Digital Silk Road After the Coronavirus*, CSIS (Apr. 13, 2020), https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus [https://perma.cc/A9UF-Y5ER] (predicting that demand for digital infrastructure projects will continue to increase post-pandemic as they are less risky and "easier to monetize"); Joshua Kurlantzick, *Assessing China's Digital Silk Road: A Transformative Approach to Technology Financing or a Danger to Freedoms?*, COUNCIL ON FOREIGN REL. (Dec. 18, 2020, 10:38 AM), https://www.cfr.org/blog/assessing-chinas-digital-silk-road-transformative-approach-technology-financing-or-danger [https://perma.cc/HJP5-973N] (estimating that as many as one-third of the countries participating in the Belt and Road initiative are working with China on Digital Silk Road projects).

22. Sheridan Prasso, *China's Digital Silk Road Is Looking More Like an Iron Curtain*, BLOOMBERG (Jan. 10, 2019, 12:01 AM), https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain [https://perma.cc/84ND-L5W6]; Eileen Yu, *Alibaba Rolls Out First Overseas Smart City AI Platform in Malaysia*, ZDNET (Jan. 29, 2018, 6:33 PM), https://www.zdnet.com/article/alibaba-rolls-out-first-

similar expansion of Chinese influence has occurred in the area of cybersecurity law,[23] where national governments are frequently learning from and copying one another.[24] Countries as diverse as Vietnam,[25] Uganda, and Tanzania[26] have already adopted cybersecurity laws with provisions that mirror the CSL, suggesting that other countries within China's influence are willing to replicate its approach to cybersecurity.[27]

When the CSL first came into effect, multiple countries and global technology companies protested that the CSL represented an illegitimate attempt to protect domestic technology and force intellectual property (IP) transfer.[28] Some argued that the law threatened U.S. national security by increasing the Chinese government's access to information.[29] Scholars highlighted the vagueness of the CSL's provisions, noting that key terms such as "critical information infrastructure" and "network operator" were not clearly defined—the lack of definition thus left the Chinese government broad discretion to interpret the law.[30]

---

overseas-smart-city-ai-platform-in-malaysia/ [https://perma.cc/M3DT-CJQL]; Joshua Kurlantzick, *China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom?*, THE DIPLOMAT (Dec. 17, 2020), https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/ [https://perma.cc/S73J-ZD2Z] (noting that China's Digital Silk Road investments have extended from Ecuador to Egypt to Zambia).

23. Int'l Inst. for Strategic Stud., *supra* note 19.

24. *Policy Recommendations: Freedom on the Net 2020*, FREEDOM HOUSE, https://freedomhouse.org/report/report-sub-page/2020/policy-recommendations-freedom-net-2020 [https://perma.cc/77UR-R97B].

25. Thoi Nguyen, *Vietnam's Controversial Cybersecurity Law Spells Tough Times for Activists*, THE DIPLOMAT (Jan. 24, 2019), https://thediplomat.com/2019/01/vietnams-controversial-cybersecurity-law-spells-tough-times-for-activists [https://perma.cc/A8AF-Y2EC] (identifying the law's similarity to the CSL).

26. Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, THE ATLANTIC (June 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/ [https://perma.cc/CMN5-ER44].

27. Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism [https://perma.cc/P9BH-4G5P] (last visited Feb. 27, 2020).

28. Communication from the United States, *Measures Adopted and Under Development by China Relating to Its Cybersecurity Law*, WTO Doc. S/C/W/374 (Sept. 25, 2017).

29. Brandon W. Jackson, *Economics, Innovation, and the Art of a Long View: A Deep-Dive on the National Security Implications of China's 2016 Cybersecurity Law*, 10 NAT'L SEC. L. BRIEF 93, 156–57 (2020).

30. Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect [https://perma.cc/BS69-NKYM].

Despite extensive commentary on the potential impacts of the CSL, there has not yet been a comprehensive examination of the citation and use of the CSL and related regulations in the Chinese judicial system. As research on the ground in China becomes more difficult due to travel and access restrictions,[31] Chinese court decisions placed online are an increasingly valuable source of insight into the domestic application of Chinese law.[32] The discussion in this Note may be particularly valuable as several of the cases discussed on this Note are now "missing" on the official China Judgements Online site.[33]

This Note examines the citation and application of the 2017 CSL and subsequent implementing regulations in the Chinese judicial system. First, it introduces key actors within China's cybersecurity regime and notable provisions of the CSL. Second, it outlines available cases citing to the CSL and examines Chinese courts' interpretations of the CSL. Third, it argues that the domestic application and interpretation of the CSL demonstrate China's emerging vision for cybersecurity—one with robust rights for citizens in the economic sphere, but with sophisticated levels of state control regarding political speech. Analysis to date of the CSL has focused on its impact on foreign businesses, with familiar claims of protectionism and fears surrounding IP theft.[34] Insights from the domestic application of the law provide a more complete picture of China's vision for cybersecurity, with significant global implications.

I. THE CYBERSECURITY LAW AND CHINA'S CYBERSECURITY REGIME

A. China's Cybersecurity Administration and the Judicial System

1. The Preeminence of the CCP and the Judicial Structure

The Chinese Communist Party (CCP) maintains *de facto* leadership over all aspects of China's executive, legislative, and judicial

31. During the COVID-19 pandemic, China imposed some of the world's strictest entry restrictions for non-citizens. *See* Sui-Lee Wee & Keith Bradsher, *Think Covid's Messed Up Your Travel Plans? Try Getting into China*, N.Y. TIMES (Mar. 21, 2021), https://www.nytimes.com/2021/03/21/business/international/china-coronavirus-borders.html [https://perma.cc/X2RF-X6YG].

32. Benjamin L. Liebman et al., *Mass Digitization of Chinese Court Decisions: How to Use Text as Data in the Field of Chinese Law*, 8 J.L. & CTS. 177, 178 (2020).

33. *See generally* China Judgements Online, https://wenshu.court.gov.cn/website/wenshu/181029CR4M5A62CH/index.html [https://perma.cc/W4VM-58ZG].

34. *See, e.g.*, Lee, *supra* note 1, at 60–61.

systems.[35] On paper, the Chinese State government operates independently of the CCP and there are few formal linkages between the CCP and the State. In reality, the CCP and State government operate in a dual system where the CCP retains control through informal mechanisms, such as CCP policy directives and appointments,[36] and formal mechanisms, such as the Cyberspace Administration of China.[37]

The State government, led by the National People's Congress (NPC), handles day-to-day policy implementation, which includes formally passing legislation.[38] The State government also includes the State Council, a cabinet-like body, and People's governments at every level.[39]

The judicial system formally falls within the State structure.[40] The hierarchical court system begins with the People's Courts at the local level, then Intermediate People's Courts, High People's Courts, and, at the top, the Supreme People's Court.[41] The courts work closely with the public security bureaus, or police, as well as the procuratorates,[42] which conduct criminal prosecutions and investigations on behalf of the State.[43] Together, the courts, the public security bureaus,

35. Jianfu Chen, *Out of the Shadows and Back to the Future: CPC and Law in China*, 24 ASIA PACIFIC L. REV. 176, 178 (2016); SUSAN V. LAWRENCE & MICHAEL F. MARTIN, CONG. RSCH. SERV., R41007, UNDERSTANDING CHINA'S POLITICAL SYSTEM 2 (2013).

36. Chen, *supra* note 35, at 194; HORSLEY, *supra* note 10, at 1, 5–6. For examples of the CCP's directives, see, for example, SCOTT LIVINGSTON, THE CHINESE COMMUNIST PARTY TARGETS THE PRIVATE SECTOR 1 (2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201008_Livingston_CCP%20Targets%20Private%20Sector_WEB%20FINAL.pdf [https://perma.cc/KX8U-B5UZ].

37. *See* discussion *infra* Section I.A.1.

38. LAWRENCE & MARTIN, *supra* note 35, at 28.

39. *Id.* at 4, 9.

40. The Supreme People's Court, the highest court, reports to the National People's Congress. *Id.* at 4.

41. YIFAN WANG, SARAH BIDDULPH & ANDREW GODWIN, A BRIEF INTRODUCTION TO THE CHINESE JUDICIAL SYSTEM AND COURT HIERARCHY 7 (2017), https://law.unimelb.edu.au/__data/assets/pdf_file/0004/2380684/ALC-Briefing-Paper-6-Wang,-Biddulph,-Godwin_5.pdf [https://perma.cc/4M95-WEYC].

42. The procuratorates generally act as prosecutors, but their role also expands beyond the traditional purview of a prosecutor in the U.S. legal system. *See id.* at 26.

43. Zhonghua Renmin Gongheguo Renmin Jianchayuan Zuzhi Fa (中华人民共和国人民检察院组织法) [Organic Law of the People's Procuratorate of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 26, 2018, effective Jan. 1, 2019) arts. 20, 26, http://www.npc.gov.cn/npc/c12435/201810/b59a94f891794d9980e950c5cd8a0204.shtml, *translated in Organic Law of the People's Procuratorate of the PRC (2018)*, CHINA LAW TRANSLATE (2018), https://www.chinalawtranslate.com/organic-law-of-the-peoples-procuratorate-of-the-prc-2018/ [https://perma.cc/K8CQ-R64H] [hereinafter Organic Law of the People's Procuratorate].

and the procuratorates compose the *gongjianfa* (公检法), a term referring to all three institutions in one.[44]

The dual system, wherein the CCP exercises *de facto* power over the formal State structures, also applies to the courts.[45] The Central Party Political-Legal Committee, established in 1978, reports to the Central Party Committee and is responsible for the "coordinat[ion of] all legal institutions."[46] Local Party Political-Legal Committees exercise influence over judicial policies and, in some circumstances, may influence the outcome of specific cases.[47] Since Xi Jinping assumed power as the CCP's General Secretary in 2012, the CCP has emphasized the priority of "governing the country in accordance with law" (依法治国).[48] In response, CCP-led reforms have increased standardization across the court system and strengthened some protections for the judiciary.[49] It has remained clear, however. that the CCP itself is not subject to the rule of law.[50] The courts continue to lack independence under the CCP, with the CCP exercising increasing control over the legal system.[51]

2. Key Actors in China's Cybersecurity Administration

The main institutions responsible for developing and enforcing cybersecurity policies span both CCP and State organizations. At the top, the Cyberspace Administration of China ("CAC"), a CCP agency, reports to the Central Leading Group for Cyberspace Affairs, which Xi Jinping leads.[52] The CAC, which consolidated bureaucratic authority over previously overlapping and redundant institutions in 2014,[53]

---

44. WANG, BIDDULPH & GODWIN, *supra* note 41, at 26.

45. *See generally* Ling Li, *Political-Legal Order and the Curious Double Character of China's Courts*, 6 ASIAN J.L. & SOC'Y 19 (2019); HORSLEY, *supra* note 10.

46. Li, *supra* note 45, at 25–26.

47. *Id.* at 27.

48. *China New Leaders: Xi Jinping Heads Line-Up for Politburo*, BBC NEWS (Nov. 15, 2012), https://www.bbc.com/news/world-asia-china-20322288 [https://perma.cc/27KP-TADR]; HORSLEY, *supra* note 10, at 1.

49. HORSLEY, *supra* note 10, at 1, 5.

50. *Id.* at 1.

51. *Id.* at 7.

52. David Bandurski, *Web of Laws: How China's New Cyberspace Administration is Securing Its Grip on the Internet*, H.K. FREE PRESS (May 7, 2017, 10:30 AM), https://hongkongfp.com/2017/05/07/web-laws-chinas-new-cyberspace-administration-securing-grip-internet/ [https://perma.cc/V6R5-XEAX].

53. Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 430–31 (2020).

promulgates cybersecurity policy and regulates online content.[54] The CAC has publicized investigations against companies that have allegedly violated the CSL, [55] with local branches of the CAC imposing fines.[56] While the exact amount of the fine is not always made public,[57] the CAC likely bases fines on the CSL, which authorizes fines of up to 1,000,000 RMB (approx. $154,000 USD).[58] The Ministry of Public Security ("MPS"), which all local public security bureaus ultimately report to, has historically managed China's "Great Firewall" and conducted general cybersecurity management.[59] The relationship between the CAC and the MPS in implementing and enforcing cybersecurity standards was unclear immediately after the implementation of the law—recent documents suggest that the MPS has taken primary responsibility for enforcing the core provisions of the CSL.[60] For example, local public security bureaus have conducted large-scale

54. Paul Triolo et al., *China's Cybersecurity Law One Year On*, NEW AMERICA (Nov. 30, 2017), http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/ [https://perma.cc/3G2K-UQVH]; Wang, *supra* note 53, at 454.

55. Charlotte Gao, *China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law*, THE DIPLOMAT (Sept. 26, 2017), https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/ [https://perma.cc/4373-5LGK].

56. *See, e.g.*, Beijing Shi Wangxinban Yiju Wangluo Anquan Fa Dui Xinlang Weibo, Baidu Tieba Zuochu Xingzheng Chufa (北京市网信办依据《网络安全法》对新浪微博、百度贴吧作出行政处罚) [Beijing Cyberspace Office Imposes Administrative Punishments on Weibo, Baidu According to the Cybersecurity Law], WEIXIN (Sept. 25, 2017), https://mp.weixin.qq.com/s/eNkQl9JCf3kz96gAhozuEw [https://perma.cc/D69Z-X6RW].

57. *Id.*

58. Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法)[Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 6, 2016, effective June 1, 2017), art. 59, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm [https://perma.cc/94MK-UKPY], *translated in* Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, NEW AMERICA (June 29, 2018), http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ [https://perma.cc/QZ29-TN6D] [hereinafter Cybersecurity Law].

59. Triolo et al., *supra* note 54.

60. Guanche Luoshi Wangluo Anquan Dengji Baohu Zhidu He Guanjian Xinxi Jichu Sheshi Anquan Baohu Zhidu de Zhidao Yijian (贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见) [Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System], ZHONGHUA RENMIN GONGHEGUO GONG'AN BU (中华人民共和国公安部) [THE MINISTRY OF PUBLIC SECURITY OF THE PEOPLE'S REPUBLIC OF CHINA] (Sept. 22, 2020), https://www.mps.gov.cn/n6557558/c7369310/content.html, *translated in* Rogier Creemers et al., *Chinese Government Clarifies Cybersecurity Authorities (Translation)*, NEW AMERICA (Sept. 25, 2020), http://newamerica.org/cybersecurity-initiative/digichina/blog/chinese-government-clarifies-cybersecurity-authorities-translation/ [https://perma.cc/WS4X-YGYA].

inspections of companies for compliance with the CSL, and imposed fines and other administrative penalties.[61]

3. Administrative, Criminal, and Civil Litigation

There are several types of litigation within the Chinese court system—most significant to this Note are administrative, criminal, and civil litigation. Administrative litigation has received significant attention in the literature on the Chinese court system because it is the only way Chinese citizens and companies can sue the State.[62] The 1989 Administrative Litigation Law ("ALL"), amended in 2014, is the formal legal basis for administrative litigation.[63] Under the ALL, litigants may not bring general challenges to laws—they must challenge an administrative decision that is specific to the litigant, which excludes regulations and normative documents of general application.[64] Typical administrative cases include citizens challenging the local government's seizure of land, administrative punishments including fines and detentions,[65] provision of employment benefits, and the granting of government permits.[66] The courts tend to defer to the local government, with plaintiffs obtaining relief in only one-fourth of cases.[67]

---

61. DENTONS, 2019 CHINA DATA PROTECTION & CYBERSECURITY ANNUAL REPORT 17 (2019).

62. For a discussion of the ALL pre-2014, see generally Susan Finder, *Like Throwing an Egg Against a Stone—Administrative Litigation in the People's Republic of China*, 3 J. CHINESE. L. 1 (1989). For a discussion of the 2014 amendments to the ALL, see generally He Haibo, *How Much Progress Can Legislation Bring? The 2014 Amendment of the Administrative Litigation Law of PRC*, 13 U. PA. ASIAN L. REV. 137 (2018).

63. Zhonghua Renmin Gongheguo Xingzheng Susong Fa (中华人民共和国行政诉讼法) [PRC Administrative Litigation Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 1, 2014, effective May 1, 2015) http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/29/content_2024894.htm [https://perma.cc/SD9R-6K5Y], *translated in Administrative Litigation Law (2015)*, CHINA L. TRANSLATE (Oct. 1, 2015), https://www.chinalawtranslate.com/行政诉讼法 [https://perma.cc/9W7U-6T9H] [hereinafter Administrative Litigation Law].

64. He, *supra* note 62, at 141; Administrative Litigation Law, *supra* note 63, art. 13.

65. Administrative punishments are less severe than criminal penalties and are governed by the 2005 Law on Administrative Penalties for Public Securities Offenses. *See* Ruohui Zhao, *Administrative Punishment*, *in* THE ENCYCLOPEDIA OF CORRECTIONS (Kent R. Kerley ed., 2017).

66. Liebman et al., *supra* note 32, at 192–93.

67. He, *supra* note 62, at 141.

The courts also handle criminal cases, which are governed by the Criminal Procedure Law and the Criminal Law of the PRC.[68] The Criminal Law, spanning over 400 articles, constitutes the main basis for criminal liability.[69] Distinguishing characteristics of China's criminal system include the high conviction rate—ninety-nine percent—and weaknesses in procedural protections for defendants[70] that have persisted despite recent reforms.[71]

In China's civil litigation system, governed by the Civil Procedure Law, courts have significant flexibility in interpreting and applying the law.[72] For example, in tort litigation, courts may deviate from the actual provisions of the law in the interest of compensating parties that have suffered losses.[73] Courts are often balancing the interests of

68. Zhonghua Renmin Gongheguo Xing Fa (中华人民共和国刑法) [Criminal Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Mar. 14, 1997, effective Oct. 1, 1997), http://www.npc.gov.cn/wxzl/wxzl/2000-12/17/content_4680.htm [https://perma.cc/6L4X-S4YM] *translated in Criminal Law of the People's Republic of China*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA (Jan. 15, 2013), https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china [https://perma.cc/HZS3-WF3K] [hereinafter Criminal Law]; Zhonghua Renmin Gongheguo Xingshi Susong Fa (中华人民共和国刑事诉讼法) [Criminal Procedure Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Mar. 3, 2012, effective Jan. 1, 2013), http://www.gov.cn/flfg/2012-03/17/content_2094354.htm, *translated in Criminal Procedure Law of the People's Republic of China*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA (Nov. 22, 2016), https://www.cecc.gov/resources/legal-provisions/criminal-procedure-law-of-the-peoples-republic-of-china [https://perma.cc/S9WS-5BP6].

69. JIANFU CHEN, CRIMINAL LAW AND CRIMINAL PROCEDURE LAW IN THE PEOPLE'S REPUBLIC OF CHINA 5 (2013).

70. Criminal defense attorneys may themselves face sanctions if they question the judge's procedure. *"All Criminal Defendants to Have Lawyers": Is Access to Defense Lawyers Enough in a System Designed Against Defendants? Part I*, DUI HUA HUM. RTS. J. (Aug. 29, 2018), http://www.duihuahrjournal.org/2018/08/all-criminal-defendants-to-have-lawyers.html [https://perma.cc/8N3V-RBS5].

71. Reform efforts include emphasizing a "trial-centered" approach as opposed to resolving criminal cases outside of the procedural protections of the trial process. Sarah Biddulph, Elisa Nesossi & Susan Trevaskes, *Criminal Justice Reform in the Xi Jinping Era*, 2 CHINA L. & SOC'Y REV. 63, 77–78 (2017).

72. Zhonghua Renmin Gongheguo Minshi Susong Fa (中华人民共和国民事诉讼法) [Civil Procedure Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 27, 2017, effective July 1, 2017), http://www.moj.gov.cn/Department/content/2018-12/25/357_182594.html *translated in Civil Procedure Law of the People's Republic of China*, China International Commercial Court (June 29, 2017), http://cicc.court.gov.cn/html/1/219/199/200/644.html [https://perma.cc/6ZES-FEJM].

73. Benjamin L. Liebman, *Ordinary Tort Litigation in China: Law Versus Practical Justice?*, 1 J. TORT L. 197, 227 (2020).

the local government, media coverage, and common-sense notions of fairness in applying the law.[74]

B. Overview of the 2017 Cybersecurity Law

The National People's Congress passed the CSL in November 2016 and it came into effect on June 1, 2017.[75] The CSL consists of seventy-nine articles, divided into seven chapters.[76] Several key provisions are highlighted below.[77]

1. Scope

First, the CSL defines the scope and application of China's cybersecurity legal regime. The law mainly applies to two parties—"network operators" and "critical information infrastructure" operators—while also imposing responsibilities on individuals[78] and the State.[79] A "[n]etwork" is any "system comprised of computers or other information terminals."[80] "Network operators" are defined as "network owners, managers, and network service providers."[81] Practically speaking, "network operators" could include any business using the internet[82]—as the case law demonstrates, the CSL has covered internet companies from travel websites to gaming.[83] "Critical information infrastructure" encompasses: "[P]ublic communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed . . . might seriously endanger national security, national welfare, the people's livelihood, or the public interest."[84] The Chinese

74. Chinese courts emphasize "flexible problem solving" with the goal towards preventing or eliminating disputes. *Id.* at 225.

75. Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, THE DIPLOMAT (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ [https://perma.cc/6N7R-GBKG].

76. Cybersecurity Law, *supra* note 58.

77. For an excellent in-depth analysis of the law around the time of its enactment, see generally Lee, *supra* note 1.

78. Cybersecurity Law, *supra* note 58, art. 12.

79. Cybersecurity Law, *supra* note 58, arts. 3–8, 15–20.

80. Cybersecurity Law, *supra* note 58, art. 76.

81. *Id.*

82. Wagner, *supra* note 75; Lee, *supra* note 1, at 71.

83. *See infra* Section II.C.3.

84. Cybersecurity Law, *supra* note 58, art. 31.

government has continued to expand this list through subsequent regulations, for example by adding "defense technology industries" in a recent regulation,[85] while also maintaining significant discretion for interpreting the term with regard to unlisted industries.[86] While the law formally applies within the territory of mainland China,[87] the CSL's data regulation provisions, combined with data's borderless nature,[88] mean that in practice the CSL has extraterritorial effects.[89]

2. Individual Rights

While international attention has focused on China's core purposes of strengthening national security[90] and promoting China's concept of "cyber sovereignty,"[91] the CSL also includes protections for the rights of individuals using the internet and conducting business.[92] The CSL establishes rights and responsibilities for individuals, stating that individuals have a right to "use networks in accordance with the law"[93] and imposing obligations to "observe public order[] and respect social morality."[94] These articles are worded so broadly that they

85. Lester Ross, Kenneth Zhou, & Tingting Liu, *China Rolls Out Critical Information Infrastructure Security Protection Regulations*, WILMERHALE (Aug. 10, 2021), https://www.wilmerhale.com/en/insights/client-alerts/20210819-china-rolls-out-critical-information-infrastructure-security-protection-regulations [https://perma.cc/JR3P-UHRQ].

86. *See* Richard Bird, *Am I Critical (Information Infrastructure)?*, FRESHFIELDS BRUCKHAUS DERINGER (Apr. 29, 2020), https://digital.freshfields.com/post/102g5zu/am-i-critical-information-infrastructure infrastructure [https://perma.cc/94HH-7HPG].

87. Article 2 of the CSL states that the law generally applies "within the mainland territory of the People's Republic of China." Cybersecurity Law, *supra* note 58, art. 2.

88. Allison Lapehn, *Why the U.S. Should Pay Attention to China's Draft Data Security Law*, SUPCHINA (Oct. 5, 2020), https://supchina.com/2020/10/05/why-the-u-s-should-pay-attention-to-chinas-draft-data-security-law/ [https://perma.cc/6BKX-PSBP].

89. Under Article 37's data localization requirement, for example, a company physically located outside of China but serving customers in China would fall under the CSL's requirements if they were "critical information infrastructure" operators. *See* JONES DAY, IMPLEMENTING CHINA'S CYBERSECURITY LAW 4 (2017), https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf [https://perma.cc/LK72-RVZ2].

90. *See* Jackson, *supra* note 29.

91. Cybersecurity Law, *supra* note 58 art. 1; Lee, *supra* note 1, at 67–70; Wang, *supra* note 53, at 396 (describing the Chinese government's concept of "cyber sovereignty" as its ability to control the internet within Chinese territory).

92. The CSL aims to "protect the lawful rights and interests of citizens, legal persons, and other organizations" and "promote the healthy development of the informatization of the economy and society." Cybersecurity Law, *supra* note 58, art. 1.

93. Cybersecurity Law, *supra* note 58, art. 12.

94. *Id.*

could be interpreted in any number of ways by the courts.[95] Crucially, some establish rights for individuals related to privacy and data security.[96] Plaintiffs could theoretically rely on these provisions as a basis for civil litigation.

3. National Cybersecurity Protections

Chapters III and IV of the CSL impose the most detailed requirements for network operators and critical information infrastructure operators, such as formulating emergency response plans for security breaches,[97] preventing cyberattacks,[98] and maintaining confidentiality in processing and storing data.[99] Articles 42, 43, and 44 concern personal information, requiring network operators to take steps to "ensure the security of personal information they gather" and prohibiting unlawful use of personal information.[100]

Several articles shed light on China's unique concepts of "cyber sovereignty"[101] and cybersecurity. Article 24 requires network providers to confirm the real names of their customers before providing service.[102] China has been the most prominent country to embrace an approach to cybersecurity that requires real names and disallows anonymity.[103] One of the most controversial provisions for foreign companies is Article 37's data localization requirement, which requires critical information infrastructure operators to store data collected within China inside the country—an expensive requirement that

95. For example, Article 12 also includes a long list of prohibited activities, such as "us[ing] the Internet to engage in activities endangering national security, national honor, and national interests" and "incit[ing] separatism." *Id*. *See also* Lee, *supra* note 1, at 89.

96. Article 22 requires "network providers" to obtain consent from the users before collecting user information. Article 43 states individuals have the right to demand deletion of their personal information. Cybersecurity Law, *supra* note 58, arts. 22, 43.

97. *Id*. art. 25.

98. *Id*. art. 21.

99. *Id*. art. 40.

100. Unlawful uses of personal information include disclosure of personal information without consent, "tamper[ing] with" personal data or destroying it. *Id*. art. 42.

101. *See supra* note 91 and accompanying text.

102. Cybersecurity Law, *supra* note 58, art. 24.

103. For more on China's actions pre-CSL to implement real-name registration rules, see generally Jyh-An Lee & Ching-Yi Liu, *Real-Name Registration Rules and the Fading Digital Anonymity in China*, 25 WASH. INT'L L.J. 1 (2016); *see also* Samm Sacks & Paul Triolo, *Shrinking Anonymity in Chinese Cyberspace*, LAWFARE (Sept. 25, 2017, 12:20 PM), https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace [https://perma.cc/XS7B-E5HT].

places data within the physical reach of the CCP.[104] Article 37 also requires security assessments for cross-border data transfer, reinforcing China's attempts to control the storage and flow of data.[105]

4. Penalties

Finally, the CSL sets specific penalties and legal remedies for violations of the CSL. The CSL may be a basis for both criminal and civil liability.[106] Penalties under the law include fines of up to 1,000,000 RMB (approx. $154,000 USD), detention by the public security organizations for up to 15 days, and suspension of business operations.[107] Some violations are only subject to punishment "in accordance with the provisions of the relevant laws and administrative regulations."[108] This allows for additional penalties to be set by the more detailed implementing regulations issued after the CSL,[109] as well as for courts to cite multiple laws or regulations in its final decisions.[110]

C. Global Response to the Cybersecurity Law

Following the CSL's release and implementation, responses from multinational companies (MNCs) and governments center on three areas. The first concerns the CSL's allegedly protectionist measures,[111] particularly the data localization requirement in Article

104. Cybersecurity Law, *supra* note 58, art. 37; Yuan Yang, *China's Cyber Security Law Rattles Multinationals*, FIN. TIMES (May 30, 2017), https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996 [https://perma.cc/UVC6-DCPW].

105. Cybersecurity Law, *supra* note 58, art. 37.

106. *Id*. art. 74.

107. *Id.* arts. 59–69.

108. *Id.* art. 70.

109. Samm Sacks, *Beijing's Cyber Governance System, in* MEETING THE CHINA CHALLENGE: RESPONDING TO CHINA'S MANAGED ECONOMY 31 (James Lewis ed., 2018).

110. *See, e.g.*, Gao Guangjun Yu Anshan Shi Gong'an Ju Tiedong Gong'an Fenju Gong'an Xingzheng Guanli: Qita (Gong'an) Yi Shen Xingzheng Panjue Shu (高广俊与鞍山市公安局铁东公安分局公安行政管理:其他(公安)一审行政判决书) [Gao Guangjun and Anshan City Public Security Bureau, Tiedong Branch, Public Security Management: Other (Public Security) First Instance Administrative Judgment] China Judgements Online, (2020) Liao 0381 Xingchu 30 Hao ((2020)辽0381行初30号) [2020 Liaoning First Instance Administrative Judgment No. 30] (Haicheng City People's Ct., June 19, 2020) [hereinafter Gao v. Tiedong Public Security Bureau] (citing to both the CSL and the PRC Law on Public Security Management Penalties, 中华人民共和国治安管理处罚法).

111. U.S.-CHINA ECON. & SEC. REV. COMM'N, *Year in Review: Economics and Trade*, in 2017 ANNUAL REPORT TO CONGRESS 35, 40–41 (2017); Eva Dou, *Global Tech Companies*

37.[112] MNCs predict the data localization requirement will grant a special advantage to domestic competitors whose data infrastructure is already located in China, while foreign competitors may need to establish expensive new data storage centers and incur additional costs with data transfers.[113] The security review requirement also raises fears that companies will be forced to disclose intellectual property.[114] Second, vaguely worded provisions, such as the definition of "network operator," potentially grant Chinese administrative agencies and public security bureaus wide discretion when applying the law.[115] Third, observers fear that the CSL will strengthen the CCP's ability to punish dissenters and limit speech, both within China and abroad.[116] Beyond the immediate impact of the law, a broader concern is that the CSL represents China's vision for cybersecurity—one that similarly situated authoritarian states, or even democratic ones, may seek to emulate.[117]

Indeed, while this Note focuses on the application of the CSL within China's judicial system, its insights into the CSL and China's cybersecurity vision are relevant to the broader international community because China's technology practices and domestic laws have an outsized impact on other states.[118] China is a sizeable exporter of both information and communications technology (ICT) and cybersecurity policy.[119] Huawei, a major supplier of ICT,[120] along with Chinese

Call on China to Delay Cybersecurity Law, WALL ST. J. (May 15, 2017, 4:31 AM), https://www.wsj.com/articles/global-tech-companies-call-on-china-to-delay-cybersecurity-law-1494837117 [https://perma.cc/V7MU-GGWG].

112. Wagner, *supra* note 75.

113. *Market Access Challenges in China: Hearing before the Subcomm. on Int'l Trade, Customs, & Glob. Competitiveness of the S. Comm. on Finance*, 115th Cong. 44 (2018) (statement of Dean Garfield, President & CEO, Info. Tech. Indust. Council).

114. *Id.* at 43.

115. Jacob Quinn, *A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law*, 20 SMU SCI. & TECH. L. REV. 407, 432 (2017); Wagner, *supra* note 75; Lee, *supra* note 1, at 89.

116. Quinn, *supra* note 115, at 430.

117. *See* notes 23–27 and accompanying text for examples of countries that are emulating China's cybersecurity laws.

118. *See infra* Section III.C .

119. Editorial Board, *Opinion: China is Exporting Its Digital Authoritarianism*, WASH. POST (Aug. 5, 2020), https://www.washingtonpost.com/opinions/china-is-exporting-its-digital-authoritarianism/2020/08/05/f14df896-d047-11ea-8c55-61e7fa5e82ab_story.html [https://perma.cc/NTC5-XHPZ].

120. Amy Mackinnon, *For Africa, Chinese-Built Internet Is Better Than No Internet at All*, FOREIGN POL'Y (Mar. 19, 2019, 3:53 PM), https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all [https://perma.cc/2HKV-RQKR]; *Our Company*, HUAWEI, https://www.huawei.com/us/corporate-information [https://perma.cc/

government representatives, is closely involved in shaping cybersecurity policy within countries that purchase its products and services.[121] Countries with existing authoritarian governments or authoritarian tendencies, such as Ecuador, Venezuela, and Zimbabwe, have welcomed Chinese technology and assistance.[122] China, one of Cambodia's largest foreign investors, has supplied surveillance technology to the country's longstanding ruler, Prime Minister Hun Sen.[123] In August 2020, a leaked draft of a Cambodian cybercrime law contained provisions nearly identical to those of the CSL—allowing fines or imprisonment for people that make false statements online threatening "public safety" and "national security," and requiring preservation of data for at least six months (mirroring CSL Article 21(3)).[124] Vietnam's pattern of enforcement has been very similar to that of China in adopting the CSL.[125] While China's investments are not generating the same level of influence in all countries, China's cybersecurity

64G6-S3S5]; *Global Smartphone Market Share: By Quarter*, COUNTERPOINT RSCH. (Feb. 22, 2020), https://www.counterpointresearch.com/global-smartphone-share/ [https://perma.cc/99C7-3RNU].

121. For example, Huawei has led training sessions for its government partners on cybersecurity practices. Abdi Latif Dahir, *China Is Exporting Its Digital Surveillance Methods to African Governments*, NEXTGOV (Nov. 1, 2018), https://www.nextgov.com/emerging-tech/2018/11/china-exporting-its-digital-surveillance-methods-african-governments/152495/ [https://perma.cc/JW93-HJA2]; Sacks, *supra* note 26.

122. Paul Mozur, *Made in China, Exported to the World: The Surveillance State*, N.Y. TIMES (Apr. 4, 2019), https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html [https://perma.cc/UGQ5-TDMK] (quoting an Ecuadorean dissident stating "I believe what the Chinese model generates is control over society . . . . A rigid control."); THE NEW BIG BROTHER: CHINA AND DIGITAL AUTHORITARIANISM, S. PRT. 116-47, at 31–35 (2020).

123. INT'L REPUBLICAN INST., CHINESE MALIGN INFLUENCE AND THE CORROSION OF DEMOCRACY 11 (David Shullman ed., 2019), https://www.iri.org/sites/default/files/chinese_malign_influence_report.pdf [https://perma.cc/C3EG-7BS7].

124. Jessica Goodfellow, *Cambodia's Draft Cybercrime Law Raises Free Speech Alarm*, CAMPAIGN ASIA (Oct. 13, 2020), https://www.campaignasia.com/article/cambodias-draft-cybercrime-law-raises-free-speech-alarm/464204 [https://perma.cc/WQL2-CXUU].

125. Jon Russell, *Vietnam Threatens to Penalize Facebook for Breaking Its Draconian Cybersecurity Law*, TECHCRUNCH (Jan. 9, 2019, 7:16 AM), https://social.techcrunch.com/2019/01/09/vietnam-threatens-to-penalize-facebook/ [https://perma.cc/2S43-F3AK]; Timothy McLaughlin, *Under Vietnam's New Cybersecurity Law, U.S. Tech Giants Face Stricter Censorship*, WASH. POST (Mar. 16, 2019, 5:07 PM), https://www.washingtonpost.com/world/asia_pacific/under-vietnams-new-cybersecurity-law-us-tech-giants-face-stricter-censorship/2019/03/16/8259cfae-3c24-11e9-a06c-3ec8ed509d15_story.html [https://perma.cc/5SXF-348J].

vision is highly attractive to existing authoritarian regimes[126] and is accelerating authoritarian tendencies in democracies.[127] Thus, China's cybersecurity vision as implemented domestically may have ripple effects extending far beyond China's borders.

II. APPLICATION OF THE CYBERSECURITY LAW

A. Enforcement of the Cybersecurity Law

Despite the extensive commentary surrounding the initial passage of the 2017 CSL, there remains little concrete guidance on how the government has applied the law in practice.[128] There have been several publicized instances of high-profile enforcement actions based on the CSL brought against major technology companies.[129] The CAC has taken the lead on these enforcement actions, which have mainly involved imposition of fines against companies.[130] However, it has not always been clear what specific actions led to the violations.[131] In addition, the CAC, in collaboration with the Ministry of Public Security and the local public security bureaus, has identified companies considered "critical information infrastructure" operators and begun security reviews.[132] China has continued to release new standards and

126. David O. Shullman, *Protect the Party: China's Growing Influence in the Developing World*, BROOKINGS INST. (Jan. 22, 2019), https://www.brookings.edu/articles/protect-the-party-chinas-growing-influence-in-the-developing-world/ [https://perma.cc/HS2P-X9QQ].

127. Sarah McKune & Shazeda Ahmed, *Authoritarian Practices in the Digital Age: The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMMC'N 3835, 3842 (2018) (highlighting that India and Pakistan joined China's Shanghai Cooperative Organization and have participated in the Chinese-led anti-terror exercises).

128. Brian Yap, *China's New Cyber Law Could Impede Data Transfers*, INT'L FIN. L. REV. (Mar. 22, 2017).

129. Josh Chin, *China Targets Social-Media Giants WeChat, Weibo in Cybersecurity Probe*, WALL ST. J. (Aug. 11, 2017, 2:14 AM), https://www.wsj.com/articles/wechat-weibo-among-targets-in-china-cybersecurity-probe-1502432081?mod=article_inline [https://perma.cc/4U7Z-G5UB].

130. While WeChat and Weibo were fined for violating Article 47 of the CSL, the specifics of how the companies failed to comply with the law in regulating their content was unclear. *See* Gao, *supra* note 55.

131. *Id*.

132. Susan Ning & Han Wu, *The 1st Year Implementation of the Cybersecurity Law*, CHINA L. INSIGHT (Jan. 10, 2018), https://www.chinalawinsight.com/2018/01/articles/compliance/the-1st-year-implementation-of-the-cybersecurity-law/ [https://perma.cc/5VTU-GDUZ].

regulations since the CSL went into effect,[133] including additional detail on the substantive requirements for security reviews.[134] On the criminal front, cyberattacks and abuse of personal data are the most common prosecutions related to the CSL.[135] These criminal cases likely reflect the prevalence of cybercrime and data theft and rising dissatisfaction with the protections in place.[136]

B. Accessing and Analyzing Chinese Court Cases

One actor that has not yet received significant attention in implementing the CSL, however, is the judiciary. The court judgments available online provide a valuable window into how Chinese judges are approaching and analyzing the CSL, the types of claims and prosecutions that are being brought, and how China's vision of cybersecurity is playing out in practice. While this analysis does not provide a comprehensive view into the CSL's implementation, the selected cases represent a heretofore overlooked source of data on how individual courts are interpreting the letter and spirit of the CSL.

Recent CCP mandates to digitize the entirety of Chinese court decisions and make them accessible to the public have opened a massive source of data on ongoing legal issues in China.[137] However, this data is subject to a number of caveats. First, not all cases are published online, as current regulations permit local courts the discretion to withhold cases.[138] While courts are required to state their reasoning for withholding a case,[139] in practice courts have taken a lax approach to

133. SACKS & LI, *supra* note 15.

134. Lester Ross & Kenneth Zhou, *China Issues New Cybersecurity Review Measures*, WILMERHALE (May 18, 2020), https://www.wilmerhale.com/en/insights/client-alerts/20200518-china-issues-new-cybersecurity-review-measures [https://perma.cc/49QG-FWUB].

135. Paul Mozur, *Apple Customer Data in China Was Sold Illegally, Police Say*, N.Y. TIMES (June 9, 2017), https://www.nytimes.com/2017/06/09/business/china-apple-personal-data-sold.html [https://perma.cc/SE4G-D2LW]; *Recent Enforcement Developments and Trends Regarding China's Cybersecurity Law*, FAEGRE DRINKER (Aug. 31, 2017), https://www.faegredrinker.com/en/insights/publications/2017/8/recent-enforcement-developments-and-trends-regarding-chinas-cybersecurity-law [https://perma.cc/5GQU-LQQJ].

136. Karen Hao, *Inside China's Unexpected Quest to Protect Data Privacy*, MIT TECH. REV. (Aug. 19, 2017), https://www.technologyreview.com/2020/08/19/1006441/china-data-privacy-hong-yanqing-gdpr/ [https://perma.cc/22ZR-GC3M].

137. Liebman et al., *supra* note 32, at 177–78.

138. *Id.* at 181.

139. Guanyu Renmin Fayuan Zai Hulianwang Gongbu Caipan Wenshu De Guiding (关于人民法院在互联网公布裁判文书的规定) [Provisions on People's Courts Release of Judgments on the Internet] (promulgated by the Adjudication Comm. Sup. People's Ct., Aug.

this requirement.[140] Thus, it is difficult to draw quantitative—as opposed to qualitative—observations from the existing data alone. Second, non-criminal enforcement of the CSL is likely taking place outside of the courts and instead through the local public security bureaus and State agencies.[141] Administrative law cases only reflect situations where a plaintiff has chosen to challenge an administrative decision.[142] Overall, the cases reflect a limited subset of court decisions and thus are not necessarily representative of the comprehensive enforcement of the CSL—rather, they are a selective glimpse into the CSL's application within the judicial system.

The following analysis is based on a dataset of approximately 200 cases downloaded from the China Judgments Online site in September 2020.[143] At the time, the dataset included all cases referencing the CSL in the text of the online judgment, which includes a summary of the arguments advanced by each party, the evidence, and the court's holding.[144] The majority of cases (approximately 145 out of 200) are civil cases, with approximately twenty-nine administrative law cases, twenty-four criminal cases, two national compensation cases, and two enforcement cases.[145] The cases date from 2017 to 2020 and represent trial-court and appellate-level judgments.[146] The following analysis focuses on the approximately fifty cases where the court (as opposed to the parties to the litigation) referenced the CSL in the holding.

29, 2016, effective Oct. 1, 2016) art. 6, http://www.court.gov.cn/zixun-xiangqing-25321.html [https://perma.cc/P54L-VT4N], *translated in The Supreme People's Court Provisions on People's Courts Release of Judgments on the Internet*, CHINA L. TRANSLATE (Aug. 30, 2016), https://www.chinalawtranslate.com/the-supreme-peoples-court-provisions-on-peoples-courts-release-of-judgments-on-the-internet/ [https://perma.cc/4TEF-PDE4] [hereinafter Provisions on People's Courts Release of Judgments].

140. While the rules requiring publication are binding on the courts, there is not a strict enforcement mechanism—lower courts are evaluated in an annual review process that serves as one form of accountability for following the regulations. *See* Liebman et al., *supra* note 32, at 189.

141. Henry Kenyon, *China Cybersecurity Regulation Allows Police to Inspect Internet Firms*, CQ ROLL CALL WASH. DATA PRIVACY BRIEFING (Oct. 24, 2018), 2018 WL 5283418.

142. *See* Administrative Litigation Law, *supra* note 63, arts. 2, 12.

143. ZHONGGUO CAIPAN WENSHUWANG (中国裁判文书网) [CHINA JUDGEMENTS ONLINE], https://wenshu.court.gov.cn/ [https://perma.cc/Z2VJ-LTY4] (last visited Mar. 1, 2021) [hereinafter China Judgments Online].

144. *Id*.

145. *Id*.

146. *Id*.

C. Analyzing Cases Relying on the Cybersecurity Law

1. Administrative Law Cases: Managing Online Speech and Targeting Dissent

The available administrative cases illustrate the Chinese government's use of the CSL to to identify and suppress deviant (as determined by the government) online behavior. The available cases only represent circumstances where plaintiffs *challenged* the administrative action.[147] Of the roughly twenty-nine administrative cases, six cited to the CSL in the holding. The plaintiffs lost in all the cases, which is consistent with a low win rate for plaintiffs in administrative cases.[148]

First, the courts generally affirm the public security bureaus' use of CSL Articles 12 and 70 to punish internet users who have made dissenting or inflammatory statements online.[149] In several of the cases reviewed, the individual plaintiffs challenged administrative detentions imposed by the public security bureau for internet activity criticizing the government.[150] In *Gao v. Tiedong Public Security Bureau*, the Tiedong Public Security Bureau arrested the plaintiff for allegedly posting in a WeChat (a popular Chinese social media app) group messages such as "Let the Chairman [Xi Jinping] come after me, sooner or later I will oppose him" (让主席给我嘣了吧早晚我要反) and other "improper reactionary speech" (不当反动言论).[151] According to the public security bureau, the plaintiff signed a confession after interrogation.[152] Signing confessions is a common practice for both administrative punishments and the criminal system.[153] Here, the

147. See *supra* Section I.A.3 for an introduction to administrative litigation.

148. He, *supra* note 62, at 145–47.

149. Cybersecurity Law, *supra* note 58, arts. 12:

> Any person . . . using networks…must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information . . . .
>
> "Publication or transmission of information prohibited by Article 12 Paragraph 2 of this Law or other laws or administrative regulations shall be punished in accordance with the provisions of the relevant laws and administrative regulations." *Id.*, art. 70.

150. For the difference between administrative detention and criminal detention, see Zhao, *supra* note 65.

151. Gao v. Tiedong Public Security Bureau, *supra* note 110.

152. *Id*.

153. Aris Teon, *Voluntary Surrender and Confession in China's Legal System—From the Empire to the People's Republic*, GREATER CHINA J. (June 20, 2016), https://china-

public security bureau based its punishment—administrative detention for fifteen days—on Article 26(4) of the 2005 Law on Administrative Penalties for Public Security Offenses[154] and Articles 12 and 70 of the CSL.[155] The plaintiff contested the punishment in the administrative lawsuit, arguing that he "hastily signed the confession at the urging of the public security bureau" (在催促下草草签了字) and did not intend to make a reference to Xi Jinping.[156] The court in its analysis noted that the alleged messages were posted on October 1, 2019,[157] the same day as the 2019 National Day Military Parade celebrating 70 years of Communist rule.[158] The court concluded that the defendant public security bureau's evidence, which included alleged screenshots from the plaintiff's phone and the plaintiff's confession, was sufficient to support the administrative punishment.[159]

In *Qian v. Rudong Public Security Bureau*, the Nantong City Intermediate People's Court determined that the public security bureau acted appropriately in detaining an individual who posted online about splitting the city to join Japan.[160] The court noted in its holding the high number of views received by the post and emphasized that "the [i]nternet has already become the main platform for public exchange . . . [thus] speaking online should be the same as it would in real

journal.org/2016/06/20/voluntary-surrender-and-confession-in-chinas-legal-system-from-the-empire-to-the-peoples-republic [https://perma.cc/R9AK-CZ4M].

154. The improper behavior under this law was the offense of "picking quarrels and causing trouble" (寻衅滋事). *See* Zhonghua Renmin Gongheguo Zhi'an Guanli Chufa Fa (中华人民共和国治安管理处罚法) [Public Security Administration Punishments Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 28, 2005, effective Mar. 1, 2006) art. 26, http://www.gov.cn/ziliao/flfg/2005-08/29/content_27130.htm [https://perma.cc/99YZ-RZDY], *translated in Public Security Administration Punishments Law of the People's Republic of China*, LAW INFO CHINA 北大法律信息网, http://www.lawinfochina.com/display.aspx?lib=law&id=4549&CGid [https://perma.cc/5HMD-DJ8H] (last visited Mar. 1, 2021).

155. Cybersecurity Law, *supra* note 58, arts. 12, 70.

156. Gao v. Tiedong Public Security Bureau, *supra* note 110.

157. *Id*.

158. Mike Ives, *In Pictures: China's National Day Parade Features Pomp and Artillery*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/world/asia/china-national-day-parade.html [https://perma.cc/3E6U-338G].

159. Gao v. Tiedong Public Security Bureau, *supra* note 110.

160. *See* Qian Xiaofei Yu Rudong Xian Gong'an Ju Xingzheng Chufa Ershen Xingzheng Panjueshu (钱小飞与如东县公安局行政处罚二审行政判决书) [Qian Xiaofei and Rudong County Public Security Bureau Administrative Punishment Second Instance Judgment] China Judgements Online, (2018) Su 06 Xingzhong 426 Hao ((2018) 苏06行终426号) [2018 Jiangsu Second Instance Administrative Judgment No. 426] (Nantong Interm. People's Ct., July 30, 2018) [hereinafter Qian v. Rudong Public Security Bureau].

life."[161] Similar cases involve plaintiffs contesting administrative punishments for publishing a post online after attempting to go to Beijing to petition,[162] or publishing a post on WeChat criticizing the local party government and the CCP.[163] These cases demonstrate, at a minimum, the courts affirming the use of CSL Article 12 to punish online behavior that expresses discontent with the government or could contribute to spreading unrest.

In the four reviewed cases involving politically controversial or anti-government speech, the courts sided with the government, rejecting attempts by plaintiffs to invoke the CSL in support of their rights to use the internet. In *Lu v. Sandu Shui Public Security Bureau*, the plaintiff-appellant received ten days of administrative detention for posting a video on Baidu (a Chinese search engine and social media website) depicting an individual being injured during a property demolition conducted by the local government.[164] The public security bureau claimed that the video was fake and damaged the reputation of the local government.[165] The plaintiff appealed the lower court's dismissal of an administrative lawsuit, invoking CSL Article 12 as support for his *right* to use networks "in accordance with the law" and arguing that exposing corrupt government behavior was part of this

161. *Id.* ("网络空间已成为人们沟通交流的公共平台 . . . 在网络空间上发表言论应当与现实生活中一样.").

162. Liang Wanmao Yu Huangmei Xian Gong'an Ju Gong'an Xingzheng Guanli: Zhi'an Guanli (Zhi'an) Yishen Xingzheng Panjue Shu (梁万茂与黄梅县公安局公安行政管理:治安管理(治安)一审行政判决书) [Liang Wanmao and Huangmei County Public Security Bureau Public Security Management: Public Security Management (Public Security) First Instance Administrative Judgment] China Judgements Online, (2019) E 1182 Xingzhong 44 Hao ((2019)鄂1182行初44号) [2019 Hubei First Instance Administrative Judgment No. 44] (Wuxue City People's Ct., June 27, 2019) [hereinafter Liang v. Huangmei Public Security Bureau].

163. Li Lijun, Yuechi Xian Gong'an Ju Gong'an Xingzheng Guanli: Zhi'an Guanli (Zhi'an) Ershen Xingzheng Panjue Shu (李立君、岳池县公安局公安行政管理:治安管理(治安)二审行政判决书) [Li Lijun and Yue Chi County Public Security Bureau Public Security Administration: Public Security Management (Public Security) Second Instance Administrative Judgment] China Judgements Online, (2019) Chuan 16 Xingzhong 44 Hao ((2019) 川16行终44号) [2019 Sichuan Second Instance Administrative Judgment No. 44] (Guang An Interm. People's Ct., May 8, 2019) [hereinafter Li v. Yuechi Public Security Bureau].

164. Lu Wenyou, Sandu Shui Zu Zizhi Xian Gong'an Ju Gong'an Xingzheng Guanli: Zhi'an Guanli (Zhi'an) Ershen Xingzheng Panjue Shu (陆文友、三都水族自治县公安局公安行政管理:治安管理(治安)二审行政判决书) [Lu Wenyou, Sandu Shui Autonomous County Public Security Bureau Public Security Administration: Public Security Management (Public Security) Second Instance Administrative Judgment] China Judgements Online, (2018) Qian 27 Xingzhong 167 Hao ((2018) 黔27行终167号) [2018 Guizhou Second Instance Administrative Judgment No. 167] (Qiannan Buyi and Miao Autonomous Interm. People's Ct., July 23, 2018) [hereinafter Lu v. Sandu Shui Public Security Bureau].

165. *Id.*

right.[166] But the court ignored this argument, instead holding that internet users should exercise caution when posting about "party and government agencies [and] mass incidents . . . that may disrupt social order" (党政机关、群体性事件 . . . 可能扰乱社会秩序).[167] In these cases, the courts never affirmed the plaintiff's internet rights when politically controversial speech was involved. While Article 12 prohibits a wide variety of internet behavior,[168] the court cases citing to the CSL focus mainly on speech referring directly to the CCP or the State.

Second, the administrative law cases involving companies generally speak to more routine enforcement of the CSL. These cases provide a window into how local public security bureaus are enforcing the CSL, for example, by fining "network operators" that fail to verify the real names of customers or retain network logs.[169] However, even these enforcement cases may involve concerns with dissenting speech. In *Xu v. Leiyang Public Security Bureau*, the public security bureau issued a warning to the plaintiff, the alleged operator of an online forum (论坛) website, claiming that the website stored only four months of network logs, violating CSL Article 21's requirement of six months of logs.[170] The plaintiff argued that the registered website owner was a different person and provided screenshots showing that the required

166. Cybersecurity Law, *supra* note 58, art. 12 ("The State protects the rights of citizens . . . to use networks in accordance with the law.").

167. Lu v. Sandu Shui Public Security Bureau, *supra* note 164 (upholding plaintiff's administrative detention for publishing videos online that "disturbed the public order").

168. Prohibited behavior includes "advocat[ing] ethnic hatred and ethnic discrimination, disseminat[ing] violent, obscene, or sexual information . . . " *See* Cybersecurity Law, *supra* note 58, art. 12.

169. Shanghai Xincheng Dianxin Youxian Gongsi Yu Shanghai Shi Gong'an Ju Minhang Fenju Xingzheng Gong'an Qita Yishen Xingzheng Panjue Shu (上海鑫澄电信有限公司与上海市公安局闵行分局行政公安其他一审行政判决书) [Shanghai Xincheng Telecom Company, Ltd. and Shanghai Municipal Public Security Bureau Minhang Branch Administrative Public Security Other First Instance Administrative Judgment] China Judgements Online, (2017) Hu 0112 Xingchu 239 Hao ((2017) 沪0112行初239号) [2017 Shanghai First Instance Administrative Judgment No. 239] (Shanghai Minhang People's Ct., Mar. 8, 2018) [hereinafter Xincheng Telecom Co. v. Shanghai Minhang Public Security Bureau] (upholding the authority of public security bureau under Article 8 to conduct security inspections and upholding the punishment of Shanghai telecom company for violating Article 24 by failing to verify customers' real names before providing network access).

170. Xu Wangren Su Leiyang Shi Gong'an Ju Gong'an Xingzheng Chufa Yi An Yishen Xingzheng Panjue Shu (侀望仁诉耒阳市公安局公安行政处罚一案一审行政判决书) [Xu Wangren v. Leiyang City Public Security Bureau, Public Security Administrative Punishment First Instance Administrative Judgment] China Judgements Online, (2019) Xiang 8602 Xingchu 118 Hao ((2019) 湘8602行初118号) [2019 Hunan First Instance Administrative Judgment No. 8602] (Hengyang Ry. Transp. Ct., Sept. 26, 2019) [hereinafter Xu v. Leiyang Public Security Bureau].

information was stored for six months.[171] The court summarily rejected the plaintiff's arguments and found the evidence submitted by the public security bureau to be a sufficient basis for the warning.[172] In some of the previously cited administrative cases involving speech,[173] the plaintiff used forum websites to share their views—the punishment of a forum website in this instance thus makes it possible that online speech may be the real issue.[174] Forum websites, also known as BBS or the bulletin-board system, are a popular way for individuals to post online and share ideas,[175] though from the perspective of the Chinese government, their popularity has triggered concerns over possible uncontrolled speech.[176]

2. Criminal Cases: Strengthening Data Privacy and Security

The criminal cases applying the CSL demonstrate the State's overwhelming concern with data theft and fraud. Most of the cases demonstrate a straightforward conviction of the defendant and focus on CSL Articles 42 and 44 and the handling of personal information.[177] For example, in *Shanghai Xuhui District People's Procuratorate v. Xu*, the defendant was charged with imitating a popular education website to collect the names, phone numbers, and other personal information of over 8,000 individuals that were then shared with a for-profit

171. *Id.*

172. *Id.*

173. *See supra* Section II.C.1.

174. *See* Xiao Qiang, *The Internet: A Force to Transform Chinese Society?*, *in* CHINA'S TRANSFORMATIONS: THE STORIES BEYOND THE HEADLINES 129, 136 (Lionel M. Jensen & Timothy B. Weston eds., 2007) (explaining the popularity of forum websites and their role in providing a place for more open exchanges of views).

175. For more on the online forum (also known as the BBS, or bulletin-board system) and its predominance in China, see Liwen Jin, Chinese Online BBS Sphere: What BBS Has Brought to China 10–11 (Aug. 15, 2008) (M.S. thesis, Massachusetts Institute of Technology) (on file with Massachusetts Institute of Technology Libraries).

176. Early attitudes of Chinese citizens towards the BBS expressed hope at free speech possibilities. *See* Guobin Yang, *The Co-Evolution of the Internet and Civil Society in China*, 43 ASIAN SURV. 405, 416 (2003).

177. Cybersecurity Law, *supra* note 58, arts. 42, 44 ("Network operators must not disclose, tamper with, or destroy personal information they gather; and, absent the consent of the person whose information was collected, must not provide personal information to others . . . Network operators shall adopt technical measures and other necessary measures to ensure the security of personal information they gather and to prevent personal information from leaking, being destroyed, or lost" and "Individuals or organizations must not steal or use other illegal methods to acquire personal information, and must not unlawfully sell or unlawfully provide others with personal information.").

school.[178] The court cited to CSL Articles 42 and 44,[179] along with the Criminal Law Articles 253 and 67,[180] to impose a three-year prison sentence and fine of 300,000 RMB (approx. $4,600 USD).[181] The three-year sentence is likely derived from Article 253 of the Criminal Law, which allows a maximum sentence of three years, and demonstrates how the CSL may serve as a general basis for liability in conjunction with other laws.[182]

The criminal cases also highlight the debate around what constitutes "personal information" within the meaning of the CSL.[183] In *People v. Deng*, twenty-three defendants were charged with violating Article 253 of the Criminal Law[184] by buying and selling a high volume of e-mail addresses and passwords, including information belonging to foreign citizens.[185] The court analyzed whether e-mail addresses and passwords fell within the meaning of "personal information" in the Criminal Law and CSL Article 44, concluding that, because e-mail addresses "can be used to communicate with others, receive security verification codes, and can also be used to log-in to online games and e-commerce platforms," they constitute "personal information."[186] In a similar case, *People v. Lu*, the defendant, who allegedly stole and sold customer data, protested that mobile numbers could not, by themselves, identify a natural person and thus were not "personal

178. Xu Moumou Qinfan Gongmin Geren Xinxi Yishen Xingshi Fudai Minshi Panjue Shu (徐某某侵犯公民个人信息一审刑事附带民事判决书) [Xu Infringement on Citizens' Personal Information First Instance Criminal and Civil Judgment] China Judgements Online, (2019) Hu 0104 Xingchu 1244 Hao ((2019) 沪0104刑初1244号) [2019 Shanghai First Instance Criminal Judgment No. 1244] (Xuhui People's Ct., Dec. 25, 2019) [hereinafter People v. Xu].

179. Cybersecurity Law, *supra* note 58, arts. 42, 44.

180. Criminal Law, *supra* note 68, art. 253 (prohibiting "any staff member of . . . an entity in such a field as . . . education . . . illegally provid[ing] personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others . . .").

181. People v. Xu. *supra* note 178.

182. Criminal Law, *supra* note 68, art. 253; Cybersecurity Law, *supra* note 58, art. 70.

183. *See, e.g.*, Cybersecurity Law, *supra* note 58, art. 44.

184. Criminal Law, *supra* note 68, art. 253.

185. Deng Fei, Ai Jia Deng Qinfan Gongmin Geren Xinxi Yishen Xingshi Panjue Shu (邓飞、艾佳等侵犯公民个人信息一审刑事判决书) [Deng Fei, Ai Jia et al. Infringement on Citizens' Personal Information First Instance Criminal Judgment] China Judgements Online, (2018) Yu 0229 Xingchu 2 Hao ((2018) 渝0229刑初2号) [2018 Chongqing First Instance Criminal Judgment No. 2] (Chengkou Cnty. Ct., Feb. 15, 2019) [hereinafter People v. Deng et al.].

186. *Id.*

information."[187] The court, however, concluded that mobile phone numbers fell within the definition of personal data because they were associated with a person.[188] These select criminal cases demonstrate the application of the CSL to enforce privacy protections and protect citizens from fraud in the commercial sphere.

3. Civil Cases: Defining Cybersecurity Rights and Responsibilities

The civil cases, spanning a wide range of disputes including defamation, copyright infringement, contract breach, and tort liability cases, illustrate the courts' evolving understanding of cybersecurity, particularly regarding powerful technology companies. The cases also demonstrate savvy behavior from plaintiffs seeking recovery when the direct perpetrator of a wrong is unknown—and, unlike the administrative cases, the plaintiffs actually prevail in some of these cases.[189]

First, the civil cases interpret Article 24's real-name requirement.[190] When plaintiffs are unable to identify online perpetrators of defamation, copyright violations, or fraud, they sue the online platform and assert that the website is liable for not verifying the identity of the online perpetrator.[191] In the defamation case *Wu v. Jinan Yiyong Electronic Co.*, the plaintiff claimed that the defendant company hosted a forum website where an anonymous user published a post that injured the plaintiff's reputation.[192] In addition to citing to the Tort Liability

187. *See* Shi Mou Qinfan Gongmin Geren Xinxi Yishen Xingshi Panjue Shu (石某侵犯公民个人信息一审刑事判决书) [Shi Infringement on Citizens' Personal Information First Instance Criminal Judgment] China Judgements Online, (2018) Lu 1321 Xingchu 89 Hao ((2018) 鲁1321刑初89号) [2018 Shandong First Instance Criminal Judgment No. 89] (Yinan Cnty. Ct., Oct. 10, 2018) [hereinafter People v. Lu] (holding that a phone number is considered "personal information").

188. *Id.*

189. Out of approximately 32 civil cases citing to the CSL in the holding, the plaintiffs won 19 cases China Judgments Online, *supra* note 143.

190. Cybersecurity Law, *supra* note 58, art. 24 ("Network operators . . . shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.").

191. *See, e.g.*, Wu Dianhe Yu Jinan Yiyong Dianzi Youxian Gongsi Mingyu Quan Jiufen Yishen Minshi Panjue Shu (吴殿河与济南易用电子有限公司名誉权纠纷一审民事判决书) [Wu Dianhe and Jinan Yiyong Electronics Company, Ltd.'s Reputation Dispute First Instance Civil Judgment] China Judgements Online, (2019) Lu 0181 Minchu 289 Hao ((2019) 鲁0181民初289号) [2019 Shandong First Instance Civil Judgment No. 289] (Zhangqiu Dist. People's Ct., Nov. 6, 2019) [hereinafter Wu v. Jinan Yiyong Electronics Co.].

192. *Id.*

Law Article 36[193] and several regulations, the court applied Article 24 of the CSL to find that the defendant website should have provided information about the anonymous user upon the plaintiff's request.[194] In *Huang v. Nanjing Lanjingren Network Technology Co.*, the court held the website liable for allegedly defamatory speech against the plaintiff because the website did not verify the identity of the person that posted the information.[195] In several copyright cases, the courts held the defendant website liable for copyright infringement when the website failed to record the real name of the user that uploaded the infringing content.[196] In *Da'an Nenjiang Shipbuilding Co. v. Shaoxing*

193. Zhonghua Renmin Gongheguo Qinquan Zeren Fa (中华人民共和国侵权责任法) [Tort Liability Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010) art. 36, http://www.gov.cn/flfg/2009-12/26/content_1497435.htm [https://perma.cc/ZB74-T8Z4], *translated in Tort Liability Law of the People's Republic of China*, NAT'L. PEOPLE'S CONG., http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620761.htm [https://perma.cc/3B8E-EHBL] (last visited Mar. 1, 2021) [hereinafter Tort Liability Law].

194. Wu v. Jinan Yiyong Electronics Co., *supra* note 191 (citing Cybersecurity Law, *supra* note 58, art. 24).

195. Huang Shengli, Huang Fengzhi Deng Yu Nanjing Lajingren Wangluo Keji Youxian Gongsi Mingyu Quan Jiufen Yishen Minshi Panjue Shu (黄胜利、黄奉志等与南京蓝鲸人网络科技有限公司名誉权纠纷一审民事判决书) [Huang Shengli, Huang Fengzhi et al. and Nanjing Lanjingren Network Technology Company Ltd.'s Reputation Dispute First Instance Civil Judgment] China Judgements Online, (2017) Min 0581 Minchu 4000 Hao ((2017) 闽0581民初4000号) [2017 Fujian First Instance Civil Judgment No. 4000] (Shishi City People's Ct., Oct. 23, 2017) [hereinafter Huang et al. v. Nanjing Lanjingren Network Technology Co.] (holding that defendant website had an obligation to record the real name of the user).

196. *See, e.g.*, Beijing Yituhoude Wangluo Keji Youxian Gongsi Yu Shenzhen Shi Yilan Wangluo Gufen Youxian Gongsi Qinhai Zuopin Xinxi Wangluo Chuanbo Quan Jiufen Yishen Minshi Panjue Shu (北京壹图厚德网络科技有限公司与深圳市一览网络股份有限公司侵害作品信息网络传播权纠纷一审民事判决书) [Beijing Yituhoude Network Technology Company, Ltd. and Shenzhen Yilan Network Company, Ltd.'s Infringement of the Right to Disseminate Information Online Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Jing 0491 Minchu 35516 Hao ((2019) 京0491民初35516号) [2019 Beijing First Instance Civil Judgment No. 35516] (Beijing Internet Ct., Nov. 12, 2019) [hereinafter Beijing Yituhoude Network Technology Co. v. Shenzhen Yilan Network Co.] (holding that defendant website bears the copyright violation liability for failing to confirm the real name of the user that uploaded the infringing article); *see also* Beijing Nuopule Wenhua Chuanbo Youxian Gongsi Yu Guangzhou Kugou Jisuanji Keji Youxian Gongsi Qinhai Zuopin Xinxi Wangluo Chuanbo Quan Jiufen Yishen Minshi Panjue Shu (北京诺普乐文化传播有限公司与广州酷狗计算机科技有限公司侵害作品信息网络传播权纠纷一审民事判决书) [Beijing Nuopule Culture Communication Company, Ltd. and Guangzhou Kugou Computer Technology Company, Ltd.'s Infringement of the Right to Disseminate Information Online Dispute, First Instance Civil Judgment] China Judgements Online, (2020) Yue 0192 Minchu 19242 Hao ((2020) 粤0192民初19242号) [2020 Guangdong First Instance Civil Judgment No. 19242] (Guangzhou Internet Ct., June 28, 2020)

Radio Network Co., the plaintiff company sued both a competitor and a business directory website for listing the legal representative of the defendant competitor under the name of the plaintiff company in the directory.[197] Because the defendant website failed to verify the business's credentials and real name when listing the information and the plaintiff could not prove that the competitor fraudulently submitted the information, the court found the website solely liable.[198] The court, citing to CSL Articles 12, 24 and 47 and Tort Liability Law Article 36, required the defendant website to pay 40,000 RMB (approx. $6,200 USD) and make a public apology.[199]

The courts are not always consistent in interpreting Article 24's requirements. In *Zhang v. Shenzhen Xin Aide Technology Co.*, the plaintiff sought reimbursement for an allegedly counterfeit tablet

---

[hereinafter Beijing Nuopule Culture Communication Co. v. Guangzhou Kugou Computer Technology Co.]; Qingheyuan (Beijing) Shangye Guwen Fuwu Youxian Gongsi Yu Guangzhou Yuzheng Wangluo Keji Youian Zhuzuoquan Quan Shu, Qinquan Jiufen Yishen Minshi Panjue Shu (清和源（北京）商业顾问服务有限公司与广州裕正网络科技有限公司著作权权属、侵权纠纷一审民事判决书) [Qingheyuan (Beijing) Business Consulting Service Company, Ltd. and Guangzhou Yuzheng Network Technology Company, Ltd.'s Copyright Ownership and Infringement Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Jing 0491 Minchu 7434 Hao ((2019) 京0491民初7434号) [2019 Beijing First Instance Civil Judgment No. 7434] (Beijing Internet Ct., June 25, 2019) [hereinafter Qingheyuan Business Consulting Service Co. v. Guangzhou Yuzheng Network Technology Co.]; Wangzhiyi Xinxi Jishu (Beijing) Youxian Gongsi Yu Guangzhou Lizhi Wangluo Jishu Youxian Gongsi Qinhai Zuopin Xinxi Wangluo Chuanbo Quan Jiufen Yishen Minshi Panjue Shu (网之易信息技术（北京）有限公司与广州荔支网络技术有限公司侵害作品信息网络传播权纠纷一审民事判决书) [NetEase Information Technology Company (Beijing) Ltd. and Guangzhou Lizhi Network Technology Company, Ltd.'s Infringement of the Right to Disseminate Information Online Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Yue 0192 Minchu 24360 Hao ((2019) 粤0192民初24360号) [2019 Guangdong First Instance Civil Judgment No. 24360] (Guangzhou Internet Ct., Feb. 27, 2020) [hereinafter NetEase Information Technology Co. v. Guangzhou Lizhi Network Technology Co.].

197. Da'an Shi Nenjiang Chuanbo Xiuzao Youxian Zeren Gongsi Yu Jilin Sheng Da'an Chuanbo Zhizao Youxian Gongsi, Shaoxing Dianbo Wangluo Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Yishen Minshi Panjue Shu (大安市嫩江船舶修造有限责任公司与吉林省大安船舶制造有限公司、绍兴电波网络有限公司不正当竞争纠纷一审民事判决书) [Da'an Nenjiang Shipbuilding Company, Ltd., Jilin Province Da'an Shipbuilding Company, Ltd., Shaoxing Radio Network Company Ltd., Unfair Competition Dispute, First Instance Civil Judgment] China Judgements Online (2018) Ji 08 Minchu 14 Hao ((2018) 吉08民初14号) [2018 Jilin First Instance Civil Judgment No. 14] (Baicheng City Interm. People's Ct., June 28, 2018) [hereinafter Da'an Nenjiang Shipbuilding Co. v. Jilin Province Da'an Shipbuilding Co.].

198. *Id.*

199. *Id.*

purchased online.[200] The court instead determined that because the plaintiff used a false online name to purchase the tablet, the plaintiff was ineligible to bring the claim.[201] The court described the purposes of the real-name requirement as facilitating "online integrity, online transaction security, and forming a positive social atmosphere" (网络诚信、网络交易安全、形成良好社会风气).[202] This case demonstrates how the real-name requirement restricts the behavior of both plaintiffs and defendants in the civil system. It is also unclear exactly what steps websites should take to avoid liability. In *Aoyin Technology Co. v. Zhenjiang Speedy Computer Technology Network Co.*, the court held that to satisfy CSL Article 24, the defendant merely needed to record the real name of the allegedly offending user without actually sharing it with the plaintiff.[203] The court noted that the offending user's personal information could not be shared with the plaintiff simply upon the plaintiff's request.[204] In a similar case, the court held that deleting the offending information at the plaintiff's request and recording the name of the user in the back-end satisfied the requirements of Article 24.[205] But in the *Jinan Yiyong Electronic* case,

200. Zhang Chong Yu Shenzhen Shi Xin Aide Keji Youxian Gongsi Wangluo Gouwu Hetong Jiufen Minshi Caiding Shu (张冲与深圳市信爱德科技有限公司网络购物合同纠纷一审民事裁定书) [Zhang Chong and Shenzhen Xin Aide Technology Company, Ltd.'s E-Commerce Contract Dispute, First Instance Civil Judgment] China Judgements Online , (2017) Lu 0302 Minchu 2379 Hao ((2017) 鲁0302民初2379号) [2017 Shandong First Instance Civil Judgment No. 2379] (Zichuan District People's Ct., Oct. 10, 2017) [hereinafter Zhang v. Shenzhen Xin Aide Technology Co.].

201. *Id.*

202. *Id.*

203. Aoyin Keji (Zhenjiang) Youxian Gongsi Yu Zhenjiang Shi Chaosu Jisuanji Keji Wangluo Youxian Zeren Gongsi Wangluo Qinquan Zeren Jiufen Yishen Minshi Panjue Shu (奥音科技（镇江）有限公司与镇江市超速计算机科技网络有限责任公司网络侵权责任纠纷一审民事判决书) [Aoyin Technology (Zhenjiang) Company, Ltd., Zhenjiang Chaosu Computer Technology Network Company, Ltd. and Zhenjiang Chaosu Computer Technology Network Company, Ltd.'s Network Infringement Dispute, First Instance Civil Judgment] China Judgements Online, (2018) Su 1191 Minchu 3023 Hao ((2018) 苏1191民初3023号) [2018 Jiangsu First Instance Civil Judgment No. 3023] (Zhenjiang Economic Development Zone People's Ct., Dec. 24, 2018) [hereinafter Aoyin Technology Co. v. Zhenjiang Chaosu Technology Co.].

204. *See id.* (holding that defendant satisfied Art. 24 obligation by recording real name of user but did not have an obligation to share the name and contact information with the plaintiff without the consent of the user, also clarifying that the defendant does not have a legal responsibility to review all articles posted on the website).

205. *See* Yiwu Tianxiang Yiliao Dongfang Yiyuan Yu Shijiu Lou Wangluo Gufen Youxian Gongsi Mingyu Quan Jiufen Yishen Minshi Panjue Shu (义乌天祥医疗东方医院与十九楼网络股份有限公司名誉权纠纷一审民事判决书) [Yiwu Tianxiang Medical Eastern Hospital and 19th Floor Network Company, Ltd.'s Reputation Infringement Dispute, First Instance Civil Judgment] China Judgements Online, (2018)

the court held the defendant company liable after they refused to provide information about the offending user to the plaintiff.[206] These inconsistent interpretations demonstrate both the vagueness of the CSL and the discretion courts have to interpret the law.

Second, the civil cases illustrate how plaintiffs are looking to the CSL in cases of data theft and fraud to hold websites accountable. The main articles cited are Articles 40, 41, and 42.[207] In *Shen v. Shanghai Ctrip Business Co., Ltd.*, a plaintiff was defrauded out of over 100,000 RMB (approx. $15,400 USD) after booking flights via Ctrip, China's largest travel website,[208] and subsequently sued Ctrip for her losses.[209] Ctrip argued that the plaintiff's information had been shared with multiple parties, including the airline, and that the plaintiff could not prove that Ctrip had in fact leaked the data.[210] The court, however, determined that the plaintiff's evidence, showing the short period of time from purchasing the airline ticket to being defrauded, was sufficient to shift the burden to Ctrip to prove that they had not negligently leaked the data.[211] The court noted that because Ctrip, as a prominent travel services provider, had benefited from the internet, it also bore responsibility for harms generated by the website.[212] The holding, citing to CSL Articles 40 and 41 along with the Tort Liability Law Article 37, required Ctrip to compensate the plaintiff for 50,000 RMB (approx.

Zhe 0782 Minchu 9873 Hao ((2018) 浙0782民初9873号) [2018 Zhejiang First Instance Civil Judgment No. 9873] (Yiwu People's Ct., Sept. 5, 2018) [hereinafter Yiwu Tianxiang Medical Eastern Hospital v. 19th Floor Network Co.] (holding that defendant network service provider fulfilled legal duty by recording the real name of a user on the back-end and deleting the offending posts criticizing a local hospital).

206. Wu v. Jinan Yiyong Electronics Co., *supra* note 191.

207. Cybersecurity Law, *supra* note 58, art. 40 ("Network operators shall strictly maintain the confidentiality of user information they collect, and establish and complete user information protection systems"); *id.* art. 41 ("Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall…obtain the consent of the persons whose data is gathered . . . "); *id.* art. 42 ("Network operators must not disclose, tamper with, or destroy personal information they gather . . .").

208. *Most Innovative Companies: Ctrip*, FAST COMPANY, https://www.fastcompany.com/company/ctrip [https://perma.cc/L59C-EPLB] (last visited Nov. 13, 2021).

209. Shen Jin Yu Zhifubao (Zhongguo) Wangluo Jishu Youxian Gongsi Deng Qinquan Zeren Jiufen Yishen Minshi Panjue Shu (申瑾与支付宝（中国）网络技术有限公司等侵权责任纠纷一审民事判决书) [Shen Jin, Alipay (China) Network Technology Company, Ltd., and Others Tort Liability Dispute First Instance Civil Judgment] China Judgements Online, (2018) Jing 0105 Minchu 36658 Hao ((2018) 京0105民初36658号) [2018 Beijing Civil Judgment No. 36658] (Chaoyang District People's Ct., Dec. 29, 2018) [hereinafter Shen v. Alipay et al.].

210. *Id*.

211. *Id*.

212. *Id*.

$7,700 USD).[213] This case demonstrates how, even if the plaintiff cannot prove exactly what actions the defendant took to leak the data, the court may hold the website responsible for the plaintiff's losses associated with fraud and leaked data.[214]

The cases also show how the courts are strictly defining data privacy protections for consumers. In *Yu v. Tmall*, the plaintiff sued the Leyou Dakang store as well as Alipay, China's largest mobile payments provider,[215] Taobao, China's largest online marketplace,[216] and Tmall, China's largest business-to-consumer website.[217] The plaintiff alleged that the defendants violated the CSL's privacy protections by "default" authorizing the sharing of the plaintiff's transaction at the Leyou store with Taobao and Tmall without the plaintiff's express consent.[218] The companies argued, based on Article 76 of the CSL, that there is a difference between personal and non-personal user information, and that the allegedly shared information was not personal information.[219] The court held that the unique user identification code shared between the defendants constituted personal information within the meaning of the CSL.[220] Interestingly, the plaintiff sought only symbolic relief in this case—a public apology and symbolic damages of 1 RMB.[221] The court ultimately granted only the symbolic damages and did not require the companies to issue public apologies.[222] This case demonstrates the plaintiff's concern with privacy protections vis-

213. *Id*.

214. *Id*.

215. John Heggestuen, *Alipay Overtakes PayPal as the Largest Mobile Payments Platform in the World*, BUS. INSIDER (Feb. 11, 2014, 8:32 AM), https://www.businessinsider.com/alipay-overtakes-paypal-as-the-largest-mobile-payments-platform-in-the-world-2014-2 [https://perma.cc/H2GU-5MSL].

216. *The Everything Creditor*, THE ECONOMIST (June 6, 2015), https://www.economist.com/china/2015/06/04/the-everything-creditor [https://perma.cc/YF76-RJCS].

217. *Tmall: An Introduction to the World's Largest e-Commerce Marketplace*, EXPORT NOW, https://www.exportnow.com/2014/06/tmall-introduction-worlds-largest-e-commerce-marketplace Nov. 13[https://perma.cc/3XQB-28YN] (.

218. Yu Yanbin Yu Zhejiang Tian Mao Wangluo Youxian Gongsi Deng Wangluo Qinquan Zeren Jiufen Yishen Minshi Panjue Shu (俞延彬与浙江天猫网络有限公司等网络侵权责任纠纷一审民事判决书) [Yu Yanbin, Zhejiang Tmall Network Company, Ltd. and Others' Network Infringement Dispute, First Instance Civil Judgment] China Judgements Online, (2018) Jing 0108 Minchu 13661 Hao ((2018) 京0108民初13661号) [2018 Beijing First Instance Civil Judgment No. 13661] (Beijing Haiding Internet Ct., Dec. 10, 2019) [hereinafter Yu v. Tmall].

219. *Id.*

220. *Id*.

221. *Id.*

222. *Id.*

à-vis the large technology companies that dominate China's marketplace. In *Anhui Meijing Information Technology Company v. Taobao*, the court concluded that Taobao's use of aggregated, anonymized customer information in a "big data" tool did not constitute a violation of data privacy.[223] These decisions demonstrate how the CSL's data privacy protections are playing out in practice, especially in China's growing technology industry.

Third, these cases provide clues for companies on how to protect themselves from liability for fraudulent activity that takes place using data from their websites. For example, the defendant company in *Xu v. Guangzhou Huaduo Network Technology Co.* posted warnings on the website reminding users not to scan QR codes received by unknown third-parties and generally warning against fraud.[224] The court held that these measures satisfied the requirements of CSL Articles 9 and 10[225] and declined to hold the defendant liable for the plaintiff's losses of 18,000 RMB (approx. $2,700 USD).[226] In a similar case, the court noted the defendant company's efforts to warn customers about

223. Anhui Meijing Xinxi Keji Youxian Gongsi, Taobao (Zhongguo) Ruanjian Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Zaishen Shencha Yu Shenpan Jiandu Minshi Caiding Shu
(安徽美景信息科技有限公司、淘宝（中国）软件有限公司不正当竞争纠纷再审审查与审判监督民事裁定书) [Anhui Meijing Information Technology Company Ltd., and Taobao (China) Software Company, Ltd. Unfair Competition Dispute, Civil Rehearing Judgment] China Judgements Online, (2019) Zhe Minshen 1209 Hao ((2019) 浙民申1209号) [2019 Zhejiang Rehearing Civil Judgment No. 1209] (Zhejiang High People's Ct., Dec. 10, 2019) [hereinafter Anhui Meijing Information Technology Company v. Taobao].

224. Xu Changfu Yu Guangzhou Huaduo Wangluo Keji Youxian Gongsi Wangluo Fuwu Hetong Jiufen Yishen Minshi Panjue Shu
(徐常富与广州华多网络科技有限公司网络服务合同纠纷一审民事判决书) [Xu Changfu and Guangzhou Huaduo Network Technology Company, Ltd., Network Service Contract Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Yue 0192 Minchu 35087 Hao ((2019) 粤0192民初35087号) [2019 Guangdong Civil Judgment No. 35087] (Guangzhou Internet Ct., Nov. 11, 2019) [hereinafter Xu v. Guangzhou Huaduo Network Technology Co.].

225. Cybersecurity Law, *supra* note 58, art. 9 ("Network operators carrying out business and service activities must follow laws and administrative regulations, respect social morality, abide by commercial ethics, be honest and credible, perform obligations to protect cybersecurity, accept supervision from the government and public, and bear social responsibility."); *id.* art. 10:

The construction and operation of networks, or the provision of services through networks, shall be done: in accordance with the provisions of laws and administrative regulations, and with the mandatory requirements of national standards; adopting technical measures and other necessary measures to safeguard cybersecurity and operational stability; effectively responding to cybersecurity incidents; preventing cybercrimes and unlawful activity; and preserving the integrity, secrecy, and usability of online data.

226. Xu v. Guangzhou Huaduo Network Technology Co., *supra* note 224.

scammers on the site, including anti-fraud videos, security tips on the webpage, and sharing information about common fraudulent schemes.[227]

III. FROM THE CYBERSECURITY LAW TO CHINA'S ALTERNATE VISION

The administrative, criminal, and civil cases analyzed in Part II provide a window into the ongoing interpretation of the CSL and how expectations and requirements for individuals and companies under the law are changing. In a globalized context where China's cybersecurity rules are increasingly exerting cross-border influence, these cases reveal new insights regarding China's vision of cybersecurity and the policy concerns driving China's cybersecurity laws.

A. Insights into the Chinese Judicial System

To date, the court cases published online not only provide information about the CSL, but also highlight several notable trends concerning the judicial system itself. First, the available court judgments generally do not cite to the CSL as a standalone legal basis for the judgment.[228] Rather, they cite to the CSL in conjunction with another

227. *See* Deng Shijin Yu Guangzhou Huaduo Wangluo Keji Youxian Gongsi Wangluo Fuwu Hetong Jiufen Yishen Minshi Panjue Shu (邓仕锦与广州华多网络科技有限公司网络服务合同纠纷一审民事判决书) [Deng Shijin and Guangzhou Huaduo Network Technology Company Ltd.'s Network Service Contract Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Yue 0192 Minchu 35106 Hao ((2019) 粤0192民初35106号) [2019 Guangdong Civil Judgment No. 35106] (Guangzhou Internet Ct., Nov. 13, 2019) [hereinafter Deng v. Guangzhou Huaduo Network Technology Co.].

228. *See, e.g.*, Qian v. Rudong Public Security Bureau, *supra* note 160; Guangzhou Wangyi Jisuanji Xitong Youxian Gongsi Yu Shanxi Yi Liu Keji Youxian Gongsi Qinhai Zuopin Xinxi Wangluo Chuanbo Quan Jiufen Yishen Minshi Panjue Shu (广州网易计算机系统有限公司与山西易流科技有限公司侵害作品信息网络传播权纠纷一审民事判决书) [Guangzhou NetEase Computer System Company Ltd., and Shanxi Yiliu Technology Company Ltd.'s Internet Dissemination Right Infringement Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Yue 0192 Minchu 22718 Hao ((2019) 粤0192民初22718号) [2019 Guangdong Civil Judgment No. 22718] (Guangzhou Internet Ct., Mar. 16, 2020) [hereinafter Guangzhou NetEase Computer System Co. v. Shanxi Yiliu Technology Co.]; Chen Guoxing Yu Zhejiang Taobao Wangluo Youxian Gongsi Caichan Sunhai Peichang Jiufen Yishen Minshi Panjue Shu (陈国星与浙江淘宝网络有限公司财产损害赔偿纠纷一审民事判决书) [Chen Guoxing and Zhejiang Taobao Network Company, Ltd.'s Property Damage Compensation Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Hu 0117 Minchu 6495 Hao ((2019) 沪0117民初6495号) [2019 Shanghai Civil Judgment No. 6495] (Songjiang Dist. People's Ct., May 31, 2019) [hereinafter Chen v. Taobao].

more specific regulation or judicial interpretation, such as the Regulations on the Security Protection of Computer Information Systems[229] and the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Endangering the Security of Computer Information Systems.[230] The courts also rely on core statutes such as the Tort Liability Law[231] and the Criminal Law.[232] In cases involving online activity and network providers, the CSL operates in conjunction with these statutes and regulations to provide a basis for liability. The courts will likely continue to refer to other regulations or statutes along with the CSL for administrative, civil, and criminal cases since there are core statutes defining the law in those areas, such as the Administrative Litigation Law and the Criminal Law. In light of this constant stream of regulations and interpretations, it is critical

229. Regulation issued in 1994, cited in Xu v. Leiyang Public Security Bureau, *supra* note 170; Zhonghua Renmin Gongheguo Jisuanji Xinxi Xitong Anquan Baohu Tiaoli (中华人民共和国计算机信息系统安全保护条例) [Regulations of the People's Republic of China on the Security Protection of Computer Information Systems] (promulgated by the Standing Comm. Nat'l People's Cong., Feb. 18, 1994, effective Feb. 18, 1994), http://www.gov.cn/flfg/2005-08/06/content_20928.htm [https://perma.cc/BK7D-HG8P].

230. *See* Ma Chunyu, Mo Xiyong Tigong Qinru, Feifa Kongzhi Jisuanji Xinxi Xitong Chengxu, Gongju Zui Yishen Xingshi Panjue Shu (马春雨、莫锡勇提供侵入、非法控制计算机信息系统程序、工具罪一审刑事判决书) [Ma Chunyu, Mo Xiyong Illegally Intruding and Controlling Computer Information System Programs and Tools First Instance Criminal Judgment] China Judgements Online, (2019) Su 1091 Xingchu 157 Hao ((2019) 苏1091刑初157号) [2019 Jiangsu First Instance Criminal Judgment No. 157] (Yangzhou Economic & Technological Development Zone People's Ct., Dec. 10, 2019) [hereinafter People v. Ma] (citing the Supreme People's Court judicial interpretation); Liang Gao Guanyu Banli Weihai Jisuanji Xinxi Xitong Anquan Xingshi Anjian Yingyong Falu Ruogan Wenti De Jieshi, Fashi (2011) Yi Jiu Hao (两高关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释, 法释(2011) 19号) [Interpretation of the Supreme People's Court and the Supreme People's Court on Several Issues Concerning the Application of Law in Handling Criminal Cases Endangering the Security of Computer Information Systems, Judicial Interpretation No. 19 (2011)] (promulgated by the Judicial Comm. Sup. People's Ct., July 11, 2011, effective Sept. 1, 2011), http://www.court.gov.cn/zixun-xiangqing-7494.html [https://perma.cc/PZM4-D83L].

231. *See, e.g.*, Zhou Yuchan, Guangdong Kuai Ke Dianzi Shangwu Youxian Gongsi Wangluo Qinquan Zeren Jiufen Ershen Minshi Panjue Shu (周裕婵、广东快客电子商务有限公司网络侵权责任纠纷二审民事判决书) [Zhou Yuchan and Guangdong Kuaike Electronic Commerce Company, Ltd. Online Tort Liability Dispute, Second Instance Civil Judgment] China Judgements Online, (2019) Yue 03 Minzhong 3954 Hao ((2019) 粤03民终3954号) [2019 Guangdong Civil Judgment No. 3954] (Shenzhen Interm. People's Ct., May 5, 2019) [hereinafter Zhou v. Guangdong Kuaike Electronic Commerce Co.] (citing Tort Liability Law).

232. *See, e.g.*, People v. Deng et al., *supra* note 185 (citing Criminal Law).

to continue examining these rules to understand how China's approach to cybersecurity is evolving.[233]

Second, the civil cases, in particular, illustrate creative arguments for providing compensation to victims when the direct perpetrator of a wrong is unknown.[234] Civil litigants seek relief from a website or internet company, and in many cases the court actually grants relief to the beleaguered plaintiffs.[235] The CSL and its real-name requirement provide a convenient avenue for the courts to compensate plaintiffs injured due to data breaches and fraud, copyright infringement, and the publication of defamatory articles online when the actual perpetrator is unknown.[236] This is consistent with the pattern of judges providing compensation to victims in tort cases and, in some cases, even overlooking the legal provisions to provide compensation.[237]

Third, the court judgments illustrate the emerging role of internet courts. Multiple civil judgments come from the Hangzhou,[238] Beijing,[239] and Guangzhou Internet Courts[240]—where all proceedings,

233. SACKS & LI, *supra* note 15.

234. *See, e.g.*, NetEase Information Technology Co. v. Guangzhou Lizhi Network Technology Co., *supra* note 196.

235. *See, e.g.*, Shen v. Alipay et al., *supra* note 209.

236. *See, e.g.*, NetEase Information Technology Co. v. Guangzhou Lizhi Network Technology Co., *supra* note 196; Qingheyuan Business Consulting Service Co. v. Guangzhou Yuzheng Network Technology Co., *supra* note 196.

237. Liebman, *supra* note 73, at 200; *See, e.g.*, Shen v. Alipay et al., *supra* note 209.

238. Guangdong Zhong Ao Wuye Guanli Youxian Gongsi Yu Li Pengbo, Shijiu Lou Wangluo Gufen Youxian Gongsi Mingyu Quan Jiufen Yishen Minshi Panjue Shu (广东中奥物业管理有限公司与李鹏博、十九楼网络股份有限公司名誉权纠纷一审民事判决书) [Guangdong Zhong Ao Property Management Company, Ltd. and Nineteenth Floor Network Company, Ltd.'s Reputation Right Dispute, First Instance Civil Judgment] China Judgements Online, (2017) Zhe 0192 Minchu 691 Hao ((2017) 浙0192民初691号) [2017 Zhejiang Civil Judgment No. 691] (Hangzhou Internet Ct., Feb. 24, 2018) [hereinafter Guangdong Zhong Ao Property Management Co. v. Nineteenth Floor Network Co.].

239. Qingheyuan Business Consulting Service Co. v. Guangzhou Yuzheng Network Technology Co., *supra* note 196.

240. Zeli (Guangzhou) Xinxi Jishu Youxian Gongsi Yu Hangzhou Shi Chuo Xinxi Keji Youxian Gongsi Qinhai Zuopin Xinxi Wangluo Chuanbo Quan Jiufen Yishen Minshi Panjue Shu
(泽利（广州）信息技术有限公司与杭州时戳信息科技有限公司侵害作品信息网络传播权纠纷一审民事判决书) [Zeli (Guangzhou) Information Technology Company, Ltd. and Hangzhou Time Stamp Information Technology Company, Ltd.'s Information Dissemination Right Dispute, First Instance Civil Judgment] China Judgements Online, (2019) Yue 0192 Minchu 35104 Hao ((2019) 粤0192民初35104号) [2019 Guangdong Civil Judgment No. 35104] (Guangzhou Internet Ct., Mar. 16, 2020) [hereinafter Zeli Information Technology Co. v. Hangzhou Time Stamp Information Technology Co.]; NetEase Information Technology Co. v. Guangzhou Lizhi Network Technology Co., *supra* note 196.

including hearings, take place online and which first emerged in 2017.[241] These courts handle e-commerce-related disputes and any other disputes involving online activity, such as copyright infringement.[242] As the number of internet users and volume of e-commerce continues to grow, these courts are addressing a need for resolving internet-related disputes in a timely and efficient manner.[243] The internet courts also reflect a trend towards innovation in the Chinese judicial system, with the use of online hearings and, in limited instances, blockchain to authenticate evidence.[244]

B. Comparing Case Law with the Expectations for the Cybersecurity Law

The bigger question is what the application and interpretation of the CSL mean for China's vision of cybersecurity—both domestically and abroad. This section compares the predictions for the CSL with the interpretations of the cases examined in this Note. These cases illustrate how China's vision of cybersecurity is playing out in practice. First, the provisions of the CSL are in fact being enforced against domestic companies, though it remains unclear how consistently the law is enforced across companies. Second, the available cases indicate the State uses the CSL to target online dissent and stability-threatening speech. Third, relevant civil and criminal litigation reveal continued development of the meaning of online privacy for consumers—strong protections against data theft, fraud and infringement, but little to no protection vis-à-vis the government. These three trends hint at China's overarching vision for cybersecurity—one where online commercial activity flourishes, but digital anonymity and dissenting speech are strictly controlled.

241. Jason Tashea, *China's All-Virtual Specialty Internet Courts Look Set to Expand into Other Areas of the Law*, ABA JOURNAL (Nov. 1, 2019, 2:00 AM), https://www.abajournal.com/magazine/article/china-all-virtual-specialty-internet-courts [https://perma.cc/WK8Q-GL7S].

242. *Id*.

243. *Id.*

244. Vivien Chan & Anna Mae Koo, *Blockchain Evidence in Internet Courts in China: The Fast Track for Evidence Collection for Online Disputes*, LEXOLOGY (July 15, 2020), https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb [https://perma.cc/SM4V-54WN]; Mimi Zou, *"Smart Courts" in China and the Future of Personal Injury Litigation*, J. PERS. INJ. L. (forthcoming June 2020) (manuscript at 5).

1. Enforcement against Domestic Companies

While foreign analysis of the CSL focuses on the law's potential impact on foreign companies, including protectionism and forced data transfer, commentators are uncertain how China's enforcement of the CSL will impact locally operating companies.[245] The case law for this Note primarily focuses on domestic enforcement.[246] On a practical level, the administrative cases illustrate how the public security bureaus, or local police, are the key enforcers of the CSL. The case law is consistent with publicized incidents of CSL enforcement, which point to the public security bureaus carrying out cybersecurity inspections and issuing warnings and punishments for failure to comply.[247] It is notable that the public security bureaus, which have the power to arrest, detain, and interrogate individuals,[248] are enforcing the CSL, as opposed to an organization with more specialized, technical expertise.[249]

Another significant question is whether the CSL enhances domestic companies' cybersecurity. The administrative case law, while

245. Lee, *supra* note 1, at 94.

246. There were two main cases involving foreign parties out of the cases reviewed. The litigants only referenced the CSL in their arguments, but the court did not cite to the CSL in the holding. One was a plaintiff seeking to reverse a domestic commercial arbitration decision, arguing that due to the foreign nature of the contract (including data originating outside the People's Republic of China), the case should have been conducted as an international commercial arbitration case. *See* Shanghai Lianshang Wangluo Keji Youxian Gongsi Yu Shanghai Yiqi Lian Keji Youxian Gongsi Shenqing Chexiao Zhongcai Caijue Minshi Caiding Shu (上海连尚网络科技有限公司与上海亿起联科技有限公司申请撤销仲裁裁决民事裁定书) [Shanghai Lianshang Network Technology Company, Ltd. and Shanghai Yiqilian Technology Company, Ltd. Application for a Revocation of the Civil Arbitration Award] China Judgements Online, (2018) Jing 04 Minte 30 Hao ((2018) 京04民特30号) [2018 Beijing Civil Judgment No. 30] (Beijing Fourth Intermediate People's Ct., May 9, 2019). The other case involved a Japanese airline that was a third-party to a data privacy dispute. *See* Zan Yongnan Yu Zhongguo Guoji Hangkong Gufen Youxian Gongsi Hangkong Lüke Yunshu Hetong Jiufen Yishen Minshi Caiding Shu (昝勇男与中国国际航空股份有限公司航空旅客运输合同纠纷一审民事裁定书) [Zan Yongnan and Air China Airline Traveler Air Contract Dispute First Instance Civil Judgment] China Judgements Online, (2019) Jing 0113 Minchu 15922 Hao ((2019) 京04民初15922号) [2019 Beijing Civil Judgment No. 15922] (Beijing Shunyi District People's Ct., June 16, 2020).

247. Kenyon, *supra* note 141.

248. Suzanne E. Scoggins, *Policing Modern China*, 3 CHINA L. & SOC'Y REV. 79, 89, 106 (2018).

249. Lee, *supra* note 1, at 96 (noting that it is uncertain whether the government has the technical expertise to be creating and imposing cybersecurity standards, as opposed to private cybersecurity firms).

an extremely limited sample, includes cases of administrative punishments for failure to verify the real names of users before providing service (Article 24),[250] failure to store network logs for six months (Article 21),[251] and online data theft (Article 44).[252] The administrative punishments for the violations of Articles 24 and 21 were administrative orders to "make corrections" and an administrative warning respectively, while the penalty for violating Article 44 was a 50,000 RMB fine (approx. $7,700 USD).[253] Notably, real-name requirements and network storage requirements may not enhance the actual cybersecurity of local companies, [254] raising the question of why the public security bureaus are choosing to enforce these specific articles. It may very well be that more routine or technical infractions are not being challenged by plaintiffs, or are more difficult to enforce, thus not ending up in the court system. At the very least, these cases highlight that Articles 21, 24, and 44 are being enforced in practice.

The civil cases also show the involvement of some of China's largest technology companies, such as Ctrip[255] and Taobao.[256] The CAC has publicized enforcement against some of these large companies, perhaps as an example to others.[257] The courts generally seem willing to require these companies to pay damages to plaintiffs, such as requiring Ctrip to compensate a plaintiff for 50,000 RMB (approximately $7,700 USD) in losses.[258] However, this may say more about the court's desire to compensate the plaintiff than about the court's willingness to restrain the behavior of private companies. In *Yu v. Tmall*, a data privacy case where the plaintiff sued for purely symbolic

250. Xincheng Telecom Co. v. Shanghai Minhang Public Security Bureau, *supra* note 169.

251. Xu v. Leiyang Public Security Bureau, *supra* note 170.

252. Rugao Shi Gong'an Ju Yu Rugao Shi Yurui Jiancai Jingying Bu Xingzheng Fei Su Shencha Caiding Shu (如皋市公安局与如皋市宇瑞建材经营部行政非诉审查裁定书) [Rugao City Public Security Bureau, Rugao City Yurui Building Materials Management Department Administrative Non-Litigation Ruling] China Judgements Online, (2019) Su 0682 Xingshen 156 Hao ((2019) 苏0682行审156号) [2019 Jiangsu Administrative Judgment Re-Examination No. 156] (Rugao City People's Ct., Oct. 15, 2019) [hereinafter 2019 Jiangsu Administrative Judgment Re-Examination No. 156].

253. Xincheng Telecom Co. v. Shanghai Minhang Public Security Bureau, *supra* note 169; Xu v. Leiyang Public Security Bureau, *supra* note 170; 2019 Jiangsu Administrative Judgment Re-Examination No. 156, *supra* note 252.

254. *See* Lee & Liu, *supra* note 103, at 18–19 (discussing the failure of real-name requirements in South Korea as they actually *increased* security risks for hacking and internet fraud).

255. Shen v. Alipay et al., *supra* note 209.

256. Yu v. Tmall, *supra* note 218.

257. Chin, *supra* note 129.

258. Shen v. Alipay et al., *supra* note 209.

damages—a public apology and compensation of 1 RMB—the court only granted the 1 RMB compensation.[259] It did not require the companies to apologize, possibly indicating the court's reluctance to require a public gesture from a large company.[260] Similarly, the court declined to find that Taobao's business intelligence tool constituted a violation of personal information privacy.[261] While these cases are insufficient to draw full conclusions on the courts' posture towards technology companies regarding the CSL, the civil cases at the very least demonstrate how courts are balancing the companies' business objectives with the need to safeguard consumer privacy.[262]

2. Controlling Speech

Scholars expected the CSL to expand the surveillance state in the name of promoting a "stable" internet.[263] To the CCP, a stable internet is one without dissenting speech or any other type of expression that the State perceives as a threat.[264] The CCP itself has confirmed that "social stability" (社会稳定) is a critical component of China's vision of cybersecurity.[265] The CSL concretizes this expansive vision of cybersecurity in Article 12, which prohibits "spread[ing] information of violence and terror, false rumors, pornography, and other information that jeopardizes national security, public safety and social order."[266]

The available case law confirms that the State relies on the CSL as a legal basis for punishing speech that may threaten "social stability." While administrative law cases provide a narrow view into the scope of regulatory enforcement,[267] the existing cases demonstrate that

259. Yu v. Tmall, *supra* note 218.

260. *Id.*

261. Anhui Meijing Information Technology Company v. Taobao, *supra* note 223.

262. *See, e.g.*, Yu v. Tmall, *supra* note 218; Anhui Meijing Information Technology Company v. Taobao, *supra* note 223.

263. Lee, *supra* note 1, at 91; Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State*, 30 J. DEMOCRACY 53, 55 (2019).

264. *See* Lee, *supra* note 1, at 101 (noting the Chinese government's tight control over dissenting speech and ban on human rights activity perceived as threatening the regime or social stability).

265. Yu Hong, *Reading the 13th Five-Year Plan: Reflections on China's ICT Policy*, 11 INT'L J. COMMC'N 1755, 1767 (2017).

266. Cybersecurity Law, *supra* note 58, art. 12; Lee, *supra* note 1, at 92–93.

267. Enforcement of the CSL is carried out by the CAC and Ministry of Public Security, mainly through local public security bureaus. Administrative cases only arise when the party

the public security bureaus are interpreting Article 12 broadly, so as to arrest individuals who suggest petitioning or opposing the government via WeChat groups and online forums.[268] Where plaintiffs challenged the local governments' actions, the courts consistently sided with the public security bureaus, affirming their broad interpretation of Article 12.[269] Even in cases where the court did not specifically cite the CSL in its judgment (but where the public security bureau based its punishment on the CSL),[270] the court's upholding of the administrative action may be read as an implicit endorsement of the public security bureau's interpretation.

The case law also demonstrates that courts support administrative efforts to enforce the real-name requirement of Article 24, which has a powerful role in restricting online dissent. Many of the civil cases rely on the CSL to hold the website operator or internet company liable for the activity of an anonymous user on their website, on the ground that the website should have enforced the real-name requirement.[271] In the administrative cases, the public security bureaus are directly enforcing the real-name requirement.[272] To protect against legal liability, internet companies may become stricter about enforcing real-name registration and eliminating space for anonymous discussion.[273] This is consistent with the more recent adoption of specific regulations implementing real-name registration requirements,[274] a practice which was proposed as early as 2003.[275]

While the concept of cracking down on online speech in China is not new, the legal framing of restricting speech that threatens "social stability" *as a core component of cybersecurity* fundamentally expands

---

under administrative punishment *challenges* the punishment in court. For more on enforcement, see *supra* Section II.A.

268. *See, e.g.*, Gao v. Tiedong Public Security Bureau, *supra* note 110; *see also supra* Section II.C.1.

269. *See supra* Section II.C.1.

270. *See* Liang v. Huangmei Public Security Bureau, *supra* note 162 (upholding the public security bureau's decision to detain a plaintiff who published a post online about petitioning under CSL Articles 12 and 70).

271. *See, e.g.*, Guangzhou NetEase Computer System Co. v. Shanxi Yiliu Technology Co., *supra* note 228.

272. *See supra* Section II.C.1.

273. Qiang, *supra* note 263, at 60.

274. Melissa Cyrill, *New Curfew Rules, Real-Name Registration for China's Young Online Gamers*, CHINA BRIEFING (Nov. 7, 2019), https://www.china-briefing.com/news/china-online-gaming-curfew-minors-real-name-registration-system/ [https://perma.cc/B6B5-PSCA].

275. Lee & Liu, *supra* note 103, at 11.

the concept of cybersecurity as it exists in the West.[276] The framing of cybersecurity in the West focuses on both defensive and offensive capabilities towards cyber threats, while the Chinese government's framing involves information security and content regulation.[277] This expansive vision—coupled with weak protections for individual rights[278]—anticipates an internet with little room for dissent or anti-government speech even as online commerce otherwise flourishes.

3. Protecting Consumer Privacy

Commentators were mixed on the expected impact of the CSL on data privacy, with some stating that the CSL provides "unprecedented protection" of data privacy.[279] Yet others noted that the CSL "actively works against any preservation of privacy alone."[280] This confusion may be because the Western concept of privacy and data security focuses primarily on citizens' right to privacy vis-à-vis the State,[281] while privacy concerns in China (at least, those permitted by the government) are framed around e-commerce and fraud.[282]

The cases illustrate a growing concern to protect personal information and data privacy in both the civil and criminal context. For example, despite the lack of affirmative proof that Ctrip leaked the plaintiff's information, the court still held Ctrip liable for the eventual leakage of the plaintiff's information that led to the plaintiff being defrauded.[283] The court also sided with the plaintiff in the civil case where the plaintiff brought a privacy action against Taobao, Tmall, and

276. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 332 (2015).

277. *Id.*; *see also supra* note 5 and accompanying text.

278. *See supra* notes 164–168 and accompanying text.

279. Lee, *supra* note 1, at 101; *see also* Cybersecurity Law, *supra* note 58, art. 22.

280. Quinn, *supra* note 115, at 430.

281. Lee, *supra* note 1, at 101.

282. *In China, Consumers are Becoming More Anxious About Data Privacy*, ECONOMIST (Jan. 27, 2018), https://www.economist.com/china/2018/01/25/in-china-consumers-are-becoming-more-anxious-about-data-privacy [https://perma.cc/235Z-7Q2M]; Hao, *supra* note 136; Josh Rudolph, *Translation: Enough with Your Eavesdropping, WeChat*, CHINA DIGIT. TIMES (Oct. 20, 2020), https://chinadigitaltimes.net/2020/10/translation-enough-with-your-eavesdropping-wechat [https://perma.cc/524M-SHF3]; *see also* Hu Wen-Tao, *Wo Guo Geren Xinxi Yinsiquan Baohu Falü Cunzai de Wenti ji Sikao Yi yü Hulianwang Qiye Liyi Pingheng Wei Shijiao* (*我国个人信息隐私权保护法律存在的问题及思考以与互联网企业利益平衡为视角*) [*Problems Concerning the Legal Protection of the Right to Information Privacy and Possible Solutions in China in the Perspective of the Shared Interests of Internet Enterprises*], 48 (云南师范大学学报) J. YUNNAN NORMAL U. 92, 92 (2016).

283. Shen v. Alipay et al., *supra* at 209; *see supra* Section II.C.1.

Alipay for "default" sharing transaction data across multiple companies without the user's permission.[284] However, it declined to require the companies to issue public apologies.[285]

The criminal cases also reflect this focus on protecting personal information and preventing data leakage and fraud. The criminal cases heavily focus on the CSL provisions governing personal information storage and sharing: Articles 42, 43, and 44. These cases are also notable for imposing criminal liability for the sharing of user data such as phone numbers.[286]

Both the criminal and civil cases demonstrate the broader push to fight cybercrime and online fraud in China. The sharp rise in e-commerce fraud and data leakages has raised legitimate domestic concerns about data security within China.[287] The CSL, along with the recent Personal Information Protection[288] and Data Security Laws,[289] represent the State's legal response to these concerns. These statutes, along with the case law examined in this Note, show that consumers are certainly experiencing stronger privacy protections in online commerce.

What do these cases tell us about China's cybersecurity vision? First, the administrative cases involving domestic companies highlight that public security bureaus are driving local enforcement. The actual efficacy of the CSL in strengthening China's cybersecurity, at least based on these cases, is questionable given the provisions that the public security bureaus focus on, such as the real-name registration requirement. Second, the case law strongly affirms that China's vision of cybersecurity centers on restricting online speech that may threaten social stability, as interpreted by the State. Third, the cases

284. Yu v. Tmall, *supra* note 218.

285. *Id*.

286. People v. Lu, *supra* note 187; *see also* Guanyü Banli Qinfan Gongmin Geren Xinxi Xingshi Anjian Shiyong Falü Ruogan Wenti De Jieshi (关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释) [Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing Citizens' Personal Information] (promulgated by the Sup. People's Ct., Mar. 3, 2017, effective June 1, 2017), https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml [https://perma.cc/MT9V-XSSF].

287. Laurie Chen, *China Wakes up to Wide Web of Online Data Leaks and Privacy Concerns*, SOUTH CHINA MORNING POST (Jan. 27, 2020), https://www.scmp.com/news/china/society/article/3047186/china-wakes-wide-web-online-data-leaks-and-privacy-concerns [https://perma.cc/35YE-6JV7]; Ron Cheng, *Cybercrime in China: Online Fraud*, FORBES (Mar. 28, 2017, 2:58PM), https://www.forbes.com/sites/roncheng/2017/03/28/cybercrime-in-china-online-fraud [https://perma.cc/42QT-8YEG].

288. *See generally* Personal Information Protection Law, *supra* note 17.

289. *See generally* Data Security Law, *supra* note 16.

demonstrate a genuine effort to regulate and enforce the CSL's data privacy and personal information protections. This reflects a response to strong consumer demand for more robust protections against online fraud, defamation, and other online crimes.[290] The real-name requirement, however, while minimally providing protection in making it easier to identify purveyors of fraudulent schemes and defamation, also aides the State in identifying online dissenters.[291]

China's approach offers a unique model where people have privacy rights and protections vis-à-vis businesses, with the implicit understanding that none of these protections apply against the government. The policy benefits to China are obvious—citizens retain robust personal information and data privacy rights in the economic sphere, fostering further economic growth and development. At the same time, the CCP easily identifies and swiftly punishes internet activity that hints at dissent. China's model is an alternative to the multi-stakeholder, libertarian approach to regulating cyberspace in the West.[292] Much scholarship has focused on China's concept of "cyber sovereignty,"[293] encompassing the three aspects of cyberspace governance, national defense, and internal control.[294] The domestic cases in this Note provide the most insight into China's model of cybersecurity as it applies to internal influence and control.

C. Exporting China's Vision of Cybersecurity

The CSL and its application within China's domestic judicial system illustrate China's cybersecurity vision—fostering domestic technology innovation and growth, restricting dissenting online speech, and building robust privacy protections for consumers that apply in the commercial realm, but not against the State. These developments are sobering in light of China's increasing effort to influence both international legal norms around cybersecurity and the direct export of its cybersecurity vision to other countries.[295] China's domestic

290. *Cf.* Sacks, *supra* note 26.

291. The real-name registration requirement is being rolled out across websites. When the author began research in June 2020 accessing the China Court Judgments website (see *supra* Section II.B), it was available to access, search, and download cases without any registration or identification. In September 2020, the website started requiring registration via phone number (including country code) and confirmation of the phone number to access the website. *Id.*

292. Wang, *supra* note 53, at 444.

293. *Id.*; *see also* McKune & Ahmed, *supra* note 127.

294. McKune & Ahmed, *supra* note 127, at 3837.

295. *See supra* Section I.C.

policies provide a window into what vision of cybersecurity it may seek to promote abroad.

First, China has made concerted efforts to define international law and legal norms on cybersecurity[296] as global cybersecurity norms are still developing.[297] This has included proposals in 2011[298] and 2015 at the U.N. around a "Code of Conduct" on cybersecurity, with language agreeing to "cooperate in combating criminal and terrorist activities . . . and curbing the dissemination of information that incites terrorism, separatism or extremism."[299] The language in the U.N. proposals is similar to the wording in Article 12 of the CSL.[300] Further, China has established its own international institutions to promote its vision of cybersecurity and build global consensus around its vision. The Shanghai Cooperation Organization ("SCO"), established in 2001, has notably focused on combatting "terrorist, extremist, or separatist" ideologies.[301] In 2015 and 2017, the SCO's Regional Anti-Terrorist Structure held Anti-Cyberterror Exercises utilizing Chinese digital forensics technology and sharing information and best practices.[302] The World Internet Conference, a separate meeting held in

296. ROBERT D. WILLIAMS, INTERNATIONAL LAW WITH CHINESE CHARACTERISTICS: BEIJING AND THE "RULES-BASED" GLOBAL ORDER 10 (Oct. 2020), https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201012_international_law_china_williams.pdf [https://perma.cc/5EUE-RMKJ]; Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization* 2 (Mar. 3, 2020) (unpublished manuscript), https://papers.ssrn.com/abstract=3532421 [https://perma.cc/QFS5-ZR4R] (highlighting China's proposals at the UN around global cybersecurity policy).

297. *See* McKune & Ahmed, *supra* note 127, at 3840 (noting that China's promotion of legal norms around internet sovereignty is still in the "norm emergence" phase).

298. Permanent Reps. of China, the Russian Federation, Tajikistan, and Uzbekistan to the U.N., Letter dated Sept. 12, 2011 from the Permanent Reps. of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, at 4, U.N. Doc. A/66/359 (Sept. 14, 2011) (calling on countries to cooperate in combatting online activities "undermining . . . political, economic, and social stability").

299. Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the U.N., Letter dated Jan. 9, 2015 from the Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723, at 5 (Jan. 13, 2015); Lee, *supra* note 1, at 91.

300. Cybersecurity Law, *supra* note 58, art. 12 (prohibiting advocacy of "terrorism or extremism").

301. McKune & Ahmed, *supra* note 127, at 3841–42 (noting the SCO's membership includes China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, with India and Pakistan joining as full members in 2017).

302. Meng Qingsheng, *SCO Joint Anti-cyber Terrorism Exercise Held in Xiamen*, CGTN (Dec. 6, 2016, 8:25 PM), https://news.cgtn.com/news/326b7a4d30637a6333566d54/share_p.html [https://perma.cc/7S4R-PS4G]; McKune & Ahmed, *supra* note 127, at 3842; THE NEW BIG BROTHER, *supra* note 122, at 38–39.

China that includes heads of state, technology executives, and officials from global internet organizations, has been held annually since 2014 and is another prominent forum for China to influence cybersecurity norms and share technology.[303]

In the international sphere, China has promoted its view of "cyber sovereignty," borrowing from the international law concept of state sovereignty to emphasize the right of the State to control cyberspace.[304] As part of its efforts to influence key international law norms, China has de-emphasized the role of civil society in enforcing international human rights law[305] and endorsed the view that international human rights law is purely a matter of state-to-state relations.[306] With the support of other countries, China may generate enough momentum to shape the underlying international legal norms.[307]

Second, apart from its efforts to influence multilateral institutions and international law, China is exerting considerable influence on individual countries through its bilateral relations. China has positioned itself as representing the interests of developing countries, characterizing its own model of internet sovereignty and cybersecurity as a helpful model for other developing countries.[308] China's cybersecurity vision offers improvements in data privacy (in the commercial sense),[309] while supplying tools that work to fight cybercrime and to maintain a dissent-free internet. In an internet framework with

303. McKune & Ahmed, *supra* note 127, at 3845; *World Internet Conference Unveils Leading Cyberspace Sci-tech Achievements in Wuzhen of E China's Zhejiang*, XINHUA (Nov. 24, 2020, 2:15 PM), http://www.xinhuanet.com/english/2020-11/24/c_139539783.htm [https://perma.cc/R4F2-CU3R].

304. McKune & Ahmed, *supra* note 127, at 3849 (arguing that China has misapplied the public international law concept of state sovereignty, which applies only to states, to non-state actors such as civil society organizations, NGOs, and human rights groups).

305. Sophie Richardson, *China's Influence on the Global Human Rights System*, HUM. RTS. WATCH (Sept. 14, 2020, 2:51 PM), https://www.hrw.org/news/2020/09/14/chinas-influence-global-human-rights-system [https://perma.cc/W6Y6-RCW6]; McKune and Ahmed, *supra* note 127, at 3849.

306. Richardson, *supra* note 305; Yu-Jie Chen, *China's Challenge to the International Human Rights Regime*, 51 N.Y.U. J. INT'L L. & POL. 1179, 1204 (2019).

307. McKune & Ahmed, *supra* note 127, at 3839.

308. Benjamin L. Liebman, *Authoritarian Justice in China: Is There a "Chinese Model"?*, *in* BEIJING CONSENSUS?: HOW CHINA HAS CHANGED WESTERN IDEAS OF LAW AND ECONOMIC DEVELOPMENT 225, 235–36, 248 (Weitseng Chen ed., 2017).

309. Maja Zivanovic, *Serbia Tightens Cyber-Security as Internet Crime Rises*, BALKAN INSIGHT (Sept. 28, 2018, 8:01 AM), https://balkaninsight.com/2018/09/28/serbia-to-form-anti-cyber-criminal-units-09-27-2018 [https://perma.cc/A2CX-J8SG].

standards and technology dominated by western countries, China offers an alternative.[310]

Through providing ICT, ordinary bilateral trade, and investment via the Digital Silk Road, China is arguably one of the most influential voices driving cybersecurity policy in developing countries. Investment and provision of technology do not necessarily indicate that China is forcing the spread its cybersecurity policies.[311] However, in practice, many countries such as Vietnam and Uganda are implementing laws and strategies that closely resemble China's approach.[312]

CONCLUSION

China's 2017 CSL generated a flurry of attention when it first appeared. The implementation of the CSL reveals that, in practice, courts are supporting the State's efforts to target dissenting online speech that may threaten social stability, while also addressing the domestic demand for more substantial privacy rights vis-à-vis businesses. China's alternate vision, then, is for an internet that protects individuals and companies in their business transactions—including through strict adherence to the use of real names—but with minimal protections for individuals posting anti-government or stability-threatening speech. China's model is highly attractive for developing countries seeking to maintain stability, while generating sufficient protections to facilitate online commerce and economic growth. In the absence of a strong international framework defining cybersecurity norms and rights, or more robust engagement from democracies in defense of international human rights, China's cybersecurity vision may be on a path to global adoption. As the case law demonstrates, this may be a harbinger for reduced cybercrime and fraud—but potentially at the cost of digital anonymity and internet freedom.

*Grace Pyo**

310. McKune & Ahmed, *supra* note 127, at 3835, 3840.

311. THE NEW BIG BROTHER, *supra* note 122, at 35.

312. *See supra* notes 17–24 and accompanying text.

*J.D Candidate, Columbia Law School, 2022. Thank you to Professor Benjamin Liebman for his excellent guidance on this Note and more broadly for his insights as a mentor during law school. Thank you to Tim Wang, Vineet Surapaneni, Krista Landis, Daniel Spicehandler and the hardworking staffers of the *Columbia Journal of Transnational Law* for their constructive feedback and detailed edits. Finally, I am grateful to God, Derek, and my family and friends, without whom this Note would not have been possible.