Authoritarian Privacy

Mark Jia†

Privacy laws are traditionally associated with democracy. Yet autocracies increasingly have them. Why do governments that repress their citizens also protect their privacy? This Article answers this question through a study of China. China is a leading autocracy and the architect of a massive surveillance state. But China is also a major player in data protection, having enacted and enforced a number of laws on information privacy. To explain how this came to be, the Article first discusses several top-down objectives often said to motivate China's privacy laws: advancing its digital economy, expanding its global influence, and protecting its national security. Although each has been a factor in China's turn to privacy law, even together, they tell only a partial story.

Central to China's privacy turn is the party-state's use of privacy law to shore up its legitimacy amid rampant digital abuse. China's whiplashed transition into the digital age has given rise to significant vulnerabilities and dependencies for ordinary citizens. Through privacy law, China's leaders have sought to interpose themselves as benevolent guardians of privacy rights against other intrusive actors—individuals, firms, and even state agencies and local governments. So framed, privacy law can enhance perceptions of state performance and potentially soften criticism of the center's own intrusions. The party-state did not enact privacy law despite its surveillance state; it embraced privacy law to maintain it. This Article adds to our understanding of privacy law, complicates the relationship between privacy and democracy, and points toward a general theory of authoritarian privacy.

† Associate Professor, Georgetown University Law Center. This Article was supported by outstanding research assistance from Margaret Baughman, Qi Lei, Yizhou Shao, and Joanna Zhang. For generous comments, I thank William Alford, Ngoc Son Bui, William Buzbee, Anupam Chander, Habin Chung, Donald Clarke, Julie Cohen, Rogier Creemers, Xin Dai, Hualing Fu, Tom Ginsburg, Jamie Horsley, Nicholas Howson, Wei Jia, Thomas Kellogg, Margaret Lewis, Benjamin Liebman, Daniel Rauch, Shen Kui, Yueduan Wang, Changhao Wei, Katherine Wilhelm, Angela Zhang, Jeffery Zhang, Taisu Zhang, as well as commenters at George Washington University's Northeast Corridor Chinese Law Workshop, Oxford University's Programme in Asian Laws Series, and Georgetown University Law Center's Summer Faculty Workshop, Technology Law and Policy Colloquium, and S.J.D. and Fellows Seminar. Thanks finally to the insightful editors at the *University of Chicago Law Review*, especially Max Rowe, Jonathan Jiang, and Andy Wang.

INTRODUCTION

In American law and legal theory, privacy and democracy are closely related subjects. Privacy is said to aid democratic performance,[1] to advance democratic values,[2] and to be a basic democratic right.[3] Such views are held on both sides of the public-private divide,[4] by proponents of both individual and social

---

1 *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013) [hereinafter Cohen, *What Privacy Is For*] (arguing that "the capacity for critical subjectivity shrinks in conditions of diminished privacy," reducing "the capacity for democratic self-government"); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651 (1999) (linking "strong rules for information privacy" to "deliberative democracy"); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 456 (1980) ("Denying the privacy necessary for [political negotiation] would undermine the democratic process.").

2 *See* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 845 (2013) ("Privacy is indeed valuable for democratic societies [where] . . . people need the capacity to think and act independently."); Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUT. & HIGH TECH. L.J. 27, 42 (1995) ("[Without] private inner life . . . , neither democracy nor individual freedom have worth.").

3 *See* Whalen v. Roe, 429 U.S. 589, 599–600 (1977) (asserting that the Constitution protects two kinds of privacy: the "interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions").

4 *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951–52 (2013) (noting that the harms of surveillance to intellectual freedom "transcend[ ] the public/private divide").

accounts of privacy's value,[5] and across varying notions of privacy rights—from data protection to intimate privacy.[6]

Yet democracies are not the only countries with privacy laws. Just as authoritarian governments have enacted constitutions despite their conceptual affinities with democracy,[7] so too have such governments enacted privacy laws in recent years, at a speed and scale that have at times exceeded those of major democracies. Of the 130 countries with data privacy laws today, only half are considered free.[8] The rise of privacy laws in nondemocratic nations calls for explanation. Why do governments that repress their citizens also protect their privacy?

This Article answers this question through a close study of China. China is the world's leading autocracy and the architect of a massive surveillance state. It has been described as Orwellian,[9] techno-totalitarian,[10] and the "perfect police state."[11] So understood, China would seem an unlikely sponsor of privacy

---

5 *See* Gavison, *supra* note 1, at 455 ("Privacy is . . . essential to democratic government."); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 638 (2021) (theorizing data as "a democratic medium that materializes population-level, social interests"); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 7 (2010) (linking her "contextual integrity" framework with the "traditions of contemporary liberal democracies"); Priscilla M. Regan, Assoc. Professor, Geo. Mason Univ., Privacy as a Common Good in the Digital World, Remarks Prepared for Delivery at the 1999 Annual Meeting of the American Political Science Association (Sept. 2–5, 1999) ("Privacy . . . has value not just to the individual . . . but also to the democratic political system.").

6 *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1892–93 (2013) (highlighting the social impacts of individual privacy decisions); Danielle Keats Citron, *Intimate Privacy's Protection Enables Free Speech*, 2 J. FREE SPEECH L. 3, 10 (2022) (linking intimate privacy to equality and free expression).

7 *See generally* CONSTITUTIONS IN AUTHORITARIAN REGIMES (Tom Ginsburg & Alberto Simpser eds., 2014); GÜNTER FRANKENBERG, AUTHORITARIANISM: CONSTITUTIONAL PERSPECTIVES (2020).

8 Of the over 130 countries with data privacy laws today, around thirty-five are considered "Not Free" by the nonprofit group Freedom House, and about forty are considered "Partly Free." *See Data Protection and Privacy Legislation Worldwide*, U.N. CONF. ON TRADE & DEV. (2021), https://perma.cc/T4K3-Q92E (see full data table); *Countries and Territories (Global Freedom Scores)*, FREEDOM HOUSE (2022), https://freedomhouse.org/countries/freedom-world/scores (rating countries as "free," "partly free," and "not free").

9 *See* KAI STRITTMATTER, WE HAVE BEEN HARMONIZED: LIFE IN CHINA'S SURVEILLANCE STATE 2 (2020); *see also* Dustin Carmack, *China's Orwellian Digital Surveillance Turns to Olympic Athletes*, SEATTLE TIMES (Feb. 2, 2022), https://www.seattletimes.com/opinion/chinas-orwellian-digital-surveillance-turns-to-olympic-athletes/.

10 Klon Kitchen, *Surveillance Systems and Internet Rules: Blunting China's Technototalitarianism*, AM. ENTER. INST. (May 5, 2022), https://perma.cc/2MQD-R6DE.

11 GEOFFREY CAIN, THE PERFECT POLICE STATE: AN UNDERCOVER ODYSSEY INTO CHINA'S TERRIFYING SURVEILLANCE DYSTOPIA OF THE FUTURE 5 (2021).

protections. Yet, in recent years, China's government has enacted a number of laws that protect information privacy. Aspects of these laws are said to resemble the European Union's (EU) General Data Protection Regulation (GDPR), a global standard for data protection.[12] Data thieves have been prosecuted, technology companies have been fined, and many have been sanctioned for infringing personal privacy.[13] Recently, a national legislative office declared that local regulations authorizing traffic police to search motorist cell phones were unlawful.[14] Such laws, it said, violated "citizens' freedom and privacy of correspondence."[15]

China's privacy laws do not mirror those in democratic nations. They have unreviewable exceptional zones that enable state surveillance, and their execution is not immune from the vagaries of Chinese law enforcement. But they are treated locally as law in the same manner as tort or contract law. And they perform far more than the window-dressing functions attributed to some authoritarian constitutions. How should we understand these developments?

This Article explains China's turn to privacy law from the perspective of authoritarian self-interest, with attention to both the bottom-up and top-down benefits of privacy laws to the party-state. It begins by clarifying three interrelated benefits that are sometimes said to motivate China's use for privacy laws: building trust to grow the digital economy, attracting data flows to expand global influence, and securing data to protect national security. These motivations tell an ostensibly coherent story of China's turn to privacy law, compatible with mainstream understandings of top-down authoritarian governance. And each, in limited and particular ways, is a factor in China's turn to privacy law. But even when considered together, these motivations sum only to a partial account. They cannot explain notable developments, and they cannot explain away notable exceptions.

A more complete story of China's turn to privacy law should start from the bottom up. China has datafied more quickly and more intensely than virtually any other nation.[16] It is the world's leading data generator, home to a thriving black market for

---

12 *See infra* Part I.B.

13 *See infra* Part III.C.

14 Changhao Wei, *Recording & Review Pt. 5: "Freedom and Privacy of Correspondence,"* NPC OBSERVER (June 10, 2019), https://perma.cc/92UL-Q4TR [hereinafter Wei, *Privacy of Correspondence*].

15 *Id.* (using phrasing from Article 40 of China's Constitution).

16 *See infra* Part III.A.

personal data. It is both a pioneer in, and the world's most pervasive user of, facial recognition technologies. It instituted pandemic control measures that limited citizen mobility based on location and other personal data. And it has overseen the rise of powerful technology firms that, for many years, enjoyed few meaningful constraints on their personal data collection and processing. To live ordinarily during this time is to be exposed to a staggering amount of digital dependency and vulnerability. Popular unrest over privacy violations has risen swiftly in recent years, as evidenced by a series of data privacy scandals.[17] Chinese Communist Party (Party) organs have begun describing privacy invasions as a source of social instability.[18]

The party-state's strategy has been to deploy a mix of policy responsiveness, lawmaking, and law enforcement to repair legitimation deficits stemming from data discontent. This is discernible from an array of sources, including speeches, reports, media, cases, laws, regulations, and campaigns, and finds parallels in other domains of socioeconomic governance, including food safety, public health, and environmental protection. As in these other areas, the party-state has sought to interpose itself as a protective guardian of citizens' rights against other intrusive actors.[19] Privacy violators, in this narrative, include opportunistic criminals, avaricious firms, and sloppy local governments, but never the central party-state itself. So framed, privacy law can not only improve perceptions of regime performance, but also soften criticism of the party-state's own role in driving data vulnerability, having seized the mantle as privacy's principal defender. China's leaders did not adopt privacy law in spite of their surveillance state; they enacted privacy laws in order to maintain it.

This Article makes several contributions. First, it offers a general theory of Chinese privacy law that draws on, but goes beyond, existing explanations in the literature.[20] China's privacy

---

17 *See infra* Part III.B.

18 *See infra* note 182 and accompanying text.

19 *See infra* Part III.C.

20 *See generally* Rogier Creemers, *China's Emerging Data Protection Framework*, 8 J. CYBERSECURITY, Aug. 24, 2022, at 1 (providing a careful, document-focused analysis of the Personal Information Protection Law, the Data Security Law, and their precursors); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PENN. ST. J.L. & INT'L. AFF. 49 (2020) (situating China's data protection regime as a "third way" between the U.S. and the EU); Tiffany Li, Zhou Zhou & Jill Bronfman, Saving Face: Unfolding the Screen of Chinese Privacy Law (Aug. 14, 2017) (unpublished manuscript) (on file with author) (conducting a primarily cultural analysis of China's privacy laws); Xin Dai, *Privacy, Reputation, and Control: Public Figure*

laws are not "exclusively" consumerist,[21] nor are they merely incidental to the party-state's interests in state security or global influence.[22] By understanding China's privacy turn as a story of popular legitimation, this Article shows some of the limited ways in which ordinary people can continue to influence national policies. This Article also contributes to our understanding of China's legal system generally. It highlights key developments in Chinese law, such as the rise of controlled public interest lawsuits against state organs, analyzes core tensions in the party-state's effort to leverage data and technology, and shows how legal borrowing has continued despite a recent focus on indigenous legal innovation.

From a regime-level understanding of Chinese privacy law, one can begin to build out a general theory of authoritarian privacy. Although China does not represent all of autocracy, it is a politically important case, and may well evince trends observable elsewhere. This Article offers a preliminary take on the appeal of privacy laws to authoritarian regimes, following scholars who have systemized the costs and benefits of courts and constitutions to autocratic rulers.[23] It hypothesizes that while autocrats will vary in what they seek to gain from privacy law, they will generally seek to maximize these benefits while minimizing privacy law's risks. The result may be laws that bear a family resemblance to other privacy regimes, but with larger exceptional zones, harder localization requirements, and a legal-political infrastructure designed to contain legal activism.

Finally, this Article hopes to stimulate reflection on the conceptual links between privacy, democracy, and autocracy. Theorists often stress privacy's deep connections to democracy.[24] When invoked, authoritarianism is more often treated as an Orwellian abstraction than a site of privacy law development.[25] This Article complicates traditional views of the privacy-democracy nexus in several ways. It shows descriptively how data protection laws can advance not just democratic values, but also authoritarian

---

Privacy Law in Contemporary China, 9 PEKING UNIV. L.J. (discussing the cultural origins of public figure privacy law in China).

21 *See* Paul de Hert & Vagelis Papakonstantinou, *The Data Protection Regime in China: In-Depth Analysis for the LIBE Committee*, 5, PE 536.472 (Oct. 2015) ("[W]hatever data protection exists in China today, it is aimed exclusively at the individual as consumer."); *see also infra* Part II.A.

22 *See infra* Parts II.B, II.C.

23 *See infra* Part IV.B.

24 *See infra* Part IV.C.

25 *See infra* Part IV.C.

interests; it highlights how even in authoritarian societies, there can be quasidemocratic drivers of privacy law that liberal theorists may overlook; and it suggests that autocracies and democracies can sometimes enact data privacy laws for overlapping reasons. In fact, neoliberal democracies today have more in common with market-oriented autocracies than a diametric understanding of democracy and autocracy might predict.[26] Authoritarian privacy is both a local phenomenon and part of a global trend.

Before proceeding, several notes are in order. First, there is the question of what I mean by privacy, a concept that has eluded easy definition in U.S. law[27] and that presents additional epistemic challenges in other cultural-linguistic settings. As legal scholar William Alford has cautioned, "use by different societies of common terminology does not necessarily ensure . . . the same meaning in each setting."[28] *Yinsi*, the Chinese term for privacy, has several distinct meanings: classical analogs associated with indecency,[29] modern definitions that retain notions of secrecy and shame,[30] and the legal term of art today that more closely approaches international definitions.[31]

Despite conceptual similarities between *yinsi* and privacy, this is not, strictly speaking, a study of *yinsi* in China. Following privacy scholar Daniel Solove, I understand privacy in general to refer to a "cluster of many distinct yet related" ideas.[32] Solove's

---

[26] *See infra* Part IV.C.

[27] *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 12–38 (2008) (critiquing a "multitude of different conceptions of privacy"); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) ("Privacy is a value so complex . . . that I sometimes despair whether it can be usefully addressed at all.").

[28] WILLIAM P. ALFORD, TO STEAL A BOOK IS AN ELEGANT OFFENSE: INTELLECTUAL PROPERTY LAW IN CHINESE CIVILIZATION 5 (1995).

[29] *See* Bo Zhao, *Posthumous Reputation and Posthumous Privacy in China: The Dead, the Law, and the Social Transition*, 39 BROOKLYN J. INT'L L. 269, 287 (2014); Guobin Zhu, *The Right to Privacy: An Emerging Right in Chinese Law*, 18 STATUTE L. REV. 208, 208–09 (1997) (citing a definition from China's Law Dictionary, *Faxue Cidian*, that connects *yinsi* to indecent crimes like rape and prostitution).

[30] *See Yinsi* (隐私), WENXUEWANG HANYU CIDIAN (文学网汉语词典) [Wenxue Online Chinese Dictionary], https://perma.cc/6MKR-5J3P (defining yinsi to encompass "matters one is unwilling to share with others," especially "shameful matters"); *see also Yin Si* (隐私), XINHUA HANYU CIDIAN (新华汉语词典) [Xinhua Chinese Dictionary] (Zhou Bin (周斌) ed. 2004) (defining yinsi to include "matters one is unwilling to share with others or publicize").

[31] *See* Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., May 28, 2020, effective Jan. 1, 2021), art. 1032, 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 1, 160 (English translation available at https://perma.cc/7WFA-KWFQ) [hereinafter Civil Code].

[32] SOLOVE, *supra* note 27, at 40.

pluralistic approach sees Wittgenstein-ian "family resemblances" between multiple ideas of privacy, including intimacy, personhood, secrecy, information control, and the right to be let alone.[33] As Part I traces how scholars have uncovered privacy sensibilities in China's past, one can discern how relatively fluid and contextual notions of privacy have underlain multidisciplinary analyses of Chinese privacy from the beginning.

The form of privacy that has changed the most legally in China, and the focus here, is privacy of personal information. Information privacy encompasses everything from personally identifiable information, such as names, addresses, phone numbers, financial and biometric data, and data "extracted from people as they invest, work, operate businesses, socialize, and engage in innumerable other activities."[34] In the past, Chinese sensibilities around information privacy focused narrowly on the confidentiality of letters or marital secrets.[35] In today's age of informational capitalism, platform intermediaries, pervasive datafication, predictive profiling, and mass surveillance, the quantity and variety of shareable personal information are unprecedented.[36]

This Article's focus on information privacy does not diminish other privacy forms. The pace of change in information privacy in China, relative to other areas, is itself revealing of privacy's limits under autocracy.[37] But the focus on information privacy is not unduly narrowing either.[38] When commentators raise privacy concerns with public or private surveillance in China, they are describing intrusions on information privacy: incursions on people's ability "to determine for themselves when, how, and to what extent information about them is communicated to others."[39]

The second note is that by highlighting general motivations like "security" and "legitimation," this Article does not mean to

---

33 *Id.* at 15–37.

34 JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 38 (2019) [hereinafter COHEN, BETWEEN TRUTH AND POWER].

35 *See infra* Part I.B.

36 *See infra* Part III.A.

37 For instance, one might examine legal and social changes in decisional privacy, "freedom from coercive interference with decisionmaking affecting intimate and personal affairs." *See* Anita L. Allen, *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*, 56 U. CIN. L. REV. 461, 461 (1987). China's history of birth planning policies would be centrally relevant to such an inquiry.

38 *See* NEIL RICHARDS, WHY PRIVACY MATTERS 23 (2021) (focusing on information privacy because it "is particularly important at this point in human history").

39 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

discount the role of individual actors or some level of contingency in shaping the progression of China's privacy law. As in other areas of lawmaking, China's privacy laws reflect the buy-in of senior leaders, advice from legal scholars, negotiations among competing bureaucracies, and input from industry and other societal organizations.[40] Nor does this Article mean to suggest a perfectly linear progression of popular demand and state response; informational signals may lag before reaching top leaders, and the timing of enactment or enforcement can reflect a convergence of multiple political priorities. But governments do things for reasons, and as this Article will show, those reasons can be helpfully distilled into several high-level explanations.[41]

Finally, it helps to address a set of counterarguments at the outset, one rooted more in intuitions about authoritarianism than arguments widely circulating in the literature. Privacy laws, this argument would go, are just another form of repression; the party-state adopted them to weaken rival power centers, or, more subtly, to thwart collective action by atomizing individuals within greater information silos. While both motivations are plausibly a part of China's privacy story, they are not the heart of it. First, as Part I.B will detail, the state has been steadily adopting data privacy laws, regulations, and guidelines for the better part of a decade. Yet for most of this period, central leaders were sparing in their regulation of the technology sector. To the extent they were concerned about political threats posed by such firms, that realization only came to the fore after Ant Financial founder Jack Ma's fateful 2020 speech criticizing financial regulators.[42] But the state's draft of its most comprehensive privacy law was posted for public comments *before* Ma's speech,[43] suggesting that such laws were on an independent legislative track, devised before central leaders had fully perceived the political threats emanating from Big Tech.[44] Second, although privacy law can conceivably thwart

---

40 *See infra* Part I.B.

41 *See infra* Part III.C.

42 *See* Angela Huyue Zhang, High Wire: How China Regulates Big Tech and Governs Its Economy 63 (Feb. 2024) (unpublished manuscript) (on file with author) [hereinafter Zhang, High Wire]; *infra* note 156.

43 *See China's Draft "Personal Information Protection Law" (Full Translation)*, NEW AM. (Rogier Creemers et al. trans., Graham Webster ed., Oct. 21, 2020), https://perma.cc/3ADK-4VNP (English translation).

44 *See* Angela Huyue Zhang, *Agility over Stability: China's Great Reversal in Regulating the Platform Economy*, 63 HARV. INT'L. L.J. 457, 460 (2022) [hereinafter Zhang, *Agility over Stability*] (describing "information lag" between regulators and top policymakers, leading to sudden fluctuations "from very lax to very harsh enforcement").

collective action by limiting information sharing, it is hardly the most effective or direct tool for doing so compared to the extensive censorship and surveillance apparatus the party-state already has in place. Even if privacy laws marginally increase the costs of data sharing, they do not prevent citizens from willingly sharing information with one another compared to far more direct and obvious interventions already at the party-state's disposal.

The remainder of this Article proceeds as follows. Part I surveys the history of privacy and privacy law in China. It will show that while privacy laws are new to China, privacy sensibilities in China are old and in a sense universal. The next two parts explain China's turn to privacy law. Part II analyzes three top-down benefits of privacy law for the party-state: growth, influence, and security. Although these factors have mattered to varying degrees, they leave critical developments unexplained. Part III models Chinese governance from the bottom up, arguing that China's turn to privacy law should be understood more centrally as a story of popular legitimation. The party-state's turn to privacy law reflects a kind of authoritarian responsiveness, an effort to co-opt privacy by framing the party-state as the principal defender of privacy rights. Part IV concludes with implications for Chinese law, authoritarian legality, and the privacy-democracy nexus.

I. PRIVACY IN CHINA'S PAST AND PRESENT

The idea of Chinese privacy law may seem counterintuitive. Privacy is sometimes depicted as an "alien concept in Chinese culture,"[45] an idea that, if it existed once, is assuredly "dead and buried" today.[46] Part I synthesizes a rich literature—from sinology to history to law—that has argued otherwise. Section A will show that one can speak meaningfully of privacy sensibilities in China's premodern tradition. This suggests that the popular privacy awakening in China today is not a modern invention, but follows long-standing human patterns. What is novel today is the use of law to provide limited protections to privacy interests. Section B surveys these modern legal developments.

---

[45] Luisa Tam, *Why Privacy Is an Alien Concept in Chinese Culture*, S. CHINA MORNING POST (Apr. 2, 2018), https://www.scmp.com/news/hong-kong/article/2139946/why-privacy-alien-concept-chinese-culture.

[46] STRITTMATTER, *supra* note 9, at 213.

A. Privacy in China's Premodern Tradition

There is a descriptive sense in which all cultures can be said to observe privacy. Putting aside questions of laws and rights, privacy can also be a means of "distinguish[ing] between what is open or overt and what is concealed" as a matter of social practice.[47] A seminal formulation of this approach comes from the social psychologist Irwin Altman, who defined privacy as "a boundary control process whereby people sometimes make themselves open and accessible to others and sometimes close themselves off from others."[48] So understood, privacy involves a "network of behavioral mechanisms that people use to achieve desired levels of social interaction."[49] Privacy then is a "culturally universal process," even where its mechanisms are culturally specific.[50]

Following this approach, several scholars have located privacy concepts in corners of Chinese tradition.[51] Perhaps the best example is *Chinese Concepts of Privacy*, a collection of essays seeking to uncover indigenous privacy concepts from Chinese art, literature, and history.[52] Its contributors find privacy norms in sources as varied as Zhou dynasty (c. 1046–256 B.C.) bronze ritual vessels,[53] Ming dynasty (c. 1368–1644 A.D.) medical records,[54] the eighteenth-century novel, *Dream of the Red Chamber*,[55] the

---

47 Christina B. Whitman, *Privacy in Early Confucian and Taoist Thought*, *in* INDIVIDUALISM AND HOLISM: STUDIES IN CONFUCIAN AND TAOIST VALUES 85, 85 (Donald J. Munro ed., 1985).

48 Irwin Altman, *Privacy Regulation: Culturally Universal or Culturally Specific?* J. SOC. ISSUES, Summer 1977, at 66, 67.

49 *Id.*

50 *Id.* at 66, 79; *see also* WESTIN, *supra* note 39, at 13 ("Needs for individual and group privacy and resulting social norms are present in virtually every society.").

51 Many have said so explicitly. *See, e.g.*, Bonnie S. McDougall, *Particulars and Universals: Studies on Chinese Privacy*, *in* CHINESE CONCEPTS OF PRIVACY 3, 7 (Bonnie S. McDougall & Anders Hansson eds., 2002) (citing Altman favorably) [hereinafter McDougall, *Particulars and Universals*]; Kenneth Neil Farrall, *Global Privacy in Flux: Illuminating Privacy Across Cultures in China and the U.S.*, 2 INT'L J. COMMC'N 993, 1000–01 (2008) (same); Lara A. Ballard, *The* Dao *of Privacy*, 7 MASARYK U. J.L. & TECH. 107, 142 (2013) (same).

52 McDougall, *Particulars and Universals*, *supra* note 51, at 21–24 (summarizing contributions).

53 *See generally* Maria Khayutina, *Studying the Private Sphere of the Ancient Chinese Nobility Through the Inscriptions on Bronze Ritual Vessels*, *in* CHINESE CONCEPTS OF PRIVACY, *supra* note 51, at 81.

54 *See generally* Charlotte Furth, *Solitude, Silence and Concealment: Boundaries of the Social Body in Ming Dynasty China*, *in* CHINESE CONCEPTS OF PRIVACY, *supra* note 51, at 27.

55 *See generally* Cathy Silber, *Privacy in* Dreams of the Red Chamber, *in* CHINESE CONCEPTS OF PRIVACY, *supra* note 51, at 54.

late nineteenth-century moral discourses of reformer-intellectual Liang Qichao,[56] and edited love letters between the early twentieth-century writer Lu Xun and a student, Xu Guangping.[57] In the introduction to *Chinese Concepts of Privacy*, sinologist Bonnie McDougall resisted the idea that the Chinese word *si*, which she associated with both "private" and "privacy," has always been tied to notions of selfishness or profit.[58] Similarly, historian Peter Zarrow argued that although *si* was often juxtaposed unfavorably with *gong* ("public"), there was a trend in late Imperial China "to allow *si* greater scope."[59]

Others have uncovered privacy concepts from classical texts. In her review of Confucian and Daoist canons, legal scholar Christina Whitman concluded that modern privacy values—"family, friends, self-development, and introspection"—"have counterparts in premodern China."[60] Likewise, sociologist Barrington Moore found in Confucian, Daoist, and Legalist texts "a sharp distinction between the concepts of public and private."[61] U.S. diplomat Lara Ballard examined privacy "through the lens of traditional Daoist metaphysics."[62] She concluded that "East Asian concepts of privacy easily rival their Western counterparts in historical depth, cultural breadth, nuance and psychological complexity."[63]

These works well illustrate the sociocultural and philosophical functions of privacy in China's past. But, unsurprisingly, none have located thicker privacy concepts found in liberal-democratic societies. Whitman, for example, finds no classical Chinese analog to the "modern belief that a human being is fully autonomous only if he is free to discover what is distinctive about himself as an individual."[64] While reserve, withdrawal, and keeping confidences

---

56 *See generally* Peter Zarrow, *The Origins of Modern Chinese Concepts of Privacy: Notes on Social Structure and Moral Discourse*, *in* CHINESE CONCEPTS OF PRIVACY, *supra* note 51, at 121.

57 *See generally* Bonnie S. McDougall, *Functions and Values of Privacy in the Correspondence Between Lu Xun and Xu Guangping, 1925–1929*, *in* CHINESE CONCEPTS OF PRIVACY, *supra* note 51, at 147 [hereinafter McDougall, *Functions and Values*].

58 McDougall, *Particulars and Universals*, *supra* note 51, at 8–9.

59 Zarrow, *supra* note 56, at 132–33. Communications scholarship has drawn similar conclusions. *See* Farrall, *supra* note 51, at 995–97 (challenging the notion that China lacked a "concept of privacy until [ ] exposure to Western culture").

60 Whitman, *supra* note 47, at 86.

61 BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 221 (1984).

62 Ballard, *supra* note 51, at 114.

63 *Id.* at 141.

64 Whitman, *supra* note 47, at 86.

are valued in the *Analects* and the *Dao De Jing*, she explained, their aims in Chinese tradition are not to enable individuals to "exercise free choice as part of a process of self-determination."[65] Rather, withdrawal is thought to enable a "union of the individual with something greater—the natural ordering of men and nature, in Confucianism; or the all-encompassing [D]ao, in [D]aoism."[66]

Also absent from these accounts are references to privacy protection as a state responsibility, or of privacy as a legal right. Although conceptual predecessors to rights can be found in Confucian works, no commentator has, to my knowledge, sourced from Chinese tradition a right to privacy as a legally protected entitlement.[67] The Chinese term for "right" (*quanli*) was first used in missionary W.A.P. Martin's translation of diplomat Henry Wheaton's *Elements of International Law* in the 1860s, and entered the political discourse thereafter.[68] But even in the late Qing era, as thinkers such as Liang Qichao and Liu Shipei meditated on concepts of *quanli*,[69] the dominant rights discourse generally centered on ethics, not law.[70] Ballard concluded that China "has a tradition of privacy, but not privacy rights."[71] Scholar Zhou Hanhua, a pioneer in Chinese data protection, found in the "legal tradition in China" no "privacy right to confront [ ] state power."[72] It is one thing to value privacy in interpersonal and sociocultural relations. It is another to encode privacy within formal legal rules.

B. Privacy and Law in Modern China

It was not until the reform period that one could meaningfully speak of privacy law in China. The preceding Mao era was a low point for social expectations of privacy. At its worst, it recalls political theorist Hannah Arendt's observation that totalitarian governments distinguish themselves from ordinary tyrannies by destroying not merely public, but also private life.[73] Government

---

65 *Id.* at 88, 97.

66 *Id.* at 88.

67 *See* STEPHEN C. ANGLE, HUMAN RIGHTS AND CHINESE THOUGHT: A CROSS-CULTURAL INQUIRY 74–100 (2002) (describing Neo-Confucian contributions to Chinese rights discourse).

68 *Id.* at 3.

69 *See id.* at 140–77.

70 *See id.* at 161 ("It is clear [ ] that Liang has little to say about the relationship between law and *quanli*.").

71 Ballard, *supra* note 51, at 116 ("What is novel to East Asia is Western legalism.").

72 *Id.* at 165 n.249; *see also* Hao Wang, *The Conceptual Basis of Privacy Standards in China and Its Implications for China's Privacy Law*, 7 FRONTIERS L. CHINA 134, 138–40 (2012) (explaining why privacy did not receive legal protections in imperial China).

73 HANNAH ARENDT, THE ORIGINS OF TOTALITARIANISM 475 (1958).

intrusions occurred largely through work units known as *danwei*, "the most basic collective unit in the Chinese political and social order" through "which the state control[led] members of the cadre corps" and "monitor[ed] ordinary citizens."[74] Through the *danwei*, bureaucrats "supervised not only their employees' work, but also their political thoughts, their recreational activity, [and] their decisions to marry, divorce, or have a baby."[75] Privacy intrusions arguably peaked during the Cultural Revolution and in the decade that followed. For instance, neighborhood committees were known to enforce birth limits by maintaining menstrual charts.[76]

Privacy sensibilities evolved considerably in the late 1980s and 1990s, as former Chinese leader Deng Xiaoping's economic pragmatism gave "new legitimacy to private venture."[77] Decollectivization shifted leisure activities from the village toward the home; market reforms brought about larger living spaces and consumerism; and an influx of Western ideas fostered a growing rights consciousness.[78] Privacy sensibilities began to broaden from a focus on shameful secrets to concern over the security of personal information.[79] One could discern "the state's step-by-step retreat from citizens' intimate lives" through the 1980s.[80]

It was then that the party-state first began to enact laws purporting to protect certain privacy interests.[81] Several recitations of China's early privacy laws begin with the 1982 Constitution's

---

74 Xiaobo Lü, *Minor Public Economy: The Revolutionary Origins of the* Danwei, *in* DANWEI: THE CHANGING CHINESE WORKPLACE IN HISTORICAL AND COMPARATIVE PERSPECTIVE 21 (Xiaobo Lü & Elizabeth J. Perry eds., 1997).

75 Martin King Whyte, CHINA J., Jan. 1999, at 182, 182 (reviewing DANWEI: THE CHANGING CHINESE WORKPLACE IN HISTORICAL AND COMPARATIVE PERSPECTIVE (Xiaobo Lü & Elizabeth J. Perry eds., 1997)); *see also* McDougall, *Functions and Values*, *supra* note 57, at 165.

76 McDougall, *Functions and Values*, *supra* note 57, at 166.

77 Farrall, *supra* note 51, at 1014. Fears of being reported were reduced as the terrors of the Cultural Revolution receded. *Cf.* Mary Gallagher, *China's Rewritten Past: How the Communist Party Weaponizes History*, FOREIGN AFFS., July/Aug. 2023, at 190 (reviewing TANIA BRANIGAN, RED MEMORY: THE AFTERLIVES OF CHINA'S CULTURAL REVOLUTION (2023)).

78 *See* Farrall, *supra* note 51, at 1014–15; Ballard, *supra* note 51, at 152 (citing YUNXIANG YAN, PRIVATE LIFE UNDER SOCIALISM: LOVE, INTIMACY, AND FAMILY CHANGE IN A CHINESE VILLAGE 1949–1999, at 218 (2003); Lü Yao-Huai, *Privacy and Data Privacy Issues in Contemporary China*, 7 ETHICS & INFO. TECH. 7, 7–9 (2005).

79 Lü, *supra* note 78, at 8–9.

80 KE LI, MARRIAGE UNBOUND: STATE LAW, POWER, AND INEQUALITY IN CONTEMPORARY CHINA 172 (2022).

81 Mao-era laws did occasionally reference the term *yinsi*, or privacy, mostly in the context of nonpublic trials. *See* Zhou Hanhua, *Consumer Data Protection in China*, *in* CONSUMER DATA PROTECTION IN BRAZIL, CHINA AND GERMANY: A COMPARATIVE STUDY 35, 37–38 (Rainer Metz et al. eds., 2016).

restrictions on violating "personal dignity" and "citizens' freedom and privacy of correspondence," and its prohibitions of the "unlawful search of, or intrusion into, a citizen's home."[82] Before that, the 1979 Criminal Law touched on privacy by forbidding the concealing, destroying, or unlawful opening of others' letters.[83] In the late 1980s and 1990s, following a general increase in legislative activity, the state enacted more laws with privacy-related aspects to protect minors and women, and to regulate lawyers' and banks' obligations to their clients.[84]

Perhaps the most notable privacy-related law of the early reform era was a 1986 provision of the General Principles of the Civil Law protecting citizens' "dignity" and "right of reputation."[85] Claims could be brought for reputational harms arising not only from false reports, but also from the unauthorized revelation of personal details.[86] Cases alleging such harms grew steadily during this period.[87] According to legal scholar Hilary Josephs, the most commonly litigated reputation cases in Beijing involved "disputes between relatives or neighbors alleging invasion of privacy or misrepresentation."[88] In his review of cases from

---

[82] XIANFA [Constitution] arts. 37–40 (1982); *see also* Zhu, *supra* note 29, at 210–11; Lü, *supra* note 78, at 9.

[83] Zhonghua Renmin Gongheguo Xingfa (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., July 6, 1979, effective Jan. 1, 1980), art. 149, 2009 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 306, 319 (English translation available at https://perma.cc/VS7A-YVTF).

[84] Lü, *supra* note 78, at 9. The late 1980s and 1990s also saw a flowering in academic discourse on privacy rights. *See* Zhu, *supra* note 29, at 209–13.

[85] Zhonghua Renmin Gongheguo Minfa Tongze (中华人民共和国民法通则) [General Principles of the Civil Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Apr. 12, 1986, effective Jan. 1, 1987, rev'd Aug. 27, 2009), art. 101, 2009 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 21, 29 *translated in General Principles of Civil Law of the People's Republic of China*, 34 AM. J. COMPR. L. 715, 735 (Whitmore Gray & Henry Ruiheng Zheng trans., 1986) ("Citizens and legal persons enjoy a right to their reputation; a citizen's dignity is protected by law; it is forbidden for anyone to damage the reputation of a citizen or a legal person by the use of slander, libel, or similar means."). There was also a criminal law analog. *See* Benjamin L. Liebman, *Innovation Through Intimidation: An Empirical Account of Defamation Litigation in China*, 47 HARV. INT'L L.J. 33, 40 n.29 (2006) ("Regulations also permit the police to detain persons for up to fifteen days for insulting or slandering another person."); Hilary K. Josephs, *Defamation, Invasion of Privacy, and the Press in the People's Republic of China*, 11 PAC. BASIN L.J. 191, 198 & n.41 (1993).

[86] Liebman, *supra* note 85, at 40 (summarizing judicial interpretations of the Supreme People's Court).

[87] *Id.* at 43–53; Josephs, *supra* note 85, at 197.

[88] Josephs, *supra* note 85, at 198 & n.39. A more modern iteration of these suits concern the use of surveillance cameras overlooking a neighbor's unit. *See* Zhenshi Anli: Linju Zai Jia Menqian Anzhuang Jiankong Shexiangtou, *Qinfan Ni De Yinsi Le Ma?* (【真实案例】邻居在家门前安装监控摄像头，侵犯你的隐私了吗?) [*A Real-World Case: Is Your*

1995–2004, legal scholar Benjamin Liebman found that the rise of reputation suits demonstrated, among other things, an "increased willingness and ability of individuals to use the legal system to pursue rights-based grievances."[89] For a share of litigants, law was starting to assume a larger role in boundary management.

Technological changes accelerated the party-state's use of law to manage privacy interests. Legal scholar Rogier Creemers traced the origins of China's modern data laws to the party-state's long-standing interest in guarding network information security and state secrets.[90] Yet as increasing amounts of data became digitized in the early 2000s, regulations began also to focus on personal information under the auspices of several new bodies, including a new Informatization Office inside the State Council.[91] In 2003, that office charged a team of scholars led by Zhou Hanhua of the Chinese Academy of Social Sciences with drafting a comprehensive personal information protection law.[92] The draft was said to reflect both foreign privacy models and local requirements.[93] It incorporated principles on data quality, data security, data processor duties, and remedies that were largely "similar," wrote data privacy scholar Graham Greenleaf, to "data protection principles usually found in international privacy agreements."[94]

The experts' draft stalled, despite some early momentum.[95] Lawmaking on data privacy proceeded instead in sectoral increments.[96] A 2009 Criminal Law revision barred state personnel, among other actors, from selling personal information.[97] The 2009

Privacy Violated When Your Neighbor Installs a Surveillance Camera in Front of Your Home?], SOHU (Nov. 8, 2017), https://perma.cc/ZT2C-SYNB.

89 Liebman, *supra* note 85, at 93.

90 Creemers, *supra* note 20, at 3 (describing the Ministry of Public Security's multi-level protection system as "a graduated protection regime for all network systems").

91 *Id.*; Yehan Huang & Mingli Shi, *Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law*, DIGICHINA (June 8, 2021), https://perma.cc/FA3U-NXC7 [hereinafter Zhou Interview]. The State Council is the country's chief administrative authority.

92 Creemers, *supra* note 20, at 3.

93 Zhou Interview, *supra* note 91.

94 Graham Greenleaf, *China's Proposed Personal Information Protection Act (Part I): The Principles*, PRIV. L & BUS. INT'L NEWSL. (Feb. 7, 2008), https://perma.cc/9ZAV-AP3C.

95 *Id.*

96 *See* Pernot-Leplay, *supra* note 20, at 71. For a thorough account of many laws and regulations that followed, see Zhou, *supra* note 81, at 36–49.

97 Creemers, *supra* note 20, at 3. For a more recent account of how the criminal law's personal information protection provisions are selectively applied today, see generally Donald Clarke, *Don't Ask, Don't Sell: The Criminalization of Business Information-Gathering in China and the Case of Peter Humphrey*, 33 PAC. BASIN L.J. 109 (2016).

Tort Liability Act[98] gave explicit protection to the "right to privacy," and made medical institutions and their workers liable for nonconsensual disclosure of medical history data.[99] The Ministry of Industry and Information Technology (MIIT) issued regulations in 2011 obligating online services to follow principles of informed consent and necessity in data use and collection.[100] The National People's Congress Standing Committee (NPCSC) issued a 2012 Decision on Information Protection that broadened the MIIT regulations to cover other providers and forbade state agencies from "leaking, distorting or selling personal information."[101] The Consumer Protection Law was revised to include a right to consumer data protection and to incorporate "core" protection principles from the NPCSC Decision.[102]

The next major legal event was the enactment of the 2017 Cybersecurity Law.[103] Although targeted at a range of cybersecurity issues, the Cybersecurity Law also contains several privacy provisions that would be familiar to data protection experts. Article 41 requires all network operators collecting or using personal information to follow "principles of legality, propriety, and necessity," to obtain consent, and to desist from collecting personal data "unrelated" to the services provided.[104] Article 42 states that network operators may not "disclose, tamper with, or destroy personal information they gather" and must adopt "remedial measures" in the event of leak, loss, or destruction.[105] Article 43 gives individuals the right to request deletion and correction of their personal information.[106]

---

98 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), 2010 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 4–10 (English translation available at https://perma.cc/WY8T-ZB44).

99 Zhou, *supra* note 81, at 42.

100 Creemers, *supra* note 20, at 3.

101 *Id.* at 4.

102 Pernot-Leplay, *supra* note 20, at 71 & n.104; *see also id.* at 72 (listing later-issued regulations and sectoral laws).

103 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. 11, 2016, effective June 1, 2017), 2016 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 899–907 *translated in Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2007)*, DIGICHINA (Rogier Creemers et al. trans., June 29, 2018), https://perma.cc/SRC2-26MM [hereinafter Cybersecurity Law].

104 *Id.* art. 41.

105 *Id.* art. 42.

106 *Id.* art. 3.

In 2018, a standard-setting body supervised by the Cyberspace Administration of China (CAC) issued a Personal Information Security Specification, a nonbinding regulatory tool, that gave more extensive treatment to data protection.[107] Creemers noted that the Specification drew "clear inspiration from the GDPR"—the EU's General Data Protection Regulation—with detailed guidance on data collection, storage, and use.[108] Chinese technology expert Samm Sacks wrote that, despite important differences, "the language in the standard is comprehensive and contains more onerous requirements than even the . . . [GDPR]."[109]

China's Civil Code, completed in 2020, gives formal definition to the "right to privacy" as a species of personality rights.[110] In a chapter on "Rights to Privacy and Protection of Personal Information," the Code defines privacy as "the undisturbed private life of a natural person and his private space, private activities, and *private information* that he does not want to be known to others."[111] The chapter states that "no organization or individual may infringe upon" the right to privacy "by prying into, intruding upon, disclosing, or publicizing other[s'] private matters."[112] Notably, the provisions on the right to privacy apply explicitly to personal information.[113] The provisions also mandate data processing requirements similar to those of earlier rules, including consent, necessity, and the right to correction and deletion.[114]

---

[107] Samm Sacks, *New China Data Privacy Standard Looks More Far-Reaching Than GDPR*, CTR. FOR STRATEGIC & INT'L STUD. (Jan. 29, 2018), https://perma.cc/N6CJ-NU9J [hereinafter Sacks, *New China Data Privacy*]; *Translation: China's Personal Information Security Specification*, NEW AM. (Mingli Shi et al. trans., Feb. 8, 2019), https://perma.cc/ZUH4-Y2HQ. For an insightful overview of the CAC as essentially a party institution, see Jamie P. Horsley, *Behind the Façade of China's Cyber Super Regulator*, DIGICHINA (Aug. 8, 2022), https://perma.cc/N5TB-8ZLW. The central government recently established a National Data Administration to develop and regulate data-related infrastructure and resources. *See* Li Yan, *New Data Governance Regulator Unveiled*, CHINA DAILY (Oct. 26, 2023), https://perma.cc/77QZ-3CJ4.

[108] Creemers, *supra* note 20, at 5.

[109] Sacks, *New China Data Privacy*, *supra* note 107; *see also* Samm Sacks, *China's Emerging Data Privacy System and GDPR*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 9, 2018), https://perma.cc/QR44-PJ9H.

[110] Civil Code, *supra* note 31, arts. 1032–39. For scholarly analyses of personality rights in China, see generally CHINESE LAW OF PERSONALITY RIGHTS I: THEORY AND PRACTICE (Wang Liming & Shi Jiayou eds., 2023).

[111] Civil Code, *supra* note 31, art. 1032 (emphasis added).

[112] *Id.*

[113] *Id.* art. 1034 ("The provisions on the right to privacy . . . shall be applied to [ ] private personal information.").

[114] *Id.*, arts. 1034–1038.

In 2021, China's national legislature enacted the Personal Information Protection Law (PIPL), the country's first law dedicated to personal information protection.[115] The PIPL built on many of the data protection principles adopted in earlier laws. Familiar concepts like legality, necessity, and transparency appear again as basic principles.[116] The law limits personal information handling to certain enumerated circumstances, starting with the individual's consent, but extending to other events like public health exigencies.[117] It also creates a separate category of "sensitive personal information," including biometric, health, financial, and location-tracking data, now subject to heightened handling requirements.[118]

By its terms, the PIPL applies to both private actors and state organs.[119] This brings a variety of government institutions, from central ministries to local governments, under the PIPL's data handling requirements.[120] But state organs are exempt from their notification duties where other laws or regulations require "confidentiality," or where "notification will impede State organs' fulfillment of their statutory duties and responsibilities."[121] This exception would almost certainly "apply to national security and law enforcement matters," observed legal scholar Jamie Horsley,[122] opening a sizable gray zone outside the law's notification requirements. Creemers thus saw in this provision "a balance . . . between the need to discipline government departments . . . and the need to ensure that police and security services are not impeded in their surveillance activities."[123]

---

115 Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 1117–25 *translated in Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DIGICHINA (Rogier Creemers & Graham Webster trans., Aug. 20, 2021), https://perma.cc/LV48-GFRH [hereinafter PIPL].

116 *Id.* arts. 5–8.

117 *Id.* arts. 13–15.

118 *Id.* arts. 28–32. This follows a trend in global privacy law. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133–34 (2015).

119 PIPL, *supra* note 115, art. 33.

120 Jamie P. Horsley, *How Will China's Privacy Law Apply to the Chinese State?*, BROOKINGS INST. (Jan. 29, 2021), https://perma.cc/4UGA-CWQK.

121 PIPL, *supra* note 115, art. 35.

122 Horsley, *supra* note 120.

123 Creemers, *supra* note 20, at 6.

The PIPL envisions several modes of enforcement.[124] It requires all personal information handlers to establish internal compliance structures, and, where the amount of personal data handled is high, to appoint personal information protection officers.[125] In case of a data leak or loss, handlers must "immediately adopt remedial measures" and notify relevant departments and individuals.[126] High-volume, complex internet platform services are subject to heightened compliance requirements.[127] Administratively, the law designates the CAC as its central enforcement authority, in charge of issuing rules and standards and overseeing the personal information protection work of designated units at various levels of government.[128] Enforcers may investigate violations and require audits, and can order correction, confiscate income, and impose fines.[129] Individuals may sue when personal information handlers "reject individuals' requests to exercise their rights."[130] And where handlers infringe on "the rights and benefits of many individuals," procuratorates (public prosecutors) and designated consumer organizations may sue as well.[131]

Like the laws and regulations that preceded it, the PIPL draws inspiration from the GDPR. It establishes data minimization principles, subjects certain categories of data to heightened safeguards, and applies extraterritorially to data handling

---

[124] Scholars have since debated whether China's privacy laws ought to be enforced primarily administratively or through private law remedies. *See, e.g.*, Wang Xixin (王锡锌), Geren Xinxi Guojia Baohu Yiwu ji Zhankai (个人信息国家保护义务及展开) [The National Obligation to Protect Personal Information and Potential Paths for Development], 2021 ZHONGGUO FAXUE (中国法学) [Chinese Jurisprudence] 145, 145 (summarizing the debate, and taking the former position).

[125] *See* PIPL, *supra* note 115, arts. 51–56.

[126] *Id.* art. 57.

[127] *Id.* art. 58 (requiring such entities to establish "personal information protection compliance systems"); Graham Greenleaf, *China's Completed Personal Information Protection Law: Rights Plus Cyber-Security* 2–3 (Univ. of New S. Wales L. Rsch. Series, Working Paper No. 21-91, 2021) [hereinafter Greenleaf, *Rights Plus Cyber-Security*].

[128] PIPL, *supra* note 115, arts. 60, 62; *see also id.* arts. 61, 63 (requiring responsible departments to engage in publicity, process complaints and reports, and investigate violations, including through on-site inspections and interviews).

[129] *Id.* arts. 66–71; *id.* art. 68 (stating that, if state organs violate PIPL duties, "superior organs" or other designated departments "shall order correction" and sanction responsible individuals).

[130] *Id.* art. 50.

[131] *Id.* art. 70. This follows a trend of outsourcing enforcement in mass cases to politically approved "NGOs." *See* Yueduan Wang & Ying Xia, *State-Sponsored Activism: How China's Law Reforms Impact NGOs' Legal Practice*, LAW & SOC. INQUIRY, Jan. 12, 2023, at 1, 7–8, 19–24.

outside China.[132] Greenleaf suggested that, as written, the PIPL may be "stronger than the GDPR" in areas like automated decision-making.[133] But the PIPL also departs from foreign data protection laws in notable areas. Several provisions advance the party-state's broader cybersecurity goals, requiring strict security assessments prior to data export.[134] Other provisions sound more in geopolitics, permitting China to retaliate against countries that take "discriminatory" actions, and encouraging the state to "vigorously" shape global data privacy rules.[135] Some might therefore conclude that security and geopolitics are the primary motivations behind China's privacy turn. That, however, would be a mistake. As the next Part will suggest, these motivations have shaped China's data laws generally, but they do not specifically explain why the party-state has begun to protect data privacy.

II. PRIVACY FROM THE TOP DOWN

Part II introduces three interrelated factors that are often said to drive China's turn to privacy law: economics, geopolitics, and security. Privacy laws are thought to promote economic growth by fostering trust in the digital economy. Privacy laws are said to enhance global influence by positioning countries as hubs for global data flows. And privacy laws are thought to advance national security by protecting sensitive national data. All three factors matter in China's privacy story, but in more limited ways than are commonly depicted. This Part clarifies these limitations while suggesting significant gaps that warrant explanation.

A. Development

Among the most cited reasons for China's turn to privacy law is development of its digital economy. A European Parliament report states that China's data privacy laws are "aimed exclusively at the individual as consumer."[136] The report goes on to say that

---

[132] *See* Julia Zhu, *The Personal Information Protection Law: China's Version of the GDPR*?, COLUM. J. TRANSNAT'L L. (Feb. 14, 2022), https://perma.cc/T63Z-3AUS (comparing the two laws).

[133] Greenleaf, *Rights Plus Cyber-Security*, *supra* note 127, at 6; *see also id.* at 2–3 (noting that PIPL provisions include a right to refuse automated decision-making, requirements to provide options "that do not target specific personal characteristics," and bans on automated price discrimination).

[134] PIPL, *supra* note 115, arts. 36–42.

[135] *Id.* arts. 12, 43.

[136] De Hert & Papakonstantinou, *supra* note 21, at 14 (emphasis added).

the "basic [ ] concept [of Chinese] data protection" is that it is "instrumentally necessary for the development of e-commerce."[137] Scholar Emmanuel Pernot-Leplay has similarly said that the main challenge of Chinese data protection law "is to secure the flow of personal data that is vital for the development of the digital economy" without losing state control.[138]

The link between privacy law and development has intuitive appeal. Data protection laws prevent misuse of data, fostering trust and participation in data-intensive industries. As the Center for Global Development put it:

> Effective data protection laws and regulations help build trust in digital tools and systems by establishing *rights* that protect citizens against the misuse of their personal data and *obligations* that require organizations to use data in a fair, transparent, and accountable manner. In theory, this greater trust should translate to greater acceptance of services that rely on data sharing and data use, leading to more investment . . . needed to fuel a country's digital transformation.[139]

Many have echoed this view. European officials have claimed that "a high level of data protection is [ ] crucial to enhance trust in online services and to fulfill the potential of the digital economy."[140] U.S. lawmakers have urged passage of federal privacy law to promote domestic "innovation and competition."[141] Some empirical studies have suggested that stronger privacy protections can increase consumer participation.[142]

---

[137] *Id.* (quotation marks and citation omitted); *see also* Cao Jingchun, *Protecting the Right to Privacy in China*, 36 VICTORIA U. WELLINGTON L. REV. 645, 648 (2005) ("[P]ublic confidence is essential for e-commerce and for the [Chinese] economy to grow.").

[138] Pernot-Leplay, *supra* note 20, at 110.

[139] MICHAEL PISA, PAM DIXON & UGONMA NWANKWO, CTR. FOR GLOB. DEV., WHY DATA PROTECTION MATTERS FOR DEVELOPMENT: THE CASE FOR STRENGTHENING INCLUSION AND REGULATORY CAPACITY 2 (2021) (emphasis in original).

[140] Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INT'L DATA PRIV. L. 119, 124 (2012).

[141] *Wicker, Blackburn Introduce Federal Data Privacy Legislation*, U.S. SENATE COMM. ON COM., SCI., & TRANSP. (July 28, 2021), https://perma.cc/5KCP-BESX [hereinafter *Federal Data Privacy Legislation*].

[142] *See, e.g.*, Miremad Soleymanian, Charles B. Weinberg & Ting Zhu, Privacy Concerns, Economic Benefits, and Consumer Decisions: A Multi-Period Panel Study of Consumer Choices in the Automobile Insurance Industry 45 (Aug. 13, 2021) (on file with author); Mousa Albashrawi & Luvai Motiwalla, *Privacy and Personalization in Continued Usage Intention of Mobile Banking: An Integrating Perspective*, 21 INFO. SYS. FRONTIERS, 1031, 1031–32 (2019).

Beyond doubt, China's leaders are invested in developing the country's digital economy through optimizing data flow and allocation.[143] The government recently designated data as a formal factor of production, joining traditional factors such as land, labor, and capital.[144] And it has made clear that informatization is key to the country's modernization.[145] Some Chinese leaders may also see a supporting role for privacy law specifically in boosting China's digital economy. The party-state's latest Five Year Plan for National Informatization, which focuses in part on "accelerating digitized development," calls at several points for strengthening "privacy protection."[146] Chinese academics have also urged passage of the PIPL on economic grounds.[147]

But for several reasons, China's economic goals are less central to the privacy story than is often depicted. First and most importantly, the privacy grievances borne by China's citizens in recent years, and the injuries policed by China's privacy laws, are not limited to market-related harms. The PIPL, for example, purports to police not only private individuals and firms, but also state organs. As later detailed, scandals involving local government abuse of pandemic-control codes, or recent legislative efforts

---

143 *See* Qiheng Chen, *China Wants to Put Data to Work as an Economic Resource—But How?*, DIGICHINA (Feb. 9, 2022), https://perma.cc/CQ7Q-DXPU. The government's "national big data strategy" is now a decade old. *See* Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUD. COMPAR. INT'L DEV. 45, 48 (2021) [hereinafter Liu, *Data Politics*]; Lindsay Gorman, *China's Data Ambitions*, NAT'L BUREAU FOR ASIAN RSCH. (Aug. 14, 2021), https://perma.cc/6YAA-ACG3.

144 *Zhonggong Zhongyang Guowuyuan Guanyu Goujian Gengjia Wanshan De Yaosu Shichanghua Peizhi Tizhi Jizhi De Yijian* (中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见) [*Opinions of the Central Committee of the Communist Party of China and the State Council on Constructing a More Complete System and Mechanism for the Market-Based Allocation of Production Factors*], XINHUA (Mar. 30, 2020), https://perma.cc/7A7F-H76C.

145 *See generally* STANFORD CYBER POL'Y CTR., TRANSLATION: 14TH FIVE-YEAR PLAN FOR NATIONAL INFORMATIZATION—DEC. 2021 (Rogier Creemers et al. trans., Jan. 24, 2022).

146 *See id.* at 5, 22, 34, 55. Yet even here, privacy does not come off as central to China's economic informatization strategies. Privacy laws are mentioned sparingly in this report, and each time without elaboration and only in formalistic recitations with related concepts such as "data management, sharing, and openness." *Id.* at 22. Experts convened to analyze the Plan make no mention of data privacy either. *See* Rogier Creemers & Paul Triolo, *Analyzing China's 2021–2025 Informatization Plan: A DigiChina Forum*, DIGICHINA (Jan. 24, 2022), https://perma.cc/DE3J-JH2Q.

147 *See, e.g.*, Dai Long (戴龙), *Shuzi Jingji Chanye Yu Shuzi Maoyi Bilei Guizhi: Xianzhuang, Tiaozhan ji Zhongguo Yinying* (数字经济产业与数字贸易壁垒规制：现状、挑战及中国因应) [*The Digital Economy Industry and the Regulation of Digital Trade Barriers: Current Status, Challenges, and China's Responses*], CAIJING WENTI YANJIU (财经问题研究) [STUD. IN FIN. ISSUES] (June 10, 2020), https://perma.cc/YTC2-U7CT (urging the speedier establishment of the PIPL in part to promote digital economic growth).

to end provincial regulations empowering police to search motorist cell phones, do not well conform to a neoliberal story about trust in marketplaces.[148] These events have less to do with fostering China's digital economy and more with pacifying a population that has suffered the costs of a rapidly datafying society.

A predominantly economic model is questionable for other reasons. For one, Chinese e-commerce developed rapidly even in the absence of robust data privacy protections. The industry grew from less than 1% of the global market at the start of the 2010s to the largest e-commerce market in the world, with over 40% of the global market today.[149] Indeed, the size of the Chinese e-commerce market surpassed the U.S. market in 2013, well before most of its data protection laws and regulations were enacted.[150] There is thus little evidence that weak privacy protections have significantly impeded the adoption of online retail services.[151]

To the contrary, privacy law was often discussed as an inhibitor to economic performance. This is a familiar theme here, where privacy competes with values like "efficiency" and "entrepreneurship."[152] Scholars have similarly said that data protection laws "weaken the comparative advantage Chinese firms had over foreign ones in their ability to extract value from data."[153] Tencent's research center has published multiple pieces arguing that that the EU's restrictive data protection laws have hurt its

---

148 *See infra* Part III.B.

149 Liu, *Data Politics*, *supra* note 143, at 48; Dashveenjit Kaur, *China vs. US e-Commerce – How They're Very Different,* TECHWIRE ASIA (Jan. 28, 2021), https://perma.cc/F4AV-KP2V.

150 *China's e-Commerce Revolution*, MORGAN STANLEY RSCH. (Mar. 13, 2015), https://perma.cc/U96Z-3NBZ (comparing China's $314 billion in online sales to America's $244 billion in 2013).

151 *Cf.* SHITONG QIAO, CHINESE SMALL PROPERTY: THE CO-EVOLUTION OF LAW AND SOCIAL NORMS 3 (2017) (documenting a boom in China's rural real estate market despite the absence of formal property rights).

152 Cohen, *What Privacy Is For*, *supra* note 1, at 1904 & n.3; Nicholas Martin, Christian Matt, Crispin Niebel & Knut Blind, *How Data Protection Regulation Affects Startup Innovation*, 21 INFO. SYS. FRONTIERS 1307, 1307 (2019) (reviewing literature). The GDPR is often criticized for slowing growth and stifling innovation. *See* NICK WALLACE & DANIEL CASTRO, CTR. FOR DATA INNOVATION, THE IMPACT OF THE EU'S NEW DATA PROTECTION REGULATION ON AI (Mar. 27, 2018). *But see* Min Jiang & King-Wa Fu, *Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?*, 10 POL. & INTERNET 372, 378 (2018) (criticizing the "false dichotomy between privacy and innovation").

153 Tamar Giladi Shtub & Michal S. Gal, *The Competitive Effects of China's Legal Data Regime*, 18 J. COMP. L. & ECON. 936, 952 (2022). Of course, such effects may also be uneven, hurting smaller businesses more than larger ones that are better able to shoulder compliance costs.

businesses.[154] And Zhang Xinbao, a scholar and data protection adviser to the Chinese government, has acknowledged that the PIPL's "largest impact on data processors is its high compliance costs."[155] In this light, China's turn to privacy law may have even proceeded despite, and not because, of its economic effects.

Finally, an economic story of China's privacy turn does not explain regulators' use of privacy law to impair China's technology giants in 2021. After Ant Group owner Jack Ma chided China's financial regulators in 2020—an event that precipitated the so-called "tech crackdown"—a politically embedded news outlet excoriated Ant for, inter alia, "collecting excessive amounts of consumer data[ ] and infringing personal privacy."[156] Similarly, the CAC's $1.2 billion fine on rideshare giant Didi Chuxing was based principally on violations of data laws, including the PIPL.[157] A growth-based account of Chinese privacy law cannot well explain the use of such law to inflict $1 trillion in losses on the country's technology sector.[158] Here, as in other areas, growth was hardly the main factor in the party-state's turn to privacy law.

B. Geopolitics

China's privacy laws are sometimes framed in geostrategic terms. Compared with economic accounts, geopolitical explanations have been less clear as to how privacy laws advance specific goals. Media accounts that describe China's privacy laws as geopolitical often lack detail.[159] Scholars and analysts have provided more sophisticated accounts, but have focused mostly on the

---

154 Creemers, *supra* note 20, at 4. A China-based executive said in 2018 that "[w]hat will make China be big in AI and big data is: China has no serious law protecting data privacy." Yen Nee Lee, *China Will Win the A.I. Race, According to Credit Suisse*, CNBC NEWS (Mar. 22, 2018), https://perma.cc/8CP8-PGXJ.

155 Shen Yiran (沈怡然), *Zhuanfang "Geren Xinxi Baohu Fa" Canyu Qicao Zhuanjia Zhang Xinbao: Hegui Chengben Hui Tigao, Dan Qiye Meiyou Biyao Danyou* (专访《个人信息保护法》参与起草专家张新宝：合规成本会提高，但企业没有必要担忧) [*Interview with Zhang Xinbao, Expert Drafting Participant of the "Personal Information Protection Law": Compliance Costs Will Increase, but Firms Need Not Worry*], JINGJI GUANCHA BAO (经济观察报) [ECON. OBSERVER] (Sept. 11, 2021), https://perma.cc/FGG2-X3CD.

156 Zhang, *Agility over Stability*, *supra* note 44, at 489.

157 *See infra* note 440.

158 Donny Kwok & Scott Murdoch, *Beijing's Regulatory Crackdown Wipes $1.1 Trillion Off Chinese Big Tech*, REUTERS (July 12, 2023), https://perma.cc/PZ3X-FSV5.

159 *See, e.g.*, Arjun Kharpal, *In a Quest to Rein in Its Tech Giants, China Turns to Data Protection*, CNBC (Apr. 11, 2021), https://perma.cc/R64U-UUSK (describing China's new data privacy laws as having a geopolitical factor amid U.S.-China tensions); Natasha Lomas, *China Passes Data Protection Law*, TECHCRUNCH (Aug. 20, 2021), https://perma.cc/TFD7-37PZ ("Regulating the internet is clearly the new geopolitical battleground.").

geostrategic value of data generally.[160] The aim of this Section is to spell out how privacy law contributes to China's global goals, while also stressing the limits of geopolitics as a primary theory.

Beyond question, China's leaders regard data as a strategic commodity. Government speeches, reports, and articles are replete with such references.[161] According to analyst Emily de La Bruyère, a popular narrative is that new factors of production like data can spur new industrial revolutions, and new industrial revolutions are what alter the global order.[162] "With the digital revolution," states an article in the People's Bank of China's journal, "the world structure will be reshuffled. The countries that are the first to seize the opportunity will rise quickly and occupy a dominant position in the new world order."[163] Chen Wenhui, a leader in China's National Social Security Fund, is even more explicit: "China has a first-mover advantage . . . and is [thus] expected to achieve a revival in the fourth industrial revolution."[164]

China's privacy laws might advance the country's geopolitical goals in two ways. First, they might help China compete for global data flows by providing the assurances needed to secure data transfers from outside China. This is the external analog to the idea that privacy rights undergird participation in the digital economy. But the goals are not only economic. They are geoeconomic, in that stronger privacy laws may help China's leading enterprises better access global trade and data flows to enhance their industrial competitiveness.[165] And they are geostrategic, in that greater access to global data also translates to greater control over data. "Data is revolutionary as a factor of production because control over data promises control over not only

---

[160] *See* Karen M. Sutter, *Capturing the Virtual Domain: The Expansion of Chinese Digital Platforms*, *in* CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER 23, 28–29 (Emily de La Bruyère et al. eds., 2022) (discussing the PIPL in relation to China's global economic ambitions) [hereinafter CHINA'S DIGITAL AMBITIONS]; *infra* note 165.

[161] *See, e.g.*, *Hearing on Promoting Competition, Growth, and Privacy Protection in the Technology Sector Before the S. Fin. Subcomm. on Fiscal Resp. & Econ. Growth*, 117th Cong. 1–2 (2021) (testimony of Samm Sacks, Senior Fellow, Paul Tsai China Ctr. at Yale L. Sch.) [hereinafter Sacks Testimony]; *Translation: Big Data Security White Paper 2018*, DIGICHINA (Graham Webster et al. trans., July 31, 2018), https://perma.cc/QX44-JRCQ ("Big data is progressively becoming a national basic strategic resource.").

[162] Emily de La Bruyère, *Introduction* to CHINA'S DIGITAL AMBITIONS, *supra* note 160, at 1, 4.

[163] *Id.*

[164] *Id.*

[165] *See* Gorman, *supra* note 143 (describing the PIPL as an effort to bolster "data-driven economic innovation" alongside an "external push to . . . vacuum up global data").

production but also distribution and consumption of other resources," explained La Bruyère.[166] "In a digital environment, power is therefore a function of both capturing data and controlling the architecture of digital exchange."[167]

More concretely, China's geostrategic outlook on privacy has been shaped by international trends in data protection. Whether because of the EU's market power, its regulatory capacity, or the substantive appeal of its regulatory approach, many countries have, in recent years, modeled their privacy laws on the GDPR.[168] Greenleaf found that 145 countries had enacted data privacy laws by the start of 2021, and that "most of these laws [were] influenced substantially by the EU's GDPR."[169] In addition, as scholars Anupam Chander and Paul Schwartz have found, dozens of laws in and outside the EU now condition data exports on the "adequacy" of recipient data privacy laws, creating additional incentives for nations to align their data protections laws with global standards.[170] Against this backdrop, China has felt competitive pressures to enact comparable legislation lest it lose access to critical data flows.[171] Local commentators have defended the PIPL as a means of promoting international trust through following an unmistakable "global trend" in privacy legislation.[172]

The second way China's privacy laws might advance global goals follows from the first. By becoming a major data protection

---

166 La Bruyère, *supra* note 162, at 5.

167 *Id.* at 5.

168 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 778–83, 810–17 (2019); Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 5, 23–26 (2012) (pointing to various "conditions under which a single country can externalize its regulations on other countries"); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 176 (2006) (attributing the EU's external legal influence to its "enormous market power and its unusual concern for its citizen[s'] privacy"). *But see* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734, 1781–92 (2021) (arguing that California has emerged as an alternate "dark horse contender").

169 Graham Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, 176 PRIV. L. & BUS. INT'L REP. 1, 1 (2022).

170 Anupam Chander & Paul Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49, 74, 126–34 app. A (2023) (finding sixty-five countries outside the EU "whose data laws permit or require adequacy reviews of foreign jurisdictions").

171 *See* Sacks Testimony, *supra* note 161, at 4 (citing scholar Hong Yanqing on the importance of preserving "access to global data flows").

172 Yu Xiaoyang (于晓洋) & He Bo (何波), *Woguo "Geren Xinxi Baohu Fa" Lifa Beijing Yu Zhidu Xiangjie* (我国《个人信息保护法》立法背景与制度详解) [*A Detailed Explanation of the Legislative Background and Institutions of Our Country's "Personal Information Protection Law"*], 8 DASHUJU (大数据) [BIG DATA RSCH.] 168, 171 (2022) (citing the 128 countries that have enacted such laws).

player, China may be in a better position to shape global data governance norms in self-interested ways. Whereas the first factor is rooted primarily in attraction and norm-taking, the second is rooted in influence and norm-making.[173]

China's interest in shaping global standards has been well documented.[174] In data governance, scholars have emphasized China's focus on data sovereignty, the assertion of "traditional state sovereignty over the online domain."[175] Data sovereignty is thought to preserve political security by maintaining regime control over what citizens and outsiders can access and use.[176] A number of scholars have described data sovereignty as the most distinctive aspect of Chinese data governance for export.[177] They have shown how China has sought to shape transnational data norms through a number of "push" and "pull" factors, from the promotion of data sovereignty in global forums to Chinese firms' export of digital infrastructures to other countries.[178]

It follows that China has strong reason to establish in its own laws a degree of credibility and interoperability with foreign data privacy regimes. In order to shape norms, China may be better off building on what is already common.[179] As a data protection latecomer, China cannot hope to create "law . . . for the world" any

---

[173] There is a broader debate on the extent to which China is a rule taker, shaper, or breaker. *See, e.g.*, Margaret K. Lewis, *Why China Should Unsign the International Covenant on Civil and Political Rights*, 53 VAND. J. TRANSNAT'L L. 131, 203 (2020) (portraying China as a norm disruptor). *See generally* SCOTT KENNEDY & SHUAIHUA CHENG, FROM RULE TAKERS TO RULE MAKERS: THE GROWING ROLE OF CHINESE IN GLOBAL GOVERNANCE (2012).

[174] *See, e.g.*, RUSH DOSHI, THE LONG GAME: CHINA'S GRAND STRATEGY TO DISPLACE AMERICAN ORDER 328 (2021); COHEN, BETWEEN TRUTH AND POWER, *supra* note 34, at 226.

[175] Anupam Chander & Haochen Sun, *Sovereignty 2.0*, 55 VAND. J. TRANSNAT'L L. 283, 292–93 (2022) (defining data sovereignty broadly "to cover a state's sovereign power to regulate not only cross-border flow of data through uses of internet filtering technologies and data localization mandates, but also speech activities . . . and access to technologies").

[176] *See infra* Part II.C. National security may also encompass examination of foreign data for anti-Chinese perspectives. *See* TOM GINSBURG, DEMOCRACIES AND INTERNATIONAL LAW 256–62 (2021).

[177] *See, e.g.*, ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY 292 (2023); Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance*, 54 NYU J. INT'L L. & POL. 1, 24–35 (2021).

[178] Erie & Streinz, *supra* note 177, at 21–24; BRADFORD, *supra* note 177 at 292; Nigel Cory, *Writing the Rules: Redefining Norms of Global Digital Governance*, *in* CHINA'S DIGITAL AMBITIONS, *supra* note 160, at 73, 80–83.

[179] *See* Jonathan E. Hillman, *A "China Model?" Beijing's Promotion of Alternative Global Norms and Standards*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 13, 2020), https://perma.cc/9V7V-GTK3 (describing China's efforts in existing institutions); Mark Jia, *Special Courts, Global China*, 62 VA. J. INT'L L. 559, 594 (2022) [hereinafter Jia, *Special Courts*] (describing recognition among officials that the global influence of China's judiciary depends in part on its global appeal).

time soon.[180] But by hitching onto a rubric that is becoming universal, it might better position itself to nudge next-generation global data protection norms in self-interested directions.

As with economic accounts, geopolitical factors are a part of China's privacy turn. The problem with geopolitics as a primary theory, however, is that it ignores too much. By envisioning the party-state as a domestically unconstrained and external-facing actor, a geopolitical account privileges reductionism over sociological complexity. Geopolitics cannot explain the use of privacy law in China's domestic campaigns. Geopolitics cannot account for why draft privacy legislation began in the early 2000s, before the leadership endorsed data's geostrategic value or began promoting cyber sovereignty principles abroad.[181] And geopolitics has little to say about abusive data practices that have sparked national outrage. In 2021, a major Party body named "violations of citizens' personal information" as a risk factor for social instability.[182] Internal stability remains of paramount importance in understanding legal developments today.[183]

C. Security

Finally, China's privacy laws are often understood as national security measures. One National Bureau of Asian Research report states briefly that the PIPL "nods" to the GDPR before stressing how "[i]n practice, it strengthens data localization" and provides "the foundation for a blacklist that would ban certain overseas data controllers and processors."[184] Another report repeatedly portrays the PIPL as primarily targeted toward security

---

180 Schwartz, *supra* note 168, at 772.

181 *See* Cory, *supra* note 178, at 75 (noting that China has only recently begun to advocate for "cyber sovereignty" in international data governance).

182 *Zhonggong Zhongyang Bangongting Guowuyuan Bangongting Yinfa "Guanyu Zuohao 2021 Nian Yuandan Chunjie Qijian Youguan Gongzuo De Tongzhi* (中共中央办公厅 国务院办公厅印发《关于做好 2021 年元旦春节期间有关工作的通知》) [*The General Office of the Chinese Communist Party Central Committee and the State Council General Office Issues a "Notice Relating to Performing Good Work During New Year's Day and the 2021 Spring Festival"*], XINHUA (Dec. 24, 2020), https://perma.cc/KMF4-CDTV.

183 *See* Benjamin L. Liebman, *Legal Reform: China's Law-Stability Paradox*, 143 DAEDALUS, Spring 2014, at 96, 96; Willy Wo-Lap Lam, *"Stability Maintenance" Gets a Major Boost at the National People's Congress*, JAMESTOWN FOUND. (Mar. 22, 2019), https://perma.cc/3SWF-S622. *See generally* THE POLITICS OF LAW AND STABILITY IN CHINA (Susan Trevaskes et al. eds., 2014).

184 Gorman, *supra* note 143.

and control.[185] These works are not wrong for what they say, but they can be misleading for what they miss. Security concerns underlie all of China's framework data policies, but they are not the main reason for China's turn to privacy law in particular.

National security is a major pillar of Chinese digital governance.[186] China's leaders regard cybersecurity (*wangluo anquan*) as key to China's national security, and have been for many years broadening "the Chinese security paradigm in order to safeguard the programmatic objectives of the Party-state."[187] As understood here, cybersecurity is closely related to the idea of data sovereignty. Both are rooted in ideas of territorial sovereignty and defended on grounds of "national and ideological security."[188] State security concerns range from combatting traditional threats like terrorism to censoring "inappropriate and illegal content that threatens core socialist values."[189] They are evident in each of China's major data laws today. The Cybersecurity Law requires "critical information infrastructure" to establish internal security management processes and localize large categories of data.[190] The Data Security Law calls for establishing a "graded protection system for data" based in part on risks to national security and requires stricter handling of "core national data," including "[d]ata related to national security."[191] The PIPL also mandates

---

[185] *See* Samantha Hoffman, *Securing the Foundation: Building the Physical Infrastructure of the Digital World*, *in* CHINA'S DIGITAL AMBITIONS, *supra* note 160, at 11, 15; Sutter, *supra* note 160, at 29; Cory, *supra* note 178, at 76.

[186] Henry S. Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND GLOBAL TRADE LAW 245, 261 (Mira Burri ed., 2021) ("The key to understand data regulation in China . . . must be 'security.'"). For more on General Secretary Xi Jinping's "comprehensive national security concept," see generally Hearing on the United States' Strategic Competition with China Before the S. Armed Servs. Comm., 117th Cong. 1–8 (2021) (testimony of Sheena Chestnut Greitens, Assoc. Professor, Univ. of Tex. at Austin).

[187] Rogier Creemers, *Cybersecurity Law and Regulation in China: Securing the Smart State*, 6 CHINA L. & SOC. REV. 111, 111–13 (2023).

[188] Chander & Sun, *supra* note 175, at 295; *see also id.* at 296.

[189] Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 397, 466 (2020); Jonathan Zittrain & Benjamin Edelman, *Internet Filtering in China*, IEEE INTERNET COMPUTING, Mar./Apr. 2003, at 70, 70–74 (categorizing types of internet content censored by the Chinese government).

[190] Cybersecurity Law, *supra* note 103, arts. 21, 31, 37; Erie & Streinz, *supra* note 177, at 27–34. "Critical information infrastructure" refers to information networks in areas like power, traffic, water, finance, and public broadcasting. Cybersecurity Law, *supra* note 103, art. 31.

[191] Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), art. 21, 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 951, 953 *translated in Translation: Data Security*

data localization while empowering the CAC to blacklist foreign information handlers who endanger national security.[192]

There is a narrower, more relevant, sense in which privacy law can reinforce security objectives. By mandating stricter guardianship of personal data, privacy laws can impede the unauthorized access and use of such data by foreign or domestic agents with antagonistic agendas. Consider China's investigation of the ride-hailing firm Didi, which had an extensive repository of personal data with potential security implications, including—one would imagine—the user locations and facial recognition information of government officials and corporate leaders.[193] Privacy and national security goals are thus intertwined.[194] In the United States, there is no better illustration than the theft of federal personnel files by Chinese hackers in 2015—a breach that compromised the social security numbers, fingerprint records, and security clearance data of millions of federal employees.[195] A key point here, as noted by Chinese scholars, is that privacy harms are not national security harms in every case—the more sensitive the parties and the data, the more likely privacy and security concerns overlap.[196]

The problem with existing accounts is not that they accurately identify national security as an animating principle of Chinese data governance. Rather, it is that they ignore or underemphasize how China's privacy laws, which are but one component of its data governance, are driven by other important interests. Putting aside the limited synergy between privacy and

---

Law of the People's Republic of China (Effective Sept. 1, 2021), DIGICHINA (Emma Rafaelof et al. trans., June 29, 2021), https://perma.cc/QG5M-SDST.

192 PIPL, *supra* note 115, arts. 36, 40, 42.

193 Raymond Zhong, *China's Crackdown on Didi Is a Reminder That Beijing Is in Charge*, N.Y. TIMES (July 5, 2021), https://www.nytimes.com/2021/07/05/technology/china-didi-crackdown.html; Eva Dou & Pei-Lin Wu, *China Fines Didi $1.2 Billion for Breaking Data-Security Law*, WASH. POST (July 21, 2022), https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/.

194 *See* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED: WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 131–33 (2022); Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation Is Just a Start*, BROOKINGS (Dec. 1, 2020), https://perma.cc/K2GK-T4ZC.

195 *See* SOLOVE & HARTZOG, *supra* note 194, at 128–31.

196 *See* Zhu Xuezhong (朱雪忠) & Dai Zhizai (代志在), *Zongti Guojia Anquan Guanshi Yuxia "Shuju Anquan Fa" De Jiazhi Yu Tixi Dingwei* (总体国家安全观视域下《数据安全法》的价值与体系定位) [*The Value and Systemic Role of the "Data Security Law" from a National Security Perspective*], 2020 DIANZI ZHENGWU (电子政务) [E-GOVERNMENT] 82, 90 (suggesting that personal information has security implications where "data violations involve the personal information of special individuals and their close relatives that are related to national security").

national security, there are a number of major privacy developments that a security framework does not well explain, from modest state-imposed limits on police discretion to the state's enforcement focus on mundane cases of data theft, most of which have hardly any national security implications at all.[197] In Party General Secretary Xi Jinping's recent report to the Twentieth Party Congress, a major quinquennial event,[198] the sole mention of data privacy—a call to strengthen personal information protection—appears alongside promises to improve workplace, food, and drug safety.[199] The party-state's turn to privacy law is thus better modeled as a kind of social protection. Such laws are not principally about repelling foreign agents or quelling domestic agitators. They are about people, their grievances, and the policy imperatives that flow from the party-state's legitimation needs. The next Part will address these demands in substantially more depth.

III. PRIVACY FROM THE BOTTOM UP

Part III introduces an underemphasized factor underlying China's turn to privacy law: popular legitimation. Section A describes how the party-state's informatization strategies have produced vulnerabilities for its citizens that evoke and surpass those faced by citizens elsewhere. Section B shows through scandals, message boards, campaigns, and surveys how these vulnerabilities have generated significant social discontent over data abuse. Section C then reviews a range of party-state documents to show that a central purpose of China's privacy laws is to enhance the party-state's legitimacy by co-opting privacy and framing the party-state as privacy's primary protector.

---

197 *See infra* Part III.C.

198 The report to the Party Congress is a "critically important indication of Beijing's intentions and goals" and is regularly scrutinized by commentators. Shannon Tiezzi, *What to Watch for at the 20th Party Congress: The Work Report*, DIPLOMAT (Oct. 7, 2022), https://perma.cc/3DLZ-HGNC; *see also infra* note 321; *Key Takeaways from Xi's Report to the Party Congress*, MERCATOR INST. FOR CHINA STUD. (Oct. 20, 2022), https://perma.cc/3ZY4-YCE8 (providing a quantitative analysis of General Secretary Xi's report to the Twentieth Party Congress).

199 XI JINPING, HOLD HIGH THE GREAT BANNER OF SOCIALISM WITH CHINESE CHARACTERISTICS AND STRIVE IN UNITY TO BUILD A MODERN SOCIALIST COUNTRY IN ALL RESPECTS 46–47 (P.R.C. Ministry of Foreign Affs. trans., Oct. 16, 2022) (available at https://perma.cc/JG93-NUPE).

A. Datafication in China

China has datafied at a dizzying rate.[200] Much of this has been driven by forces that have shaped political economies across the world, as new technologies and profit motives have facilitated a broader "transformation from industrial to informational capitalism."[201] As elsewhere, China's growth in data flows can be attributed to surging demand for data in industries such as advertising, credit reporting, personal lending, and marketing, and to skyrocketing supply in data from social media platforms, e-commerce firms, and other web-based applications.[202] Chinese firms have applied sophisticated means of harvesting, refining, and marketizing personal data, and platforms have emerged as major intermediated sites for data capture and extraction.[203]

With datafication has come new vulnerabilities and dependencies. Like their counterparts abroad, China's citizens have transferred large amounts of personal data to private firms and state organs.[204] Similar to foreign firms, China's digital businesses have designed their interfaces to monopolize user attention and to encourage data disclosure.[205] And as elsewhere, sharing sensitive personal data is an increasingly unavoidable condition of participation in Chinese society. "Such exposure is necessary to participate in a digital networked society,"[206] where even "the most ordinary tasks . . . expose [people] to surveillance and data collection."[207]

---

[200] "Datafication" refers to the process of "taking all aspects of life and turning them into data." Kenneth Cukier & Viktor Mayer-Schoenberger, *The Rise of Big Data*, FOREIGN AFFS., May/June 2013, at 28, 35 (distinguishing between datafication and digitization).

[201] COHEN, BETWEEN TRUTH AND POWER, *supra* note 34, at 5; *see* Cohen, *What Privacy Is For*, *supra* note 1, at 1915 (defining "informational capitalism" based on sociologist Manuel Castells's notion of "the alignment of capitalism as a mode of production with informationalism as a mode of development").

[202] *See* Dong Han, *The Market Value of Who We Are: The Flow of Personal Data and Its Regulation in China*, MEDIA & COMMC'N, Apr. 12, 2017, at 21, 22; MARTIN CHORZEMPA, THE CASHLESS REVOLUTION 71–108 (2022) (chronicling the rise of mobile payment apps and fintech in China).

[203] *See* COHEN, BETWEEN TRUTH AND POWER, *supra* note 34, at 63–65 (describing the process of data extraction and refinement).

[204] *See* Liu, *Data Politics*, *supra* note 143, at 48; KAI-FU LEE, AI SUPERPOWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER 16–17 (2018).

[205] *See* COHEN, BETWEEN TRUTH AND POWER, *supra* note 34, at 42–44 (describing how platform providers "become and remain the indispensable point of intermediation for parties in [their] target markets"); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 12 (2020).

[206] Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 969 (2021).

[207] Balkin, *supra* note 205, at 13 (writing of the United States).

But while aspects of this story are familiar, China's citizens have been in other ways more vulnerable to privacy intrusions than their foreign counterparts. Part of it is the quantity of data that is created and replicated in China, now the world's leading data generator.[208] One study found that in 2018, China generated 7.6 zettabytes (ZB) of data, exceeding the 6.9 ZB generated in the United States that same year.[209] The same study predicted that by 2025, China and the United States would each generate 48.6 ZB and 30.6 ZB, respectively.[210] Important too has been the speed of datafication, which has outpaced changes in laws and regulations. Consider that much of China's population did not own personal computers before acquiring smartphones, having transitioned directly into a "mobile-first mobile-only era."[211]

China's greater, faster datafication has been driven by both state and private actors. As early as the 1990s, China's policymakers pursued an explicit policy of "informatization" (*xinxihua*), "the introduction of digital technologies in social, economic, and political life."[212] Its aims—improving governance, enhancing control, and promoting development—have led to data-generative activities and vulnerabilities in an array of areas. Governance-related initiatives have included the digitization of millions of state documents, from case judgments to land records, and the creation of online portals collecting comments on draft legislation and corruption tips.[213] More than digitization, China's planners are keen to join personal information like facial recognition data with other inputs. The city of Hangzhou, for example, has ceded traffic control in some areas to an AI system that integrates personal location, traffic, and surveillance data from across the city.[214] Smart city technologies have several beneficial aims, from

---

[208] Sintia Radu, *Which Country Owns Data? Increasingly, It's China*, U.S. NEWS (Feb. 14, 2019), https://www.usnews.com/news/best-countries/articles/2019-02-14/china-overtook-the-us-and-will-hold-the-largest-share-of-worlds-data-at-least-by-2025.

[209] Saheli Roy Choudhury, *As Information Increasingly Drives Economies, China Is Set to Overtake the US in the Race for Data*, CNBC (Feb. 13, 2019), https://perma.cc/H2ZR-KYJA. A zettabyte is approximately a trillion gigabytes. *Id.*

[210] *Id.*

[211] Winston Wenyan Ma, *The Chinese Have Transitioned Directly to a Mobile-Only Era*, LONDON SCH. ECON. & POL. SCI. (Jan. 19, 2017), https://perma.cc/Y55L-VYBS.

[212] Creemers, *supra* note 20, at 2.

[213] DIMITAR D. GUEORGUIEV, RETROFITTING LENINISM: PARTICIPATION WITHOUT DEMOCRACY IN CHINA 74–75, 133–34 (2021).

[214] Abigail Beall, *In China, Alibaba's Data-Hungry AI Is Controlling (and Watching) Cities*, WIRED (May 30, 2010), https://perma.cc/8FJU-DHFN; JOSH CHIN & LIZA LIN, SURVEILLANCE STATE: INSIDE CHINA'S QUEST TO LAUNCH A NEW ERA OF SOCIAL CONTROL 124–25 (2022).

managing congestion to finding lost children.[215] But they have also required the collection and use of immense amounts of personal data, significantly more than most foreign citizens have experienced.

A related cause of data creation and vulnerability stems from state-led efforts to "reinvent social control through technology."[216] China's leaders have made enormous investments in surveillance technologies.[217] These include not only tools of visual surveillance (China has over half of the world's almost one billion surveillance cameras), but also phone trackers to "connect one's digital footprint, real-life identity, and physical whereabouts" and large-scale iris-scan and DNA databases.[218] These technologies are used for varying legal and extralegal purposes, from profiling Uyghurs, a persecuted ethnic group in Xinjiang, to locating fugitives in a crowd.[219] The state has also deployed its surveillance technologies for pandemic control. Residents have had to download mobile software that determined, based on personal location and other data, whether they had to quarantine or could access public venues.[220] The application fed this data directly to the police.[221]

Perhaps the most widely known aspect of the party-state's digital control policies has been the social credit system.[222] In its pilot phase, social credit has consisted mostly of state-compiled blacklists that punish unlawful conduct.[223] The archetypal case is a ban on high-speed rail travel for someone who has failed to pay

---

215 CHIN & LIN, *supra* note 214, at 116.

216 *Id.* at 6.

217 *See* Isabelle Qian, Muyi Xiao, Paul Mozur & Alexander Cardia, *Four Takeaways from a Times Investigation into China's Expanding Surveillance State*, N.Y. TIMES (June 21, 2022), https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

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

219 Mozur, *supra* note 218; Anna Fifield, *Chinese Police Sniff Out a Fugitive—Literally—in the Case of the Telltale Hot Pot*, WASH. POST (Sept. 12, 2019), https://www.washingtonpost.com/world/asia_pacific/chinese-police-sniff-out-a-fugitive--literally--in-the-case-of-the-telltale-hot-pot/2019/09/12/86db31a8-d521-11e9-ab26-e6dbebac45d3_story.html.

220 Paul Mozur, Raymond Zhong & Aaron Krolik, *In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags*, N.Y. TIMES (July 26, 2021), https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

221 *Id.*

222 *See generally* Xin Dai, *Toward a Reputation State: A Comprehensive View of China's Social Credit System Project*, *in* SOCIAL CREDIT RATING: REPUTATION UND VERTRAUEN BEURTEILEN 139 (Oliver Everling ed., 2020); Jeremy Daum, *Far from a Panopticon, Social Credit Focuses on Legal Violations*, JAMESTOWN CHINA BRIEF, Oct. 8, 2021, at 6, 8–9.

223 Louise Matsakis, *How the West Got China's Social Credit System Wrong*, WIRED (July 29, 2019), https://perma.cc/VS25-WJAT.

a court judgment.[224] Some local experiments have gone further by assigning scores to individuals and firms for a variety of offenses.[225] While national regulations are still evolving,[226] what is clear at this stage is that social credit requires state authorities to integrate large amounts of personal data.[227] These data-sharing processes have been criticized for potential or actual misuse.[228] Local officials have at times expressed a desire for clearer authorizing mandates to avoid the legal or disciplinary risks associated with data breaches stemming from their social credit work.[229]

Finally, the party-state's development goals have also contributed to datafication and dependency. For many years, China's leaders largely stayed their hand when it came to regulating the country's technology firms, content to let the private sector drive digital growth under the auspices of national development policy.[230] Law scholar Angela Zhang has explained how this "lax regulatory environment" allowed the pursuit of data and profit to proceed more or less unencumbered, buoyed by preferential tax schemes and state-sponsored incubators.[231] Platforms amassed immense troves of online user data while other data processors began collecting information from the physical world at a rate that outstripped their counterparts in other countries.[232] Firms like Alibaba, Tencent, and Baidu found that they could "boast deeper insight into the lives of their users than Facebook, Google, and Amazon."[233] According to communications scholar Dong Han,

---

224 *Id.*

225 *Id.*; Dai, *supra* note 222, at 151–52 (describing various local scoring schemes).

226 Zeyi Yang, *China Just Announced a New Social Credit Law. Here's What It Means*, MIT TECH. REV. (Nov. 22, 2022), https://perma.cc/9LYA-W4PF.

227 Nicole Kobie, *The Complicated Truth About China's Social Credit System*, WIRED (July 6, 2019), https://perma.cc/9MAW-BT6K.

228 Xinmei Shen, *China's Social Credit System Shows First Signs of Abuse, Report Says*, S. CHINA MORNING POST (Dec. 10, 2019), https://www.scmp.com/abacus/news-bites/article/3041520/chinas-social-credit-system-shows-first-signs-abuse-report-says.

229 Interview with Beijing-Based Legal Academic, Feb. 1, 2023 (on file with author); *cf.* Chen Daofu (陈道富) & Cao Shengxi (曹胜熙), *Woguo Shehui Xinyong Tixi Jianshe de Jinzhan, Wenti Yu Duice Jianyi* (我国社会信用体系建设的进展、问题与对策建议) [*Suggestions on Our Country's Social Credit System's Progress, Problems, and Countermeasures*], ZHONGGUO JINGJI PINGLUN (中国经济评论) [CHINA ECON. REV.] (2022) (noting the need for more "top-level legislation" for social credit).

230 Zhang, High Wire, *supra* note 42, at 77–78; CHORZEMPA, *supra* note 202, at 65.

231 Zhang, High Wire, *supra* note 42, at 12, 57; *see also* CHIN & LIN, *supra* note 214, at 105 ("As long as they obeyed censorship orders, internet companies were left pretty much to do as they pleased.").

232 LEE, *supra* note 204, at 56, 79.

233 CHIN & LIN, *supra* note 214, at 104, 112.

"commercial experiments on personal data in China [were] beyond what would be tolerated under the laws of major Western countries."[234]

B. Data Abuse and Popular Politics

China's datafication era has been marked by popular discontent over intrusive data practices. A review of the available, albeit limited, survey evidence helps set the scene. In 1997, before most Chinese citizens could access the internet, a survey of residents from five large Chinese cities "showed significant public awareness of privacy" generally.[235] For example, a large majority of respondents agreed with statements like "[p]arents should not read their child's diary."[236] In 2006, as more of the country came online, a media survey found that approximately 92% of respondents were "worried that their private information can be too easily divulged and misused," and that 74% favored stricter laws protecting personal privacy.[237] By 2019, a Chinese think tank survey of 6,100 respondents found that over 80% of respondents desired more control over their data, and 75% wanted the option of traditional identification methods over facial recognition technology (FRT).[238] Interestingly, a 2019 survey of 6,600 online users found that Chinese respondents accepted private sector use of FRT at a *lower* rate (17%) than did users in the United Kingdom (20%) and the United States (30%).[239]

A closer way to track shifts in social sentiment is through studying flashpoints, where particular events or controversies cause public opinion to flare. Flashpoints are useful analytically because they can help reveal dormant social frustrations. Because flashpoints are amplified by media, they also receive attention, even scrutiny, from policymakers.[240] In nondemocratic societies,

---

234 Han, *supra* note 202, at 26.

235 McDougall, *Functions and Values*, *supra* note 57, at 167 (citing a poll of residents of Beijing, Shanghai, Guangdong, Chongqing, and Xiamen).

236 *Id.*

237 Farrall, *supra* note 51, at 1009.

238 Genia Kostka, Léa Steinacker & Miriam Meckel, *Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States*, 30 PUB. UNDERSTANDING SCI. 671, 674 (2021).

239 *Id.* at 681.

240 *See* Greg Distelhorst, Diana Fu & Yue Hou, *Making Chinese Officials Accountable, Blog by Blog*, BOS. REV. (Sept. 27, 2016), https://perma.cc/6BK8-6736 (describing the role of media in "publicity-driven accountability in contemporary China").

flashpoints are useful signals of popular opinion, helping the state to determine policy priorities and to orchestrate responses.[241]

China's informatization era has seen public sentiment rise against a number of privacy-related abuses. One notable flashpoint was the 2016 death of Xu Yuyu, an 18-year-old student from Shandong Province.[242] The summer before Xu was to start college, a scammer used her personal details to trick her out of her college tuition savings, money her father had cobbled together as a day laborer.[243] She died of a heart attack upon learning what had happened.[244] Xu's death "triggered an explosion of reactions on media and social media."[245] A widely circulated news story emphasizes Xu's academic promise and her modest background.[246] Alongside images of Xu celebrating her birthday, the story includes an extensive discussion of data privacy. It describes how Xu's death "sparked societal discussion of personal information leakage," and how the head of the university where Xu would have enrolled had publicly urged enactment of a personal information protection law in the wake of her death.[247]

The scam that ensnared Xu was no outlier. A student from a neighboring district had lost his tuition money to a similar scam at around the same time.[248] Education was a particularly common and poignant area of data abuse, not least because of its cultural-economic importance in China. In one prominent case, six defendants were convicted and sentenced in 2016 for selling the data of two million students and parents.[249] Beyond education, general data theft has been fueled by the growth of an enormous

---

241 *See generally* Seva Gunitsky, *Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability*, 13 PERSPS. ON POL. 42, 42 (2015). Since the early 2000s, the internet has been a leading forum for airing public grievances in China. *See* GUOBIN YANG, THE POWER OF THE INTERNET IN CHINA: CITIZEN ACTIVISM ONLINE 4 (2009); Rebecca MacKinnon, *Liberation Technology: China's "Networked Authoritarianism,"* J. DEMOCRACY, Apr. 2011, at 32, 33. *See generally* RONGBIN HAN, CONTESTING CYBERSPACE IN CHINA: ONLINE EXPRESSION AND AUTHORITARIAN RESILIENCE (2018).

242 Li Xingli (李兴丽), Zhang Wei (张维), Wang Yu (王煜), Zhang Diyang (张笛扬), Cao Huiru (曹慧茹) & Gong Chenxia (龚晨霞), *Diaocha: Xu Yuyu Shenbian Haiyou Henduoren Jiedaoguo Leisi Zhapian Dianhua* (调查：徐玉玉身边还有很多人接到过类似诈骗电话) [*Investigation: Many People Around Xu Yuyu Received Similar Fraudulent Calls*], XINJINGBAO (新京报) [BEIJING NEWS] (Aug. 25, 2016), https://perma.cc/6SQP-KSXN.

243 *Id.*

244 *Id.*

245 Fan Yiying, *Jail Time for China's Personal Data Thieves*, SIXTH TONE (Aug. 25, 2016), https://perma.cc/B2GZ-EJZF.

246 Li et al., *supra* note 242.

247 *Id.*

248 *Id.*

249 Fan, *supra* note 245.

underground industry.[250] A 2016 survey found "that no less than 84% of respondents said they had suffered some form of data theft."[251] Other high-profile cases include a leak of six hundred million resumes from a headhunter, the theft of 130 million hotel guests' personal details,[252] and the leak of possibly a billion people's personal information from a Shanghai police database.[253] The year Xu died, data leaks were estimated to have caused 91.5 billion RMB ($13.3 billion) in losses.[254]

The theft of biometric information has been of particular concern. In one widely read story, journalists discovered that vendors on e-commerce platforms like Taobao and Xianyu were selling facial data, along with other identifying information, for as little as half an RMB a piece.[255] For 35 RMB ($4), a vendor would include editing software that could manipulate facial features and expressions.[256] The phrase "[f]ace information is sold for 0.5 [RMB] a copy" quickly became a trending hashtag on Weibo, China's equivalent to X (formerly known as Twitter).[257] Users lamented how easy it was for such data to be exchanged, with some demanding that lawmaking on "biometric information protection" proceed at a greater pace.[258]

Other flashpoints have revolved around private sector data practices. In 2019, users publicly assailed Zao—a viral face-swapping app that used AI technology to upload users' faces into famous movie scenes—for its privacy policies.[259] Netizens

---

[250] Han, *supra* note 202, at 21.

[251] *In China, Consumers Are Becoming More Anxious About Data Privacy*, ECONOMIST (Jan. 25, 2018), https://perma.cc/9XB8-CRAH [hereinafter *Consumers Anxious About Privacy*].

[252] Lim Yan Liang, *China's Data Scandals Prompt Stiffer Laws*, STRAITS TIMES (June 30, 2019), https://perma.cc/9E2Z-YM8L.

[253] John Liu, Paul Mozur & Kalley Huang, *In a Big Potential Breach, a Hacker Offers to Sell a Chinese Police Database*, N.Y. TIMES (July 5, 2022), https://www.nytimes.com/2022/07/05/business/china-police-data-breach.html.

[254] Han, *supra* note 202, at 26 (showing losses in a one-year span between mid-2015 and mid-2016).

[255] Yan Zhihong (颜之宏), Yan Hongxin (闫红心) & Chen Yuxuan (陈宇轩), *0.5 Yuan Yifen! Shei Zai Chumai Women De Renlian Xinxi?* (0.5 元一份！谁在出卖我们的人脸信息？) [*0.5 Yuan a Copy! Who Is Selling My Facial Data?*], XINHUA (July 13, 2020), https://perma.cc/KWK9-7UJ2.

[256] *Id.*

[257] Sina Technology, WEIBO (July 13, 2020), https://s.weibo.com/weibo?q=%23%E4%BA%BA%E8%84%B8%E4%BF%A1%E6%81%AF0.5%E5%85%83%E4%B8%80%E4%BB%BD%E5%87%BA%E5%94%AE%23 ("#人脸信息 0.5 元一份出售#") ["#[F]ace information is sold for 0.5 yuan a copy#"].

[258] *Id.*

[259] *Chinese Deepfake App Zao Sparks Privacy Row After Going Viral*, GUARDIAN (Sept. 2, 2019), https://perma.cc/F8XB-HT4G.

discovered that Zao's user agreement granted it "completely free," "irrevocable," and "perpetual" rights to all uploaded content.[260] In effect, this meant Zao could retain all facial images and sell them to third parties without consent. "Furious comments flooded" Apple's Chinese app store, lowering Zao's star rating to two stars out of five, and several attorneys called for a boycott.[261] Zao apologized to consumers, removed the provision, and promised to protect user privacy "in every possible way."[262]

The Zao case followed a common pattern. Firms have pushed the boundaries of data collection and retention, and citizens have on notable occasions resisted. In 2018, Alibaba met an "online uproar" after news spread that it had automatically enrolled many of its users, without consent, in Ant's Sesame Credit service—a private version of social credit that offered loans based on users' digital information.[263] Ant was forced to remove the offending setting and apologize for its "idiocy," acknowledging users' worries over the "safety of their own personal information and privacy."[264] That same year, the China Consumer Association, a state-affiliated social organization, found that 91 out of 100 apps it had investigated "collected data in excess of what they needed to provide their services."[265] More recently, a Chinese software firm removed, under pressure, a product that helped companies detect workers planning to quit.[266] This was reminiscent, some said, of the time video app Kuaishou installed digital timers above its toilets—a story that also incurred "widespread anger online."[267]

Social criticism has targeted not only corporate policies, but also statements from corporate leaders. In 2018, Baidu cofounder Robin Li stated that Chinese people were more willing than

---

[260] *Chinese Netizens Get Privacy-Conscious*, ECONOMIST (Sept. 7, 2019), https://perma.cc/K3MQ-AR3T [hereinafter *Privacy-Conscious*].

[261] *Id.*; Cyrus Lee, *"Deepfake" App Zao Sparks Major Privacy Concerns in China*, ZDNET (Sept. 5, 2019), https://perma.cc/BG9T-8NAM.

[262] *Privacy-Conscious*, *supra* note 260.

[263] Winston Ma, *China Is Waking Up to Data Protection and Privacy. Here's Why That Matters*, WORLD ECON. F. (Nov. 12, 2019), https://perma.cc/UD2P-S2D4; *Ant Apologizes over Credit Scoring Snafu*, PYMNTS (Jan. 8, 2018), https://perma.cc/Y8Z8-3NRE.

[264] Zhima Xinyong (芝麻信用) [Sesame Credit], WEIBO (Jan. 3, 2018), https://www.weibo.com/3732213162/FCHPE5UBk (sharing the Sesame Credit apology letter at issue).

[265] Liang, *supra* note 252. The state-established association handles complaints, tests products, develops consumer warnings, and engages in consumer education. *See About Us*, CHINA CONSUMERS ASS'N, https://perma.cc/5KDN-HF96.

[266] Greg James, *Chinese Tech Workers Outraged by Surveillance Tool That Flags Employees Who Look Likely to Quit*, CHINA PROJECT (Feb. 21, 2022), https://perma.cc/N6P8-9DTS.

[267] Tom Flanagan, *Company Under Fire for Installing Timers over Employees' Toilets*, YAHOO NEWS (Oct. 29, 2020), https://perma.cc/UZ5S-XTP4.

others to trade privacy for convenience or efficiency.[268] The "remark incited uproar amongst internet users."[269] A thread discussing Li's comments generated millions of views and thousands of critical replies.[270] One comment, with over ten thousand likes, describes a restaurant scene where a customer tries repeatedly to order beef, but is told time and again there is only caterpillar. Finally, the customer relents and orders caterpillar. "Chinese people are more willing to eat caterpillars," the commenter concludes sarcastically.[271] Elsewhere, a blogger responded that Chinese people are not more willing to give up their privacy; they are "forced" do so to participate in the digital economy.[272] "Still fresh in my memory is [e-commerce firm] JD's leak of five billion pieces of citizen information last year."[273]

Another way to understand datafication's impact is to study the rise of grassroots privacy advocates. There are hacking and blogging communities that pool encryption and surveillance evasion strategies online.[274] There are consumer rights crusaders, like Wu Dong, whose activism began after a hotel leaked his personal data in retaliation for exposing its hygiene problems.[275] There are commentators like Li Sihui, who has written extensively on data privacy on subjects like pandemic control.[276] And

---

[268] Ma, *supra* note 263.

[269] *Id.*

[270] ZHIHU (Mar. 26, 2018), https://perma.cc/R4GK-87NY (asking, "Ruhe Kandai Baidu Li Yanhong Biaoshi de "Zhongguoren Geng Kaifang, Yuanyong Yinsi Huan Xiaolü" ("如何看待百度李彦宏表示的 '中国人更开放，愿用隐私换效率'"?) ["What do you think of Baidu's Robin Li's statement that 'Chinese people are more open-minded and willing to trade privacy for efficiency?'"]).

[271] Heisenberg, ZHIHU (Mar. 26, 2018), https://www.zhihu.com/question/269959475/answer/350975117 (commenting on the discussion regarding Li).

[272] Management in Life, *Baidu Li Yanhong: Zhongguoren Geng Kaifang, Yuanyong Yinsi Huan Xiaolü? Cilei Yanlun Wuchi Zhiji!* (百度李彦宏：中国人更开放，愿用隐私换效率？此类言论无耻至极！) [*Baidu's Robin Li: Chinese People Are More Open-Minded and Willing to Trade Privacy for Efficiency? Such Shameless Comments!*], SINA (May 12, 2018), https://perma.cc/3FAZ-GDGF.

[273] *Id.*

[274] Emily Feng, *In China, a New Call to Protect Data Privacy*, NPR (Jan. 5, 2020), https://perma.cc/T3QX-5GB5.

[275] *Id.*

[276] *See* Li Sihui (李思辉), *Qineng Jie Fangyi Zhiming Suiyi Shouji Gongmin Xinxi* (岂能借防疫之名随意收集公民信息) [*How Can Citizens' Information Be Collected at Will in the Name of Pandemic Prevention?*], GUANGMING ONLINE (光明网) (Mar. 10, 2020), https://perma.cc/8D6P-JH5N.

there are artists like Deng Yufeng, who exhibited the personal data of 346,000 Wuhan citizens to raise privacy awareness.[277]

Of particular note are several law scholars who have sought to challenge FRT. In 2019, a law professor named Guo Bing sued a local safari park for requiring face-scanning for entry.[278] He alleged violations of contractual and consumer rights, and ultimately won a modest victory: compensation and an order requiring the removal of his biometric data.[279] The suit garnered significant domestic media attention.[280] Another law professor, Lao Dongyan of Tsinghua University, attained prominence after objecting to a plan to require FRT in her residential community.[281] Lao wrote a letter to her neighborhood committee, asserting that the policy contravened privacy laws and regulations.[282] The committee agreed to make face-scanning optional for entry.[283] Lao has also protested a plan to integrate FRT in Beijing's subway system.[284] "My real concern," she wrote, is not "misuse of my data by commercial organizations," but the risk that "my information is being abused by public authorities."[285]

Many of these data-related vulnerabilities intensified during the pandemic. Professor Shen Kui argued that the state's use of a "huge number of commercial and social actors to help control" the pandemic, many of them "uncontrolled and uncoordinated[,] . . . . put personal privacy in great jeopardy."[286] In the early days of the outbreak, the personal information of thousands of people returning to their hometowns from Wuhan was leaked, and began

---

277 Yin Yijun, *Police Shut "Privacy Art" Exhibit for Displaying Personal Data*, SIXTH TONE (Apr. 11, 2018), https://perma.cc/AJZ6-W8BU.

278 Yuan Ye, *A Professor, a Zoo, and the Future of Facial Recognition in China*, SIXTH TONE (Apr. 26, 2021), https://perma.cc/2EZ2-AWUF.

279 *Id.* The Court rejected other demands, such as the removal of all biometric data collected. Shen Lu, *Facial Recognition Is Running Amok in China. The People Are Pushing Back*, VICE (Dec. 10, 2020), https://perma.cc/YQ9R-MZAH.

280 *See* Ye, *supra* note 278.

281 Liu Yuxiu (刘昱秀) & Ren Wu (任雾), *Faxue Jiaoshou De Yici Weiquan: Renlian Shibie De Fengxian Chaochu Ni Suo Xiang* (法学教授的一次维权：人脸识别的风险超出你所想) [*A Law Professor Defends Her Rights for the First Time: The Risks of Facial Recognition Are Beyond Your Imagination*], PENGPAI NEWS (澎湃新闻) (Oct. 21, 2020), https://perma.cc/9LJ5-FRBW.

282 *Id.*

283 *Id.*

284 Lao Dongyan (劳东燕), *Renlian Shibie Jishu De Yinyou* (人脸识别技术的隐忧) [*The Hidden Dangers of Facial Recognition Technology*], READING THE CHINA DREAM (Jeffrey Ding trans., Oct. 31, 2019), https://perma.cc/ZLU5-Z644.

285 *Id.*

286 Shen Kui, *The Stumbling Balance Between Public Health and Privacy amid the Pandemic in China*, 9 CHINESE J. COMPAR. L. 25, 37, 40 (2021).

circulating on social media.[287] Some of these returnees were reportedly harassed by strangers over texts.[288] The leak was likely traceable to local governments that were responsible for registering residents returning from Wuhan.[289] As pandemic control policies fell into place, FRT became increasingly favored as a contactless means of identification. Along with temperature checks, it became a preferred form of regulating entry into residential neighborhoods.[290] Many affected residents went online to question the safety of their data in the hands of neighborhood committees—the least popular tier of Chinese governance.[291]

Perhaps the most intrusive tools of pandemic control have been mobile apps linked to citizen health records and location data.[292] Most were developed by localities in partnership with private firms.[293] They collected and assembled large quantities of personal data, including travel history, vaccine records, and polymerase chain reaction (PCR) test results. The "health codes" (*jiankangma*) were used to assign one of three color codes to each individual: green, yellow, and red, ordered by degree of exposure to COVID-19. A green code was required for travel or entry into malls, airports, and hospitals; a red code meant the person has tested positive and had maximally restricted movement.[294] While

---

[287] *Shuju Heishi Changjue, Yinsi Pin Zao Xielou, Ruhe Lifa Du Shang Geren Xinxi Loudong?* (数据黑市猖獗，隐私频遭泄露，如何立法堵上个人信息漏洞?) [*The Black Market for Data Is Rampant, and Leaks of Personal Information Happen Frequently; How Can We Legislate to Plug These Personal Information Leaks?*], CAIJING (May 29, 2020), https://perma.cc/2CKY-MD4U.

[288] *Id.*

[289] *Id.*

[290] Xinmei Shen, *Facial Recognition Data Leaks Are Rampant in China as Covid-19 Pushes Wider Use of the Technology*, S. CHINA MORNING POST (Oct. 8, 2020), https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes.

[291] *Id.* For more on the expansion of urban local governance during the pandemic, see Hualing Fu, *Pandemic Control in China's Gated Communities*, *in* HOW COVID-19 TOOK OVER THE WORLD: LESSONS FOR THE FUTURE 175–77 (Christine Loh ed., 2023); Yutian An & Taisu Zhang, *Pandemic State-Building: Chinese Administrative Expansion Since 2012*, YALE L. & POL'Y REV. (forthcoming 2024) (on file with author). Enforcers often "barged into people's homes or killed pets left behind by quarantined owners." Vivian Wang, *China's "Zero Covid" Bind: No Easy Way Out Despite the Cost*, N.Y. TIMES (Sept. 7, 2022), https://www.nytimes.com/2022/09/07/world/asia/china-covid-lockdown.html.

[292] Mia Zhong, *China's COVID Apps: A Primer*, DIGICHINA (July 14, 2022), https://perma.cc/YTK7-8VJK.

[293] *Id.*

[294] *Id.*

many concerns have been expressed over these health apps,[295] none were more vividly illustrated than when Zhengzhou officials assigned red health codes to 1,317 citizens to prevent them from traveling to the city to protest the freezing of their bank deposits.[296] In a similar episode, purchasers of incomplete residential buildings alleged that their health codes were turned red to prevent their entry into certain hearings.[297]

In sum, China's datafication era has been characterized by wide-ranging social grievances over data misuse. Some concerns have been programmatic and particularized. Others have been broad and diffuse. Privacy victims have included academics, bloggers, workers, migrants, parents, and students. Privacy abusers have ranged from individuals to firms to local governments. To be sure, China's citizens, like citizens everywhere, hold varying views on privacy. Yet a great many have availed themselves of the country's limited public forums to express disenchantment with intrusive data practices.

C. Privacy, Law, and Legitimation

China's privacy laws are best understood as a response to the grievances detailed in the preceding Section. The party-state has had to deploy a mix of policy responsiveness, lawmaking, and law enforcement to repair legitimation deficits stemming from data discontent. As in other areas like health and safety, it has sought to portray itself as a responsive guardian of public welfare against actors that threaten harm. A review of state and Party materials shows that these legitimation concerns have been of more central interest here than economics, geopolitics, and security.

Above all else, the party-state is concerned with its legitimacy, its people's belief that "it is right and proper . . . to accept and obey the authorities and to abide by the requirements of the regime."[298] While all governments are invested in their

---

[295] *See, e.g.*, Li Houchen (李厚辰), *Ni Zuohao Yizhi Shiyong "Jiankangma" De Zhunbei Le Ma?* (你做好一直使用"健康码"的准备了吗?) [*Are You Prepared to Use Your "Health Code" Forever?*], WEIXIN (Apr. 7, 2020), https://perma.cc/9RV3-EZA9.

[296] Phoebe Zhang, *China Officials Who Abused Health Codes to Stop Bank Protests Punished*, S. CHINA MORNING POST (June 23, 2022), https://www.scmp.com/news/china/politics/article/3182742/china-officials-who-abused-health-codes-stop-bank-protests.

[297] *Id.*

[298] David Easton, *A Re-Assessment of the Concept of Political Support*, 5 BRIT. J. POL. SCI. 435, 451 (1975); *see also* Susan H. Whiting, *Authoritarian "Rule of Law" and Regime Legitimacy*, 50 COMPAR. POL. STUD. 1907, 1912 (2017); BRUCE GILLEY, THE RIGHT TO RULE: HOW STATES WIN AND LOSE LEGITIMACY 5 (2009).

legitimation, autocracies have a special interest in "maintain[ing] the belief that the existing political institutions are the most appropriate ones for [ ] society."[299] Violence might sustain temporary rule, but the long-run costs of governing without public support are too high.[300] This is especially so today, where democratization movements are a constant reminder to autocrats of the existential threat posed by liberal values. China is no exception. "[L]ike all contemporary nondemocratic systems," observed political scientist Andrew Nathan, "the Chinese system suffers from . . . the fact that an alternative form of government is by common consent more legitimate."[301] "The acquisition of public support and popular legitimacy [is] inextricably tied to long-term political survival," noted scholars Taisu Zhang and Tom Ginsburg.[302] It is "arguably *the* fundamental interest . . . of the Party leadership."[303]

Absent electoral institutions, the most powerful source of popular legitimacy in democratic societies, autocrats have leaned on growth, ideology, tradition, nationalism, and other sources to legitimate their rule.[304] China's turn to privacy law can be understood as an effort to tap into two prominent and interlocking sources of its domestic legitimacy: (1) responsiveness and (2) law.

First, there is a substantial literature on the Chinese Communist Party's longevity, sometimes referred to as its "durability" or "resilience."[305] Within this literature, there is a family of explanations focusing on the party-state's responsiveness to citizen demands. Works on "consultative authoritarianism" emphasize the "input institutions" through which the party-state solicits

---

299 SEYMOUR LIPSET, POLITICAL MAN: THE SOCIAL BASES OF POLITICS 77 (1960).

300 Yuchao Zhu, *"Performance Legitimacy" and China's Political Adaptation Strategy*, 16 J. CHINESE POL. SCI. 123, 124 (2011); *see* Tamir Moustafa & Tom Ginsburg, *Introduction: The Functions of Courts in Authoritarian Politics*, *in* RULE BY LAW: THE POLITICS OF COURTS IN AUTHORITARIAN REGIMES 1, 5 (Tom Ginsburg & Tamir Moustafa eds., 2008) ("Legitimacy is important even for authoritarian regimes, if only to economize on the use of force that is also a component of maintaining power.").

301 Andrew J. Nathan, *China Since Tiananmen: Authoritarian Impermanence*, J. DEMOCRACY, July 2009, at 37, 37–38.

302 Taisu Zhang & Tom Ginsburg, *China's Turn Toward Law*, 59 VA. J. INT'L L. 306, 376 (2019).

303 *Id.* (emphasis in original).

304 *See* Andrew J. Nathan, *The Puzzle of Authoritarian Legitimacy*, J. DEMOCRACY, Jan. 2020, at 158, 160–61; Alex Wang, *Symbolic Legitimacy and Chinese Environmental Reform*, 48 ENVTL. L. 699, 706–07 (2018).

305 *See, e.g.*, Runya Qiaoan & Jessica C. Teets, *Responsive Authoritarianism in China—A Review of Responsiveness in Xi and Hu Administrations*, 25 J. CHINESE POL. SCI., 139, 142 (2020); Andrew J. Nathan, *China's Changing of the Guard: Authoritarian Resilience*, J. DEMOCRACY, Jan. 2003, at 6, 6 (coining the term "authoritarian resilience").

citizen preferences.[306] Works on "responsive authoritarianism" focus more on the "state reaction" to societal demands.[307] Both models stress the party-state's movement from command authoritarianism toward a more "quasidemocratic" approach to "engender regime legitimacy and possibly stem pressure for democratization."[308] The legitimacy at issue here is rooted less in nationalism or ideology and more in performance—the party-state's ability to deliver favorable outcomes to its citizens. Elements of Chinese tradition may make performance an especially powerful source of popular legitimacy today.[309]

Authoritarian responsiveness does not always manifest in law, however. Often, it can take the form of individualized provision of services or political campaigns. Why law here then? The answer likely relates to the cross-cutting nature of privacy grievances and the need to economize on a response through general legislation. Underlying these factors is the more basic notion that law is itself a source of legitimacy, and that responsiveness through law can compound their legitimation effects. This is especially so in China, where the "social demand for legality has

---

[306] *See, e.g.*, Rory Truex, *Consultative Authoritarianism and Its Limits*, 50 COMPAR. POL. STUD. 329, 330 (2017) (listing examples); Baogang He & Stig Thøgersen, *Giving the People a Voice? Experiments with Consultative Authoritarian Institutions in China*, 19 J. CONTEMP. CHINA 675, 675 (2010) (describing two experimental cases); Baogang He & Mark E. Warren, *Authoritarian Deliberation: The Deliberative Turn in Chinese Political Development*, 9 PERSPS. ON POL. 269, 276–79 (2011) (describing the emergence of deliberative politics in China); Jessica C. Teets, *Let Many Civil Societies Bloom: The Rise of Consultative Authoritarianism in China*, 2013 CHINA Q. 19, 32 (describing the rise of consultative authoritarianism).

[307] Qiaoan & Teets, *supra* note 305, at 141; *see also* Jidong Chen, Jennifer Pan & Yiqing Xu, *Sources of Authoritarian Responsiveness: A Field Experiment in China*, 60 AM. J. POL. SCI. 383, 383–84 (2016); Zheng Su & Tianguang Meng, *Selective Responsiveness: Online Public Demands and Government Responsiveness in Authoritarian China*, 59 SOC. SCI. RSCH. 52, 53–56 (2016); Yoel Kornreich, *Authoritarian Responsiveness: Online Consultation with "Issue Publics" in China*, 32 GOVERNANCE 547, 549 (2019); Lai Wei, Elaine Yao & Han Zhang, *Authoritarian Responsiveness and Political Attitudes During COVID-19: Evidence from Weibo and a Survey Experiment*, 55 CHINESE SOCIO. REV. 1, 23–24 (2023) (arguing that Weibo became an interface for communications between citizens and the government during the pandemic).

[308] Truex, *supra* note 306, at 333. These ideas are reflected in General Secretary Xi's alternative conception of democracy, "whole-process people's democracy," which includes, as a major component, a focus on "consultative democracy. Cheng Tongshun, *Whole-Process People's Democracy Is the Defining Feature of Socialist Democracy*, QIUSHI (May 5, 2023), https://perma.cc/E7DT-26GN (describing "extensive consultations" with the people via "proposals, conferences, symposiums, deliberations, hearings, evaluations, discussions, online activities, and public opinion surveys").

[309] Hongxing Yan & Dingxin Zhao, *Performance Legitimacy, State Autonomy and China's Economic Miracle*, 24 J. CONTEMP. CHINA 64, 68 (2015); Elizabeth J. Perry, *Chinese Conceptions of "Rights": From Mencius to Mao—and Now*, 6 PERSPS. ON POL. 37, 38 (2008) (same).

sharply increased in recent years to the point where it now exerts major influence over government popularity and support."[310]

Legal legitimation begins with lawmaking. As law scholar Alex Wang has argued, there are independent legitimation effects that flow from the very act of reform.[311] Through legislation, leaders "can signal to the public state concern about the environment, public health, and other desirable values."[312] China's national legislature has, for example, enacted a "comprehensive" set of environmental laws to project concerns about the environment.[313] It has also promulgated high labor standards, which "allow the central government to accrue popular legitimacy" through expressing care for ordinary workers.[314] In the early days of the pandemic, the national legislature proposed changes to over a dozen laws on public health and epidemic prevention, in large part to signal competence and foresight.[315] In these areas, the party-state has sought to win public support by situating itself as the masses' foremost protector against wide-ranging societal harms.

Further legitimation effects can flow from the actual and perceived enforcement of laws, once made. Law enforcement can foster legitimacy through a number of mechanisms, including the protection of procedural or substantive rights, the constraint (or at least regularization) of state power, and even the inherent value of legality itself.[316] It is not hard to see how laws that actually curb pollution, vindicate workers' rights, or reduce regulatory corruption in areas like food safety can foster state support. Yet *perceived* law enforcement can matter as much, if not more—especially in low-information environments where propaganda and censorship have increased monitoring costs. In the area of environmental law, Wang has shown how leaders have carried out "[p]eriodic enforcement actions" and campaigns to "symbolize top-down authority, strength, resolve, and concern for the

---

310 Zhang & Ginsburg, *supra* note 302, at 377 (summarizing recent literature); Whiting, *supra* note 298, at 1909 (finding empirical support).

311 Wang, *supra* note 304, at 717–18; *cf.* IZA YUE DING, THE PERFORMATIVE STATE: PUBLIC SCRUTINY AND ENVIRONMENTAL GOVERNANCE IN CHINA 7–8 (2022).

312 Wang, *supra* note 304, at 717.

313 *Id.*

314 MARY E. GALLAGHER, AUTHORITARIAN LEGALITY IN CHINA: LAW, WORKERS, AND THE STATE 33–34 (2017).

315 Changhao Wei, *Translation: NPCSC's New Public Health Legislative Plan in Response to COVID-19*, NPC OBSERVER (Apr. 29, 2020), https://perma.cc/Q5MK-P43K.

316 *See generally* Yiqin Fu, Yiqing Xu & Taisu Zhang, Does Legality Produce Political Legitimacy? An Experimental Approach (Nov. 23, 2021) (unpublished manuscript) (on file with author) (describing the legitimation benefits of legality).

people."[317] Campaigns can be short lived, even "ephemeral," but they can also create the impression of state concern and performance.[318]

China's turn to privacy law follows a similar pattern of responsiveness, lawmaking, and law enforcement. As in areas like health and safety, China's leaders have reacted to society-wide data discontent by framing privacy law as a shelter from abuse. In major addresses, General Secretary Xi has discussed personal information protection as a public safety imperative, alongside food and drug safety. The National People's Congress (NPC) has featured articles portraying privacy law as a "sword" to be wielded on behalf of the masses. Privacy scandals are consistently framed by state media as social ills that Chinese legal institutions can and should resolve. Courts, procuratorates, and police have all circulated model cases showcasing their work bringing data abusers to justice. And in both the letter and enforcement of China's privacy laws, one can discern special attention to especially combustible sources of privacy harm. All to say, responsive legalism has been central to the party-state's privacy turn.

1. State-endorsed reports.

First, a number of party- and state-endorsed documents on China's privacy laws stress, near exclusively, their social-protective mandate. Consider first General Secretary Xi's recent report to the Party's Twentieth National Congress, a major political work report that opened the Party's twice-a-decade Congress in 2022.[319] The report's sole mention of data privacy appears not in sections on industrial policy or trade, but in a subsection titled, "Enhancing public safety governance":

> Workplace safety risk controls will be strengthened, and safety supervision in key sectors and areas will be bolstered . . . . We will tighten supervision over food and drug safety

---

[317] Wang, *supra* note 304, at 718. For more on China's long history of campaign-style governance, see Zhang, *infra* note 410; Sebastian Heilmann & Elizabeth J. Perry, *Embracing Uncertainty: Guerilla Style and Adaptive Governance in China*, *in* MAO'S INVISIBLE HAND: THE POLITICAL FOUNDATIONS OF ADAPTIVE GOVERNANCE IN CHINA 3–4 (Sebastian Heilmann & Elizabeth J. Perry eds., 2011) (characterizing China's policymaking as "a process of ceaseless change, tension management, continual experimentation, and ad-hoc adjustment"); Susan Trevaskes, *Rationalising Stability Preservation Through Mao's Not So Invisible Hand*, 42 J. CURRENT CHINESE AFFS. 51, 54–61 (2013).

[318] Wang, *supra* note 304, at 718–19.

[319] Xi, *supra* note 199.

> and improve the systems of supervision, early warning, and prevention and control for biosafety and biosecurity. *Protection of personal information will be strengthened*.[320]

For context, these quinquennial work reports are always dissected, perhaps none more closely than the one here, delivered on the eve of another term in power.[321] Privacy's placement next to items like food and drug safety was likely no accident. Other sections addressing digital development, digital trade, and foreign policy make no reference to personal information protection.[322]

Articles on the PIPL featured on the national legislature's webpage reflect a similar understanding. The most extensive of these is a piece whose title, *Shining a Sword Through Legislation*, well captures the idea of the party-state as a watchful defender.[323] The article begins by situating the PIPL as a response to popular grievances: "Personal information protection has become one of the general population's most concerning, immediate, and practical" problems, it says, and the PIPL is an "important and necessary law of epochal significance" for addressing them.[324] The article goes on to catalog the PIPL's specific protections, stating twice that these provisions embody the law's "care for the people" (*dui ren de guanhuai*).[325] But such care is not extended to violators who have given in to "interest-based temptation," it continues.[326] They, the "responsible parties," must be "strictly" policed."[327]

The legislature's other PIPL materials accord with this narrative. On the eve of enactment, the NPC website featured a long article detailing the PIPL's path to promulgation.[328] It reviewed a number of major episodes, including Xu Yuyu's death and the likely leak of citizens' HIV-positive status across thirty provinces,

---

[320] *Id.* at 46–47 (emphasis added).

[321] *See* Bonny Lin, Brian Hart, Matthew P. Funaiole & Samantha Lu, *China's 20th Party Congress Report: Doubling Down in the Face of External Threats*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 19, 2022), https://perma.cc/5TZY-MRAF.

[322] Xi, *supra* note 199, at 24–25, 27.

[323] Li Tianqi (李天琪), *Lifa Liangjian, Zhongjie Xinxi "Luoben Shidai"* (立法亮剑，终结信息"裸奔时代") [*Shining a Sword Through Legislation: Ending Information's "Streaking Era"*], MINZHU YU FAZHI ZAZHI (民主与法制杂志) [DEMOCRACY & LEGAL SYS. MAG.] (Mar. 30, 2022), https://perma.cc/26D7-GNPK [hereinafter Li, *Shining a Sword*].

[324] *Id.*

[325] *Id.*

[326] *Id.*

[327] *Id.*

[328] Lu Yue (卢越), *Yichang Xinxi Baohu De Boyi* (一场信息保护的博弈) [*A Game of Personal Information Protection*], GONGREN RIBAO (工人日报) [WORKERS' DAILY] (Oct. 22, 2021), https://perma.cc/7PRQ-Y8AJ.

before detailing how the law would concretely address concerns over data fraud and misuse.[329] After the law was passed, Yang Heqing, a senior NPC official, offered a set of "hot button" interpretations of the PIPL—reproduced by *Xinhua* under the title *Placing the Word 'Strict' at the Head: Raising the Legalization Level of the Personal Information Protection Law*.[330] The explainer focuses on "how the law will protect the safety of your personal information and mine."[331] It describes individual consent as the law's "core rule," along with other processing limitations like minimum scope and reasonable purpose.[332] It stresses the law's heightened protections for sensitive data and its escalating penalties for privacy violators.[333] And it summarizes the law as a "strict system with strict standards and strict responsibilities."[334] A further elaboration of these points is separately featured on the national legislature's official webpage.[335]

Like General Secretary Xi's report to the Party Congress, these articles do not fit well into explanations that center growth, security, or geopolitics. Not one of these factors is mentioned in the latter three articles. The first piece does state, at the end, that the PIPL may also facilitate cross-border data flows and "healthy" digital development,[336] but these considerations are given no elaboration. Instead, they are merely referenced after the article's extensive discussion of the law's social protective role, accentuated by sword imagery and notions of law as care for the people. Factors like growth and trade are a part of this story, but they are not the heart of it.

---

329 *Id.*

330 Liu Shuo (刘硕) & Bai Yang (白阳), *"Yan" Zi Dangtou, Tisheng Geren Xinxi Baohu Fazhihua Shuiping* ("严" 字当头，提升个人信息保护法治化水平) [*Placing the Word "Strict" at the Head: Raising the Legalization Level of the Personal Information Protection Law*], XINHUA (Aug. 24, 2021), https://perma.cc/89NS-4EJ5.

331 *Id.*

332 *Id.*

333 *Id.*

334 *Id.*

335 Wang Qiao (王俏) , *Geren Xinxi Baohu Fa, Goujian Yi "Gaozhi-Tongyi" Wei Hexin De Chuli Guize* (个人信息保护法：构建以 "告知-同意" 为核心的处理规则) [*The Personal Information Protection Law: Constructing Processing Rules Centered on "Notice-Consent"*], RENMIN FAYUAN BAO (人民法院报) [PEOPLE'S CT. GAZ.] (Aug. 23, 2021), https://perma.cc/7DZX-X2NU.

336 Li, *Shining a Sword*, *supra* note 323.

2. State and Party media.

Another view of the party-state's responsive legalism can be seen from examining how state and Party media outlets have framed data scandals. These stories have followed a consistent pattern. First, they convey sympathy for the data intrusions suffered. Second, they identify the sources of these intrusions, and make clear that the state stands on the side of the people. And third, they redirect social discontent to legal channels by calling for stricter data laws or citing laws already enacted. The party-state is in such a way portrayed as an earnest protector—maybe a bit slow in the face of rapid digital change, but nonetheless well-meaning in supplying legal tools to combat digital threats.

The day after Robin Li commented on the Chinese people's purported willingness to trade away their privacy, China Central Television (CCTV) delivered a critical response.[337] CCTV is the country's leading state-controlled broadcaster; its rebuke was thus the closest thing to a state reply. After summarizing Li's statement, the commentary opens by describing a popular flashlight app that requires ten permissions to access data irrelevant to its function.[338] Apps like these are now common, the article continues, and with large losses from data theft, it is "not surprising that Li's comment gave rise to a backlash in public opinion."[339] "Have Chinese users really never cared about their privacy?" the article asks rhetorically.[340] The reality is that users "are forced to surrender their right to privacy" in order to participate in the digital world.[341] The article concludes, as virtually all such pieces do, with law. It states that recent proposals to improve privacy law have "given voice to the aspirations of many people" and called for establishing "rules that will strengthen privacy protection."[342]

A month later, *Xinhua*, the official state news agency, republished an article titled *We Need Better Privacy Protections*.[343] The

---

337 *Yangshi Pinglun: Shei Shuo "Zhongguo Ren Yuanyi Yong Yinsi Huan Bianli"?* (央视评论：谁说"中国人愿意用隐私换便利"？) [*CCTV Commentary: Who Says That "The Chinese Are Willing to Trade Privacy for Convenience?"*], JIEMIAN NEWS (界面新闻) (Mar. 27, 2018), https://perma.cc/S253-8NZ9 [hereinafter *Privacy for Convenience*].

338 *Id.*

339 *Id.*

340 *Id.*

341 *Id.*

342 *Privacy for Convenience*, *supra* note 337.

343 Fu Qing, (扶青), *Women Xuyao Genghao De Yinsi Baohu* (我们需要更好的隐私保护) [*We Need Better Privacy Protection*], NANFANG RIBAO (南方日报) [NANFANG DAILY] (Apr. 17, 2018), https://perma.cc/QWK6-M5KU.

article references several data privacy scandals, including the sale of personal information for five to ten RMB and Li's privacy-for-convenience comment, and makes clear that these episodes reflect a larger problem.[344] "Most users . . . yearn for a better privacy protection mechanism," it adds,[345] and "the most powerful means of protecting privacy is the law."[346] It concludes that a "personal information protection law focused on comprehensively protecting privacy is indispensable."[347]

Party media have framed enforcement events similarly. Consider commentary published by the *People's Daily*, the official newspaper of the Party's Central Committee, responding to the verdict in the safari park suit.[348] The author celebrates the outcome of China's "first facial recognition case," making clear that the party stands on the side of the people: the case "tells us *we* can bravely say 'no' to facial recognition."[349] The first half of the article conveys awareness that FRT "may lead to personal discrimination or injury," and makes clear its view that it is "obviously unnecessary" to require face-swiping for zoo entry.[350] The second half explains that although "our country's current laws have clear personal information protection requirements," firms and state organs continue to "intentionally or unintentionally infringe on citizens' personal information."[351] It expects that the Hangzhou case will play a "demonstration role" in future litigation, as "significant individual judgments [like this one] often become a foothold for rule of law to create just outcomes."[352]

Chinese state media have also sought to expose privacy violations, inviting responsive legalist reactions from state organs. In recent years, CCTV has devoted extensive coverage to data privacy violations in its "315 Evening Gala" program on World Consumer Rights Day.[353] In 2021, CCTV exposed twenty businesses

---

344 *Id.*

345 *Id.*

346 *Id.*

347 *Id.*

348 Mo Yichen (莫一尘), *"Renlian Shibie Diyi An" Zhongshen Panjue Yiyi Feifan* (人脸识别第一案" 终审判决意义非凡) [*The Final Judgment in the "First Facial Recognition Case" Is Extraordinarily Significant*], RENMIN WANG (人民网) [PEOPLE'S DAILY ONLINE], https://perma.cc/37K3-DKAP.

349 *Id.* (emphasis added).

350 *Id.*

351 *Id.*

352 *Id.*

353 Zhang Chaoyan, *Data Security Takes Center Stage at Consumer Rights Gala*, SIXTH TONE (Mar. 17, 2021), https://perma.cc/X538-L8GY.

for the unlawful use of FRT in their stores and inadequate supervision of personal information leaks on popular job-hunting sites. [354] Local governments immediately responded to the negative press. Shenzhen's Municipal People's Congress issued a directive calling on public interest litigation in areas like personal information protection, prompting a district procuratorate to form a special unit to investigate stores for violations. [355] The procuratorate boasted of how its work achieved "practical objectives for the masses," while using the investigation as an opportunity to publicize relevant provisions of the Consumer Protection Law.[356] Its response typifies China's privacy law enforcement in general: reactive, legalistic, and often campaign-driven.

3. Model cases.

Many of the institutions charged with enforcing China's privacy laws have sought to follow central signals on responsive legalism. This is perhaps clearest from case guidance issued by police, procuratorates, and courts in the form of "Model Cases on Personal Information Protection." In China, model cases serve a dual advertisement and guidance function, cataloging notable case achievements while standardizing conduct around key holdings and principles.[357] The model cases on personal information protection emphasize the same themes in central pronouncements and state media: the dangers of cyberspace, the state's position opposite digital bad actors, and law's role in safeguarding private rights. Of particular note is the praise accorded to procuratorate-led public interest suits; public prosecutors are depicted as marching at the vanguard of the state's personal information protection forces.[358]

---

354 *Id.*

355 Shenzhen Longhua Dist. Procuratorate, *"Wo Wei Qunzhong Ban Shishi" Renlian Shibie Shexiangtou? Jiancha Gongyi Susong Zhu Lao Gongmin Geren Xinxi Anquan Fanghu Qiang* (【我为群众办实事】人脸识别摄像头？检察公益诉讼筑牢公民个人信息安全防护墙) *["I Do Practical Things for the Masses." As to Facial Recognition Cameras? The Procuratorate's Public Interest Litigation Builds a Defensive Wall for Citizen Personal Information Security*], PENGPAI NEWS (澎湃新闻) (Apr. 22, 2021), https://perma.cc/4A5Y-JFBT.

356 *Id.*

357 *See* Susan Finder, *The 996 Typical Cases*, SUPREME PEOPLE'S CT. MONITOR (Aug. 29, 2021), https://perma.cc/96LA-EMDR; Jia, *Special Courts*, *supra* note 179, at 608–09.

358 A state news outlet recently reported that such filings rose from 147 in 2019 to 750 in 2020 to 2,276 in 2021 to 5,188 in just the first three quarters of 2022. Shi Shaodan (史绍丹) & Zhang Zixuan (张子璇), *2019 Nian Yilai Jiancha Jiguan Banli Geren Xinxi Baohu Lingyu Gongyi Susong Anjian 8361 Jian* (2019 年以来检察机关办理个人信息保护领域公益诉讼案件 8361 件) [*Since 2019, Procuratorial Organs Have Handled 8,361 Public*

Consider first three sets of "model cases on personal information protection" issued by courts in Guangdong, Zhejiang, and Hangzhou. Many of the case summaries begin by acknowledging threats to personal privacy, warning, for example, that "malicious and illegal disclosure of personal information is common."[359] Like other party-state documents, each set of cases also boasts of the state's protective record: the Guangdong High Court has "severely cracked down on crimes infringing citizens' personal information";[360] the Zhejiang High Court has been "serious" about "resolutely defending" citizens' personal privacy;[361] and the Hangzhou Internet Court's core mission has been to "center the people."[362]

The chosen cases naturally support these claims. All six of the Guangzhou cases and all four of the Zhejiang cases resulted in the successful vindication of the plaintiffs' assertions of privacy rights. In one case against a real estate brokerage that was collecting face information without consent, a local court in Zhejiang not only held that the defendant violated the PIPL, but also made a "judicial suggestion" (*sifa jianyi*) to a local market regulator to intervene.[363] The Haining Municipal Market Supervision Administration promptly issued an administrative fine against the company, before conducting a series of "surprise inspections on illegal collection of face information" by similar businesses.[364] As in other areas, Chinese courts seem to have assumed a more activist and collaborative role in disputes implicating social protection.[365]

Interest Litigation Cases in the Field of Personal Information Protection], JIANCHA RIBAO (检察日报) [PROCURATORATE DAILY] (Nov. 10, 2022), https://perma.cc/P8FC-NKBP.

359 *Geren Xinxi Baohu Shi Da Dianxing Anli* (个人信息保护十大典型案例) [*Ten Model Cases on Personal Information Protection*], HANGZHOU INTERNET CT. (Aug. 19, 2022), https://perma.cc/TK3L-K5M5 [hereinafter *Hangzhou Model Cases*].

360 *Guangdong Gaoyuan Fabu Geren Xinxi Baohu Dianxing Anli* (广东高院发布个人信息保护典型案例) [*Guangdong's High Court Publishes Model Cases on Personal Information Protection*], GUANGDONG HIGH PEOPLE'S CT. (Oct. 31, 2022), https://perma.cc/78G2-3748.

361 *Zhejiang Gaoyuan Fabu Geren Xinxi Baohu Dianxing Anli* (浙江高院发布个人信息保护典型案例) [*Zhejiang High People's Court Publishes Model Cases on Personal Information Protection*], ZHEJIANG HIGH PEOPLE'S CT. (Nov. 12, 2022), https://perma.cc/Q3BM-VU34 [hereinafter *Zhejiang Model Cases*].

362 *Hangzhou Model Cases*, *supra* note 359.

363 *Zhejiang Model Cases*, *supra* note 361.

364 *Id.*

365 *Cf.* Benjamin L. Liebman, *Ordinary Tort Litigation in China: Law Versus Practical Justice?*, 13 J. TORT L. 197, 208–16 (2020). *See generally* ETHAN MICHELSON, DECOUPLING: GENDER INJUSTICE IN CHINA'S DIVORCE COURTS (2022).

The ten model cases issued by the Hangzhou Internet Court are less one-dimensional.[366] They highlight not only data abusers being brought to justice, but also more technical developments in the law that clarify procedural questions or offer guidance on PIPL-compliant conduct.[367] Thus, in these cases, the plaintiffs' win rate is lower, at 50%. Nonetheless, the court's socially protective mission is made clear in four of the first five cases, all involving successful public interest suits brought by local procuratorates. The first case, for example, was brought by a procuratorate against someone who allegedly traded over forty thousand illegally collected pieces of personal data, "violating the personal information rights and interests of many unspecified subjects in society."[368] The court ordered public interest damages and a public apology.[369] The second case was brought against a short-video app that had allegedly violated the privacy interests of minors.[370] The court brokered a mediation agreement that included a compliance schedule, compensation to children's welfare groups, and an apology to appear "prominently" in a state-owned newspaper.[371]

The Supreme People's Procuratorate (SPP), the country's highest prosecutorial authority, has also issued model personal information protection cases. Like their judicial counterparts, SPP model cases generally highlight an array of kitchen-sink privacy abuses and the role of local procuracies in addressing them. The SPP's first batch of eleven model privacy cases consists entirely of public interest cases brought by various procuracies.[372] More than half are administrative public interest cases, where procuratorates, upon learning of personal information misuse, have made prelitigation suggestions urging state entities to

366 Certain specialized courts such as the Hangzhou Internet Court have aspired to a higher level of legal professionalization, albeit bounded by party controls. *See* Jia, *Special Courts*, *supra* note 179, 599–607.

367 *See Hangzhou Model Cases*, *supra* note 359.

368 *Id.*

369 *Id.*

370 *Id.*

371 *Id.*

372 *Zuigaojian Fabu Jiancha Jiguan Geren Xinxi Baohu Gongyi Susong Dianxing Anli* (最高检发布检察机关个人信息保护公益诉讼典型案例) [*The Supreme People's Procuratorate Releases Model Cases of Procuratorial Organs' Personal Information Protection Public Interest Litigation*], ZUIGAO RENMIN JIANCHAYUAN (最高人民检察院) (SUPREME PEOPLE'S PROCURATORATE) (Apr. 22, 2021), https://perma.cc/GR2U-C8AR [hereinafter *Procuratorial Model Cases*].

follow existing law.[373] The offending departments have invariably complied with these suggestions.[374]

Most of the cases in this category deal with an alleged failure to supervise. In one case from Zhejiang, the procuratorate "suggested" that a local market-supervision entity investigate two companies for illegally obtaining information on pregnant women from local hospitals.[375] In another case, a procuratorate in Jiangsu "suggested" that a municipal education bureau strengthen its supervision of off-campus tutoring companies after learning of a leak.[376] In other cases, however, procuratorates have alerted government organs not of their regulatory failures, but of their *own* mishandling of citizen data. In one Jiangxi case, a local procuratorate discovered that a county agricultural bureau had been disclosing information on machinery purchase subsidies online without de-identifying the personal information of over one thousand farmers, including their identification numbers, addresses, bank accounts, and phone numbers.[377] Through the court, the procuratorate issued a suggestion to the agricultural bureau requesting rectification. The bureau removed the offending materials.[378]

The SPP's second batch of model privacy cases consists of five criminal cases that similarly evidence privacy law's social-protective function.[379] The report notes that from 2019 to 2022, procuracies prosecuted over twenty-eight thousand people for violating citizens' personal information.[380] It then summarizes five prosecutions that "embodied its policy orientation of severely punishing crimes that infringe on citizens' personal information according to the law," covering credit, biometric, location, and health data.[381] The SPP made a special point to highlight a case where the Tianjin procuratorate worked closely with local police to investigate an elaborate theft-of-personal-data scheme

---

373 *Id.*

374 *Id.*

375 *Id.*

376 *Id.*

377 *Procuratorial Model Cases*, *supra* note 372.

378 *Id.*

379 *Zuigao Jian Fabu 5 Jian Yifa Chengzhi Qinfan Gongmin Geren Xinxi Fanzui Dianxing Anli* (最高检发布 5 件依法惩治侵犯公民个人信息犯罪典型案例) [*The Supreme People's Procuratorate Issues 5 Model Cases on Punishing Personal Information Infringement Crimes Against Citizens in Accordance with the Law*], ZUIGAO RENMIN JIANCHAYUAN (最高人民检察院) [SUPREME PEOPLE'S PROCURATORATE] (Dec. 7, 2022), https://perma.cc/3CKN-VLZ5.

380 *Id.*

381 *Id.*

involving a rural social pension app.[382] The Tianjin procuratorate ultimately prosecuted several dozen individuals.[383]

Local procuratorates have also heeded central signals by issuing model privacy cases. Three such cases issued by the procuratorate in Zhenjiang city cover familiar ground: the theft of citizens' personal information for profit, the misuse of facial recognition information by local sales offices, and a government organ's failure to remove identifying information from documents posted in the "Government Information Disclosure" column of its website.[384] The third case is an apparently common way in which state organs have been disciplined for privacy violations—not for intrusive surveillance, but for the inadvertent publication of personal details.

Not to be outdone, the Ministry of Public Security (MPS) has issued its own model cases on personal information protection.[385] Their case summaries focus on the police's role in cracking cases, showcasing the MPS's implementation of its political mandate. Like the preceding cases, the prosecuted crimes here have little to do with foreign threats or global influence. They involve more mundane crimes, such as the theft of personal data of the elderly to sell fraudulent healthcare products, the misuse of personal information to open online game accounts for sale to minors, and the theft of personal data in express companies' delivery slips.[386]

In comparison to "model cases," each selected and edited down by their issuers, a search of China's national judicial database for "Personal Information Protection Law" reveals an unrepresentative sample of PIPL cases.[387] A recent search yielded a total of 165 case entries. Of these: eighty-three were criminal, fifty were civil, three were enforcement-related, and one was

---

382 *Id.*

383 *Id.*

384 Zhang Chichuan (张驰川), *Zhenjiang Shi Jianchayuan Fabu 3 Qi Geren Xinxi Baohu Dianxing Anli* (镇江市检察院发布 3 起个人信息保护典型案例) [*The Zhenjiang Procuratorate Issues 3 Model Cases on Personal Information Protection*], ZHENJIANG RIBAO (镇江日报) [ZHENJIANG DAILY] (Sept. 15, 2022), https://perma.cc/5FH9-UJU8.

385 *Gongan Bu Gongbu 2021 Nian Qinfan Geren Xinxi Shida Dianxing Anli* (公安部公布 2021 年侵犯个人信息十大典型案例) [*The Ministry of Public Security Announces Ten Model Cases from 2021 on the Infringement of Personal Information*], CCTV NEWS (Jan. 8, 2022), https://perma.cc/WC6K-F3QT.

386 *Id.*

387 This search was conducted on August 9, 2023. For more on case disclosure and the national database, problems of "missingness," and recent difficulties, see generally Benjamin L. Liebman, Margaret Roberts, Rachel E. Stern & Alice Z. Wang, *Mass Digitization of Chinese Court Decisions: How to Use Text as Data in the Field of Chinese Law*, 8 J.L. & CTS. 177 (2020); Benjamin Liebman, Rachel Stern, Xiaohan Wu & Margaret Roberts, *Rolling Back Transparency in China's Courts*, 123 COLUM. L. REV. 2407 (2023).

administrative. Most case entries (120) came from the Basic People's Courts, the lowest tier of China's judiciary, with forty-two from Intermediate People's Courts and three from High People's Courts. A plurality of cases (thirty-eight) came from Beijing.

Many of these cases match the responsive legalist portrayals contained in the model cases.[388] In one public interest suit against four individuals involved in a data privacy scam, a local procuratorate in Sichuan successfully obtained an award of civil damages and a public apology.[389] The court in that case opined broadly on the purpose of China's data privacy laws: "Strengthening the protection of natural persons' personal information, intimately tied to personal interests, is an important part of the people's needs for a better life in this new era, and simultaneously touches on national interests and societal public interests."[390] In another case brought by a procuratorate in a special Xinjiang reclamation area, the defendant was sentenced to eight months in prison for selling mobile phone card data in violation of various laws, including the PIPL, and was ordered to pay a fine and compensation, and to issue an apology in province-level news media.[391] Likewise, in Henan Province, the Yongcheng City Procuratorate prosecuted an individual for violating inter alia the PIPL for trading in others' WeChat information; the defendant was sentenced to over four years of prison and ordered to pay a fine and compensation.[392]

Importantly, other PIPL cases in the database show courts dismissing plaintiffs' privacy claims when pressed against competing state interests. In one case, a Shandong court rejected a plaintiff's request for a pharmacy to delete her personal information because the pharmacy was not authorized to do so under

---

[388] Several of the cases discussed were found on a separate search conducted in the fall of 2022.

[389] *See generally* Sichuan Sheng Zigong Shi Renmin Jianchayuan, Li Bolun Deng Geren Xinxi Baohu Jiufen Minshi Yishen Minshi Panjueshu (四川省自贡市人民检察院、李博伦等个人信息保护纠纷民事一审民事判决书) [First Instance Civil Judgment in a Personal Information Protection Dispute Between the People's Procuratorate of Zigong City, Sichuan Province, and Li Bolun et al.] (Sichuan Province Zigong City Interm. People's Ct., Aug. 11, 2022) (available at https://perma.cc/RE6A-S7FC).

[390] *See generally id.*

[391] *See generally* Qin Fan Gong Min Ge Ren Xin Xi Zui Yi Shen (侵犯公民个人信息罪一审刑事) [Criminal with Subsidiary Civil Judgment for Infringement of Personal Information] (Xinjiang Prod. and Constr. Corps Fangcao Lake Reclamation Dist. People's Ct., June 6, 2023) (available at https://perma.cc/5XDG-7VTM).

[392] *See generally* Xingshi Fudai Minshi Panjueshu (刑事附带民事判决书) [Criminal with Subsidiary Civil Judgment] (Henan Province Yongcheng City People's Ct., Oct. 31, 2022) (on file with author).

local public health regulations devised for pandemic control.[393] In another case, a court in Beijing sided with a local residents' committee in a suit brought by an individual who claimed personal information infringement.[394] In denying the individual's application for a retrial, the Beijing High People's Court reasoned that the Civil Code does not confer liability on those who "process personal information for the purpose of safeguarding the public interest."[395] Such cases are not often showcased in "model case" compilations, but they are a crucial feature of a privacy regime where core state interests invariably override the assertion of individual rights.

In sum, the lodestar privacy cases chosen by China's own law enforcement organs also support the popular legitimation thesis. These cases portray China's privacy laws most centrally as a tool for policing and deterring everyday abuse and misuse of personal information. Most defendants are cast as intentional wrongdoers, while local government organs come off as more careless. But in most all of these cases, privacy law is framed as the party-state's weapon for protecting citizens from harm.

4. Laws and their enforcement.

The party-state has also drafted and enforced many of its privacy laws to respond to societal grievances. Consider first the laws and regulations as written. In 2021, the Supreme People's Court (SPC) issued sixteen provisions clarifying the law in civil cases involving facial recognition.[396] One such provision called on courts to "support" residents who request alternative methods of identification if their building managers mandated FRT for

---

393 *See generally* Jiang Mou, Binzhou Shenqi Dayaofang Youxian Gongsi Bincheng Taishan Mingjundian Geren Xinxi Baohu Jiufen Minshi Yishen Minshi Panjueshu (江某、滨州神奇大药房有限公司滨城泰山名郡店个人信息保护纠纷民事一审民事判决书) [First Instance Civil Judgment in a Personal Information Protection Dispute Between Jiang Mou and Binzhou Miracle Pharmacy Co.] (Shandong Province Bincheng Dist. People's Ct., Sept. 8, 2022) (on file with author).

394 Minshi Caidingshu (民事裁定书) [Civil Judgment] (Beijing High People's Ct., Apr. 27, 2023) (on file with author).

395 *See generally id.* The plaintiff had made a PIPL claim as well, but the Court held that the law did not apply retroactively. *See generally id.*

396 *See generally* Zuigao Renmin Fayuan Guanyu Shenli Shiyong Renlian Shibie Jishu Chuli Geren Xinxi Xiangguan Minshi Anjian Shiyong Falü Ruogan Wentide Guiding (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定）[*Provisions on Several Issues on the Application of Law in Hearing Civil Cases Related to the Use of Facial Recognition Technology to Handle Personal Information*] (promulgated by Supreme People's Court, July 28, 2021, effective Aug. 1, 2021), SUP. PEOPLE'S CT. GAZ., July 28, 2021 (English translation available at https://perma.cc/9EEJ-DNPX).

access.[397] This was a direct response to housing-related FRT controversies during the pandemic. Similarly, the PIPL's ban on automated price discrimination was a reaction to popular frustrations.[398] One study of rideshare apps found that users with expensive smartphones were more likely to be matched with expensive rides.[399] According to an article on the national legislature's webpage, "[c]onclusions like this have resonated with many netizens," who "have shared their own experiences of being 'killed' on shopping, travel, and other platforms."[400]

The responsive tailoring of China's privacy laws comes into sharper relief in the enforcement setting. Many of the data scandals detailed earlier were met with highly legalistic responses. After Xu Yuyu's scammers were convicted, the SPP published an article detailing how procurators cracked the case with the aid of legal tools made available in specific response to Xu's death.[401] It describes how the SPP partnered with the SPC to issue new guidance on handling criminal violations of citizens' personal information, and how the two organs joined forces with the MPS to issue an opinion clarifying the law on telecommunications crimes.[402] One procurator said that "the release of the above two judicial interpretation documents played a decisive role" in the Xu Yuyu case.[403] Ant Financial's automatic enrollment of its users into its private social credit scheme likewise met a legalistic response. In January 2018, the CAC rebuked Ant for violating the country's data protection standards, demanding that it alter the system and take steps to prevent future violations.[404] A similar fate befell Zao, the controversial face-swap app. In 2019, MIIT officials met with agents of Zao's affiliate and ordered self-inspection and rectification.[405] Over the course of the following

---

397 *Id.* art. 10.

398 Lu, *supra* note 328.

399 *Id.*

400 *Id.*

401 Xu Ridan (徐日丹), *Gongsuren Xiangjie Xu Yuyu Bei Dianxin Zhapian Zhisi An Banan Licheng* (公诉人详解徐玉玉被电信诈骗致死案办案历程) [*Public Prosecutors Explain in Depth the Case Handling Process in Xu Yuyu's Death by Telecommunications Fraud*], SUPREME PEOPLE'S PROCURATORATE (June 27, 2017), https://perma.cc/HHA9-RFLA.

402 *Id.*

403 *Id.*

404 Josh Chin & Chuin-Wei Yap, *China Swats Jack Ma's Ant over Customer Privacy*, WALL ST. J. (Jan. 10, 2018), https://www.wsj.com/articles/china-swats-jack-mas-ant-over-customer-privacy-1515581339.

405 Bai Jinlei (白金蕾) & Luo Yidan (罗亦丹), *Gongxinbu Yuetan Yaoqiu Zhenggai Zao Yonghu Xieyi Yi Xiugai* (工信部约谈要求整改 ZAO 用户协议已修改) [*Ministry of Industry and Information Technology Interviewed and Asked for Rectification; ZAO User Agreement*

year, and not only in response to Zao, MIIT claims to have tested over eighty thousand apps and ordered eight thousand of them to adopt "rectification measures" for personal information violations.[406]

Enforcement efforts first began tightening in 2013 after the SPP, SPC, and MPS issued a joint notification calling for more vigorous enforcement against personal information crimes.[407] The notification explained that "a flood of illegal trading of citizens' personal data" was causing great social harm and strong mass reactions, and that heightened efforts were needed to "safeguard social harmony and stability."[408] Back then, personal information crimes were considered "new."[409] Later, as popular grievances intensified and more protective regulations emerged, enforcement campaigns became more frequent. Campaigns are a common supplement to regular enforcement in China; in areas like environmental protection and food safety, they are often used to signal high-level attention to particular problems, to break bureaucratic logjams, to popularize new laws and regulations, and to enhance deterrence.[410] So too with recent privacy campaigns. In 2019, the MPS conducted a nationwide "Clean Network 2019" campaign that cracked down on a number of online crimes, including "infringement of citizens' personal information."[411] MPS

Has Been Revised], XINJING BAO (新京报) [BEIJING NEWS] (Sept. 5, 2019), https://perma.cc/8YFY-KL64.

406 Iris Deng & Coco Feng, *Beijing Internet Court Rules Against Tencent, ByteDance in User Data Infringement Cases*, S. CHINA MORNING POST (Aug. 3, 2020), https://www.scmp.com/tech/apps-social/article/3095790/beijing-internet-court-rules-against-tencent-bytedance-user-data.

407 *Notice Concerning Punishing Criminal Activities Infringing Citizens' Personal Data*, CHINA COPYRIGHT & MEDIA (Rogier Creemers trans., Apr. 23, 2013), https://perma.cc/8GLX-RMTD.

408 *Id.*

409 *Id.*

410 *See* William P. Alford & Benjamin L. Liebman, *Clean Air, Clean Processes? The Struggle over Air Pollution Law in the People's Republic of China*, 52 HASTINGS L.J. 703, 748 (2001); Benjamin van Rooij, *Implementation of Chinese Environmental Law: Regular Enforcement and Political Campaigns*, 37 DEV. & CHANGE 57, 65–71 (2006); Yuanyuan Shen, *The Development of and Challenges Facing Food Safety Law in the People's Republic of China*, *in* IMPROVING IMPORT FOOD SAFETY 151, 161 (Wayne Ellefson et al. eds., 2013); Angela Zhang, *In China, Behave or Face a Campaign*, BLOOMBERG (Jan. 6, 2021), https://www.bloomberg.com/opinion/articles/2021-01-06/china-s-regulators-turn-to-communist-style-campaigns-to-keep-things-in-line.

411 *Gonganbu Tongbao "Jing Wang 2019" Zhuanxiang Xingdong Dianxing Anli* (公安部通报"净网 2019"专项行动典型案例) [*Ministry of Public Safety Issues Model Cases for Its "Clean Internet 2019" Special Campaign*], CYBERSPACE ADMIN. OF CHINA (Nov. 14, 2019), https://perma.cc/5VZ7-Z2N5.

reports that police arrested 7,647 criminal suspects across 2,868 cases of personal information infringement.[412] Listed successes included apprehension of criminal gangs selling personal data on the dark web and voyeurs using pinhole cameras to "spy on others' privacy."[413] An "App Governance Working Group" established in 2019 by several central government organs "has conducted a continuous campaign against apps, identifying and either castigating or punishing dozens of companies."[414]

China's authorities have been especially concerned about privacy harms growing out of their pandemic policies. In 2020, the CAC issued a notice urging that "all localities and all departments must pay high regard" to personal information protection laws while carrying out epidemic-control work:

> Except for [authorized bodies], no other work units or individuals may use epidemic prevention and control . . . as a reason to collect or use personal information without the agreement of the person whose data is collected . . . . The collection of personal information required for [pandemic control] shall occur with reference to the . . . "Personal Information Security Specification," [and] uphold the principle of minimal scope . . . . [A]ctual discrimination against groups in particular locations must be prevented . . . Personal information collected for epidemic control and disease prevention and treatment may not be used for other purposes.[415]

From these directives, one can sense the undercurrents of data discontent that underlie the CAC's order. It was not long before local governments fell in line. A month later, for example, the city of Tianjin's party cyberspace commission announced a "special campaign" on the "illegal collection and use of personal information relating to epidemic prevention and control."[416] The campaign targeted pandemic-control smartphone apps, calling for

---

412 *Id.*

413 *Id.*

414 Creemers, *supra* note 20, at 6.

415 *Translation: Chinese Authorities Emphasize Data Privacy and Big Data Analysis in Coronavirus Response*, DIGICHINA (Rui Zhong et al. trans., Feb. 11, 2020), https://perma.cc/FX2Z-GJ5C.

416 *Tianjin Shiwei Wangxinban Kaizhan Yiqing Fangkong Xiangguan App Weifa Weigui Shouji Shiyong Geren Xinxi Zhuanxiang Zhili Gongzuo* (天津市委网信办开展疫情防控相关 App 违法违规收集使用个人信息专项治理工作) [*The Tianjin Cyberspace Administration Launches Special Campaign to Address the Illegal Collection and Use of Personal Information by Apps Related to Pandemic Prevention and Control*], CYBERSPACE ADMIN. OF CHINA (Mar. 13, 2020), https://perma.cc/663U-MBR9.

both administrative and criminal sanctions.[417] From the party-state's perspective, privacy violations are especially concerning where, as in the epidemic context, its own policies require citizen collaboration of a sort that would be discouraged in an environment where privacy infractions are routine.

In her new book, Angela Zhang has documented an intensification of data enforcement since 2021.[418] She has recounted a number of new data measures, including a 2021 interagency notice focused on regulating mobile apps that collect excessive personal data and violate laws against uninformed consent.[419] She also showed a fourfold increase in MIIT's targeting of non-compliant apps from 2020 to 2021.[420] Zhang argued that this sharp uptick in enforcement is rooted in distinctive aspects of Chinese governance that make it especially prone to sudden regulatory swings.[421] As to social forces underlying data regulation, Zhang noted that there is "significant demand . . . to enhance the protection of personal information."[422]

5. Reassessing recent developments.

A more popularly-rooted conception of privacy law in China helps us see several privacy-related developments in new perspective. First, the legitimation root of Chinese privacy law sheds light on why legislative authorities have recently invoked privacy language from China's Constitution in its review of problematic provincial laws. Although China is no closer today in establishing judicial review of its Constitution,[423] authorities have recently enhanced the stature of a centralized oversight mechanism called Recording and Review, through which the NPCSC's Legislative Affairs Commission (LAC) checks sub-statutory regulations for conformity with national laws, party policies, and the Constitution.[424] The LAC has proceeded cautiously in exercising its

---

417 *Id.*

418 *See generally* ZHANG, HIGH WIRE, *supra* note 42.

419 *Id.* (manuscript at 174–75).

420 *Id* (manuscript at 174).

421 *See id.* (manuscript pt. I).

422 *Id.* (manuscript at 144).

423 Thomas E. Kellogg, *Constitutionalism with Chinese Characteristics? Constitutional Development and Civil Litigation in China*, 7 INT'L J. CONST. L. 215, 246 n.89 (2009).

424 Changhao Wei, *Reining In Rogue Legislation*, MADE IN CHINA (Sept. 19, 2021), https://perma.cc/8V7A-NUF5 [hereinafter Wei, *Rogue Legislation*]. It has also enhanced the role of a new Constitution and Law Committee within the NPC. *See* Keith J. Hand, *Constitutional Supervision in China After the 2018 Amendment of the Constitution:*

constitutional review powers, well aware of its relative weakness institutionally and of the sensitivity of wading into constitutional matters in general.[425]

In 2019, a domestic paper reported that the LAC had investigated road safety regulations in Gansu and Inner Mongolia that authorized traffic police to search motorists' cell phone communication records following an accident.[426] The regulations sought to combat distracted driving, a major cause of traffic accidents, by giving police a tool for identifying motorist phone use before an accident.[427] But the LAC concluded that the regulations lacked a "legal basis" because they contravened "citizens' freedom and privacy of correspondence"—a phrase found in China's Constitution.[428] Article 40 of China's Constitution forbids organizations and individuals from infringing upon this right except in certain enumerated cases such as state security and investigation of criminal offenses.[429] As legal scholar Changhao Wei explains, the provincial phone search provisions, which mostly apply to routine traffic disputes, do not meet these exceptions and would thus appear plainly to contravene Article 40.[430] The LAC's 2019 work report suggested much the same, stating that the provincial regulations "comport[ ] neither with the principle nor the spirit of freedom of privacy and correspondence."[431] Both provincial and province-level legislatures have since removed their phone search regulations upon the LAC's urging.[432] Although the LAC did not explicitly mention the Constitution, Wei has suggested that the decision "may well be the result of the Commission's first-ever *constitutional* review."[433]

The LAC's decision is not easily explained by top-down conceptions of Chinese privacy law. The phone searches at issue here

---

Refining the Narrative of Constitutional Supremacy in a Socialist Legal System, ASIAN-PAC. L. & POL'Y J., May 17, 2022, at 137, 148–55.

425 Wei, *supra* note 424.

426 Liu Man (刘嫚), *Jiaojing Ke Cha Tonghua Jilu? Jiu Zheng!* (交警可查通话记录？纠正！) [*Can Traffic Police Check Call Records? Correct the Error!*], S. METROPOLIS (Mar. 2, 2019), https://perma.cc/RR65-9M7U [hereinafter Liu, *Traffic Police*].

427 Wei, *Rogue Legislation*, *supra* note 424.

428 Liu, *Traffic Police*, *supra* note 426.

429 XIANFA art. 40.

430 Wei, *Privacy of Correspondence*, *supra* note 14 (analyzing LAC's general comments to this provision).

431 NPCSC LEGISLATIVE AFFAIRS' COMMISSION'S 2019 REPORT ON ITS RECORDING AND REVIEW WORK 241 [hereinafter LAC 2019 REPORT].

432 *Id.*

433 Wei, *Privacy of Correspondence*, *supra* note 14 (emphasis in original).

have only the most tenuous connections with digital economic growth, and have virtually nothing to do with China's geopolitical goals or national security fears. They are, however, deeply unpopular with segments of the population who drive. China's netizens have been highly critical of overbearing city and traffic police; the outlet that wrote the LAC story noted that "many car owners have experienced" similar phone searches and have "gone online to express questions and doubts" about their necessity.[434] Like judges, procuratorates, and regulators, LAC staffers heeded central signals to respond to data discontent through responsive legalism. Practically speaking, enforcement of the LAC's review decisions is not always automatic.[435] But by leveraging center-endorsed privacy themes, LAC staffers were able to bolster their case for abolition.[436] Their work here is especially notable because they appear to have relied on constitutional privacy language to reign in provincial authorities. These developments illustrate not so much the legal importance of the Chinese Constitution as they do the political importance of privacy protection in China today.

Bottom-up concepts of Chinese privacy law also add nuance to our understanding of China's recent technology crackdown. Starting in October 2020, Chinese regulatory authorities pursued a series of enforcement campaigns against its technology sector, beginning with Ant Financial, but growing to cover an array of sectors: e-commerce, education, ride hailing, social media, gaming, insurance, and even e-cigarettes.[437] Popular media and policy narratives have tended to attribute these events to Party concerns over control and security.[438] Where privacy violations were used to justify new restrictions, the tendency has been to treat privacy concerns as a sham.[439]

A more popularly-rooted conception of Chinese privacy law suggests that, while leaders were surely tapping into privacy law's legitimation effects to further other goals, their privacy

---

434 Liu, *Traffic Police*, *supra* note 426.

435 Wei, *Rogue Legislation*, *supra* note 424.

436 *See id.* (describing how the LAC has closely followed the Party's major policies).

437 *China's Big Tech Crackdown: A Complete Timeline*, CHINA PROJECT, https://perma.cc/GMC2-JBRE.

438 *See, e.g.*, Lingling Wei, *China's Xi Ramps Up Control of Private Sector. "We Have No Choice but to Follow the Party,"* WALL ST. J. (Dec. 10, 2020), https://www.wsj.com/articles/china-xi-clampdown-private-sector-communist-party-11607612531; Zhang, High Wire, *supra* note 42, at 4 n.15 (collecting sources).

439 Sutter, *supra* note 160, at 26 (portraying China's technology regulations as efforts to "enhance state control in the name of privacy").

concerns were not entirely pretextual either. Consider the Didi investigation, which culminated in a $1.2 billion fine against the ride hailing company for retroactive violations of the PIPL and several data security laws.[440] Commentators were puzzled as to how the CAC's yearlong investigation, "staged as a cybersecurity case," culminated in a decision that focused largely on privacy violations.[441] It is hard to know for sure, but one point that is often missed is that Didi's alleged personal data violations were actually quite significant. In an interview, a CAC representative painstakingly recounted Didi's various privacy-related infractions, including "illegal collection of 11.9639 million screenshots in users' mobile photo albums," "107 million pieces of passenger face recognition information," and "1.3829 million pieces of family relationship information."[442] The careful numerical delineation of each category of infraction connects the CAC's work with relatable data privacy concerns, conveying the magnitude of Didi's breach of public trust with their data. CAC regulators were likely alarmed by Didi's privacy violations, and found this to be a much more attractive and convenient public basis for sanctioning Didi than other less savory bases, given how easily they could default to habituated frames based in responsive legalism. That the PIPL could not technically be applied retroactively was apparently no barrier, showing how the party-state's legalistic approach to privacy law is not the same as an entirely legal one.[443] Privacy concerns were an overstated basis for punishment relative to other motivations, but they were not pure window-dressing either.[444]

---

[440] *Guojia Hulianwang Xinxi Bangongshi Youguan Fuze Ren Jiu Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa De Jueding Da Jizhe Wen* (国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问) [*The Lead Investigator at the CAC Answers Reporters' Questions on the Agency's Investigation into Didi Global and Its Decision to Impose Administrative Penalties*], CYBERSPACE ADMIN. OF CHINA (July 21, 2022), https://perma.cc/RW5W-A36G [hereinafter *CAC Answers*].

[441] Mingli Shi, James P. Horsley & Xiaomeng Lu, *Forum: Unpacking the Didi Decision*, DIGICHINA (July 22, 2022), https://perma.cc/6PGH-74GV ("How the decision was reached, particularly the transition from cybersecurity to privacy, was not explained.").

[442] *CAC Answers*, *supra* note 440.

[443] *See* Angela Huyue Zhang, *The Didi Case and the Party's Influence over Data Enforcement*, U.S.-ASIA L. INST. (Sept. 20, 2022), https://perma.cc/CTR4-GLRQ.

[444] For an account of the range of motivations underlying these events, see generally Rogier Creemers, The Great Rectification: A New Paradigm for China's Online Platform Economy (Jan. 9, 2023) (unpublished manuscript) (on file with author).

6. Reframing the state.

Beyond enhancing perceptions of state performance, responsive legalism can also distract from or soften criticism of the party-state's own role in fueling China's surveillance society. The party-state has contributed to surveillance in two ways. First, it has overseen rapid and unregulated datafication. Second, it is itself a major surveiller. Privacy law helps the party-state in both of these areas.

First, privacy law can help distract from the party-state's role in superintending the country's whiplashed transition into the digital age. By depicting itself as a watchful guardian of individual privacy rights, the party-state reframes itself from something of a negligent overseer of, or perhaps even an active cheerleader for, unregulated datafication, into a champion of citizens' privacy rights. This mirrors a long-standing approach in other areas of Chinese governance. For example, framing the state as a supplier of environmental protection encourages citizens to forget the state's own role in fueling pollution.[445] Likewise, portraying the state as a guardian of public health may cause citizens to overlook state failures in preparing for or preventing mass outbreaks.[446] It helps of course that many have benefitted from datafication. Popular grievances are directed not at datafication per se, but at how that process has been steered.[447] Privacy law is a means of conveying that caring and competent leaders are at the helm.

Second, privacy law may also help soften perceptions of the party-state's own surveillance practices. While there is some evidence that Chinese citizens may already be more accepting of state surveillance than others,[448] China's leaders do not have free

---

445 *See* Alex Wang, *The Role of Law in Environmental Protection in China: Recent Developments*, 8 VT. J. ENVTL. L. 195, 199–200 (2007) (describing the environmental costs of economic growth targets in China).

446 *See* Steven Lee Myers & Chris Buckley, *China Created a Fail-Safe System to Track Contagions. It Failed.*, N.Y. TIMES (last updated Dec. 22, 2020), https://www.nytimes.com/2020/03/29/world/asia/coronavirus-china.html. *But see* Wallace, *infra* note 449 (describing the sudden abandonment of China's "zero COVID" program).

447 *See* Tristan G. Brown, Alexander Statman & Celine Sui, *Public Debate on Facial Recognition Technologies in China*, MIT CASE STUD. IN SOC. & ETHICAL RESPS. OF COMPUTING (Aug. 10, 2021), https://perma.cc/85HE-EYK3 (arguing that despite public criticism of FRT, there is still "broad-based public support for uses that promise increased security or convenience").

448 The comparative survey discussed in Part III.B found that 52% of surveyed Chinese citizens generally support government surveillance, compared to 40% in Germany, 47% in the United Kingdom, and 38% in the United States. It also found that

license to control as they please. Recall that recent protests over pandemic lockdown policies, which led to an abrupt and sudden reversal in national policy, targeted not only local enforcement but also central leaders.[449] Privacy law can aid regime policies by creating and then helping to resolve cognitive dissonance regarding the state's privacy role. China's privacy laws portray its leadership as privacy protectors, but its state surveillance practices—including ubiquitous surveillance cameras—suggest the opposite. The more that the party-state floods the public sphere with evidence of its protective role, the more likely citizens are to eventually resolve the dissonance in favor of the state, reducing the cognitive burden associated with contradiction.[450] While this may not blind citizens from the most intrusive forms of surveillance, it does make them more likely to regard these intrusions sympathetically. They may see state surveillance, even in its harshest forms, as another manifestation of the party-state's protective policies. In such a setting, privacy law may grow to become not a check against, but an enabler for, China's surveillance state.

IV. CONCEPTUAL IMPLICATIONS

Part IV turns to this Article's contributions to areas of study outside Chinese privacy law. Section A explains how China's turn to privacy law fits into existing theories on China's legal system. Section B traces the contours of a general theory of authoritarian privacy. Section C explains how authoritarian privacy might complicate approaches to privacy theory here. China's turn to privacy law is both a distinctive case of autocratic politics and part of a universal story of technological change. Its theoretical implications are confirmatory in some ways but provocative in others.

Chinese citizens had the highest amount of trust in central government FRT use, at 60%, compared to 35% in the United States. Kostka et al., *supra* note 238, at 681.

449 *See* Jeremy Wallace, *Why Protestors Are Targeting Xi Jinping for China's "Zero Covid" Failures*, WASH. POST (Nov. 30, 2022), https://www.washingtonpost.com/politics/2022/11/30/china-protest-zero-covid-xi-jinping/.

450 Cognitive dissonance refers to a phenomenon where people concurrently hold "inconsistent cognitions," defined as "an unpleasant, drive-like state which motivates people to alter their cognitions to reduce their experience of dissonance." Simon Draycott & Alan Dabbs, *Cognitive Dissonance 1: An Overview of the Literature and Its Integration into Theory and Practice in Clinical Psychology*, 37 BRIT. J. CLINICAL PSYCH. 341, 342 (1998).

A. Concepts of Chinese Law

First, this Article contributes in several ways to our understanding of Chinese law. China's privacy laws are not an island outside of the legal system; they are an organic part of the country's growing legal superstructure. As a result, they reflect a number of attributes distinctive to Chinese law today. For example, administrative enforcement of China's privacy has often been campaign-like, following closely signals from above. Judicial enforcement of privacy laws can be activist and collaborative, as in other areas with a strong social protection mandate. Grassroots actors have leveraged privacy laws to pursue their own policy agendas, as is common in other areas of Chinese law. And the center has employed privacy law as a tool to reign in local misuse of citizen data, consistent with its other efforts to reduce agency costs associated with vertically fragmented governance.[451]

By emphasizing more populist roots of Chinese lawmaking, this Article has taken a bottom-up approach to modeling China's legal system.[452] This contrasts with a growing view in Chinese governance studies generally, which has taken policy centralization under General Secretary Xi to mean a drastic reduction in grassroots policy influence.[453] Scholars Runya Qiaoan and Jessica Teets have described a growing consensus that General Secretary Xi's "new governance style prioritizes 'top-level design'" at the expense of government responsiveness, especially in the localities.[454] China's privacy example suggests that whatever has changed in local governance, the central government can still be highly responsive at key junctures.[455] Especially as the economy has slowed, China's leaders have been increasingly focused on tapping into other sources for legitimation. To be sure, the party-state's consultation tools remain imperfect in the absence of civil

---

[451] *See* Carl Minzner, *Legal Reform in the Xi Jinping Era*, ASIA POL'Y, July 2015, at 4, 6 (detailing judicial reforms in the Xi era); Donald Clarke, *China's Legal System and the Fourth Plenum*, ASIA POL'Y, July 2015, at 10, 11–13 (same).

[452] *See, e.g.*, William P. Alford, *"Second Lawyers, First Principles": Lawyers, Rice-Roots Legal Workers, and the Battle over Legal Professionalism in China*, *in* PROSPECTS FOR THE PROFESSIONS IN CHINA 48–62 (William Alford et al. eds., 2011); Zhang & Ginsburg, *supra* note 302, at 313 (noting that bottom-up factors are "perhaps more important[ ]").

[453] *See* Qiaoan & Teets, *supra* note 305, at 140.

[454] *Id.*

[455] That the party-state suddenly reversed its zero COVID policy following the December 2020 protests further corroborates this point. *See* Amy Chang Chien, Chang Che & John Liu, *"Zero Covid," Once Ubiquitous, Vanishes in China's Messy Pivot*, N.Y. TIMES (Dec. 8, 2022), https://www.nytimes.com/2022/12/08/world/asia/china-covid-rollback.html.

society or contested elections, and Chinese leaders will not follow popular will when they perceive threats to their political security.

China's turn to privacy law also highlights tensions in the party-state's relationship with technology. In data, China's leaders see great opportunities to enhance social control, improve domestic governance, and grow strategic sectors of the economy. But as they have increased their investments in digital technologies, penetrating more deeply into facets of everyday life, they have encountered unappreciated risks as well.[456] Data may help improve products, create efficient cities, or contain the spread of disease, but too much, with too little protection, and there is risk of discontent. The very technologies meant to secure the durability of the regime might contribute to its undoing. As much as China's leaders have sought to use privacy law, among other tools, to minimize these risks, their long-run success remains uncertain.

Finally, China's turn to privacy law is an important case study in modern legal transplantation. It shows that despite a newfound focus on indigenous innovation and legal export, China has continued to selectively borrow from foreign legal regimes.[457] It also shows how privacy laws, like other legal forms with deep links to liberal theory—constitutions, election laws, speech protections, transparency regulations, and so on—remain amenable to appropriation by illiberal governments.[458] The party-state's embrace of privacy law is yet another example of how legal borrowing is more complex an act than copy-and-paste legal transplantation.

B. Authoritarian Privacy

China's turn to privacy law should also inform a broader theory of why authoritarian countries pursue privacy laws in general. There is now a rich literature on the functions of law under

---

[456] *Cf.* Rachel E. Stern, Benjamin L. Liebman, Margaret E. Roberts & Alice Z. Wang, *Automating Fairness? Artificial Intelligence in the Chinese Courts*, 59 COLUM. J. TRANSNAT'L L. 515, 549–50 (2021) (suggesting that "algorithmic analytics also present unseen challenges to the Chinese state").

[457] *See* Nicholas Calcina Howson, *Panel IV—"Can the West Learn from the Rest?"—The Chinese Legal Order's Hybrid Modernity*, 32 HASTINGS INT'L & COMPAR. L. REV. 815, 818–19 (2009); *id.* at 818 (describing the Chinese legal system as a "*potpourri* of formerly distinct systems" (emphasis in original)); XIAOQUN XU, HEAVEN HAS EYES: A HISTORY OF CHINESE LAW 107–17 (2020) (detailing the late Qing dynasty legal reforms that borrowed from Western legal traditions).

[458] *See* Tom Ginsburg, *Authoritarian International Law?*, 114 AM. J. INT'L L. 221, 241 (2020).

autocracy, complicating the image of authoritarian laws as either sham documents or solely repressive instruments.[459] Autocrats might use courts to support growth, to control subnational agents, or to provide routine dispute resolution.[460] Similarly, authoritarians might adopt constitutions to describe state structure, to advertise new policies, or to signal grand aspirations.[461] But laws like constitutions, and institutions like courts can also limit regime discretion and durability.[462] So autocrats have tried to minimize these dangers. They have sought to influence or control activists, litigants, lawyers, and judges, and they have drafted laws to expand and legitimize their prerogative powers.[463]

Privacy law may well follow a similar logic in authoritarian settings. As the China case suggests, information privacy laws can offer a number of regime-supporting benefits to authoritarian leaders in areas like legitimation, growth, influence, and security. But privacy laws can also have hidden risks. Privacy laws that apply too broadly might be seen as unduly constraining the state's policing, intelligence, and military activities. Privacy laws that encourage data trade and exchange may loosen the state's grip on sensitive information. Strict privacy laws may also impair the state's ability to leverage technology for growth, governance, or

---

459 *See* Rachel E. Stern, *Activist Lawyers in Post-Tiananmen China*, 42 LAW & SOC. INQUIRY 234, 235–36 (2017) (listing China alongside Russia and Singapore as "examples of legal systems that combine fair, efficient dispute resolution with ad hoc political meddling"); Trang (Mae) Nguyen, *In Search of Judicial Legitimacy: Criminal Sentencing in Vietnamese Courts*, 32 HARV. HUM. RTS. J. 147, 158–59 (2019).

460 *See, e.g.*, Stern, *supra* note 459, at 235–36 (dispute resolution); Moustafa & Ginsburg, *supra* note 300, at 4–10 (social control, legitimation, control of administrative agents, and signaling of credible economic commitments); Brian J.M. Quinn, *Vietnam's Continuing Legal Reform: Gaining Control over the Courts*, 4 ASIAN-PAC. L. & POL'Y J. 431, 449 (2003) (judicial reform in Vietnam); Jothie Rajah, AUTHORITARIAN RULE OF LAW: LEGISLATION, DISCOURSE, AND LEGITIMACY IN SINGAPORE 1–3 (2012) (rule of law in Singapore); James V. Feinerman, *New Hope for Corporate Governance in China?*, 2007 CHINA Q. 590, 590–93 (benefits of better corporate governance law); Margaret K. Lewis, *Criminal Law Pays: Penal Law's Contribution to China's Economic Development*, 47 VAND. J. TRANSNAT'L L. 371, 417–48 (2014) (criminal law's role in sustaining growth).

461 CONSTITUTIONS IN AUTHORITARIAN REGIMES, *supra* note 7, at 5–10.

462 *See* William P. Alford, *Double-Edged Swords Cut Both Ways: Law and Legitimacy in the People's Republic of China*, DAEDALUS, Spring 1993, at 45, 62; Moustafa & Ginsburg, *supra* note 300, at 11–14; Yvonne Tew, *Strategic Judicial Empowerment*, AM. J. COMPAR. L. (forthcoming 2024) (manuscript at 14–15); Wen-Chen Chang & David S. Law, *Constitutional Dissonance in China*, *in* COMPARATIVE CONSTITUTIONAL THEORY 476, 507–11 (Gary J. Jacobsohn & Miguel Schor eds., 2018).

463 *See* Kathryn Hendley, *Varieties of Legal Dualism: Making Sense of the Role of Law in Contemporary Russia*, 29 WIS. INT'L L.J. 233, 238 (2011); Hualing Fu, *Duality and China's Struggle for Legal Autonomy*, 116 CHINA PERSPS. 3, 5 (2019); SIDA LIU & TERENCE C. HALLIDAY, CRIMINAL DEFENSE IN CHINA: THE POLITICS OF LAWYERS AT WORK 2–7 (2016).

social control. And activists might even leverage privacy laws to limit regime discretion. The dilemma at the heart of authoritarian privacy is how to capitalize on privacy law's benefits while minimizing these costs.

From the China case, we can discern a multipronged solution. First, China's planners have drafted privacy laws to include large exceptional zones and harder data localization requirements.[464] These provisions help ensure that the granting of substantive privacy protections does not undercut the state's security or its capacity to leverage technology for control or governance. Second, the party-state has sought in both its framing and its enforcement of China's privacy laws to portray itself as a guardian of individual privacy rights against other malign private actors.[465] This can help foster popular goodwill and may even distract from areas of life where privacy laws do not constrain data collection and abuse. And third, China relies on its existing legal and media infrastructure, suffused with Party institutions and personnel, to ensure that any activist assertions of privacy rights are contained before they can spiral out of control.[466]

China is, of course, not a representative case. It has been unusually obsessed with digitization; it has more ambitious geopolitical goals than other authoritarian nations; and it is increasingly relying on law as an important source of legitimation. But aspects of China's approach may well have broader applicability. Russia's Federal Law on Personal Data, for example, contains familiar data privacy and data localization provisions.[467] The latter has not only been "weaponized against groups viewed as a threat to the governing regime," but also fueled imitation from other countries.[468] One might also look to other nations like Vietnam or Pakistan. Neither appears to have superpower aspirations, but they are in other relevant respects similar to China. Their governments have high-tech digital ambitions,[469] rely heavily on

---

464 PIPL, *supra* note 115, art. 35; *see also* Gorman, *supra* note 143.

465 *See infra* Part III.C.

466 *See* Stella Chen, *Another China Policy Critic Vanishes from Social Media Ahead of Party Congress*, S. CHINA MORNING POST (Sept. 20, 2022), https://www.scmp.com/news/china/politics/article/3193133/another-china-policy-critic-vanishes-social-media-ahead-20th (describing the government censorship of Lao Dongyan, an anti-FRT advocate).

467 *What Changes Do Russia's Latest Data Privacy Amendment Bring?*, SECURITI (Aug. 25, 2022), https://perma.cc/7F6P-7EDN.

468 Justin Sherman, *Russia Is Weaponizing Its Data Laws Against Foreign Organizations*, BROOKINGS (Sept. 27, 2022), https://perma.cc/7JAQ-PGF8.

469 Huong Le Thu, *Vietnam's Twin Tech Challenge: Spearheading While Catching Up*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 17, 2022), https://perma.cc/G9JF-V88Q ("The

surveillance technologies,[470] and have had to contend with a number of data privacy scandals.[471] Unsurprisingly, they have been drawn to personal information protection legislation with broad state exceptions.[472] They have also taken familiar steps to protect digital sovereignty and security.[473]

As the final Section will suggest, democracies are not cut from a wholly different cloth. Data localization laws are not the exclusive province of autocratic nations, nor do democracies have an exemplary record of embracing privacy when balanced against national security.[474] But to understand why repressive governments with no tradition of privacy laws are starting to embrace them, it helps to consider the nature of authoritarian legality generally.

Vietnamese government wants the digital economy to contribute to some 30 percent of GDP."); PAK. MINISTRY OF INFO. TECH. & TELECOMM., DIGITAL PAKISTAN POLICY 5 (2018) (describing the Digital Pakistan Policy, "a strategic enabler for an accelerated digitization ecosystem to expand the knowledge economy and spur socioeconomic growth").

[470] Gerard McDermott & Alice Larsson, *The Quiet Evolution of Vietnam's Digital Authoritarianism*, DIPLOMAT (Nov. 19, 2022), https://perma.cc/L5SD-X8ZK (describing how "Vietnam is attempting to imitate China's system of surveillance and information control"); Erie & Streinz, *supra* note 177, at 71–75 (describing Pakistan's adoption of digital surveillance technologies in partnership with Chinese companies).

[471] *See* Luu Quy, *Vietnam Has Major Data Leak Problem, Citizens Suffer*, VN EXPRESS (Aug. 19, 2022), https://perma.cc/YN8Y-LZ6P (discussing data leaks, data black markets, and the state response); Gaurvi Narang, *Nothing Secure About Pakistan's Cybersecurity. PMO Leaks Latest Example*, PRINT (Sept. 27, 2022), https://perma.cc/TX8J-YJSA (discussing personal data leaks).

[472] *See generally* Dominic Paulger, *New Report on Limits of "Consent" in Vietnam's Data Protection Law*, FUTURE OF PRIV. F. (Aug. 3, 2022), https://perma.cc/76J9-9GFM (referring to broad exceptions for "national security, social order, and safety" in Vietnam's draft data protection laws); Erie & Streinz, *supra* note 177, at 79–80 (referring to "huge exceptions" for state-held data in Pakistan's draft privacy laws). Vietnam recently enacted a Decree on the Protection of Personal Data codifying some of these broad limitations. Kat MH Hille, *Vietnam's Personal Data Protection Decree: Overview, Key Takeaways, and Context*, FUTURE OF PRIV. F. (May 12, 2023), https://perma.cc/MY5B-BWGL (analyzing Article 14 on national security, public order, and safety exceptions).

[473] *See* McDermott & Larsson, *supra* note 470 (describing how Vietnam's 2019 Cybersecurity Law requires local data storage); Erie & Streinz, *supra* note 177, at 78–79; *id.* at 80 (concluding that "Pakistan and China demonstrate congruence in approaches to data governance").

[474] *See* Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 AM. U. BUS. L. REV. 11, 12–13, 15 (2015) (discussing National Security Agency (NSA) surveillance in the United States); David C. Vladeck, *Litigating National Security Cases in the Aftermath of 9/11*, 2 J. NAT'L SEC. L. & POL'Y 165, 166 n.6, 190 (2006) (describing warrantless surveillance in the wake of 9/11); James D. Fry, *Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. PA. J. INT'L L. 419, 422, 481 (2015) (suggesting that the United States' approach to internet surveillance is in one sense less honest and transparent than China's).

C. Privacy, Autocracy, and Democracy

Finally, there is a constructive tension between the story told here and ideas about privacy in the United States. Privacy scholars have long seen privacy as conceptually interwoven with democracy.[475] In his classic work, *Privacy and Freedom*, scholar Alan Westin "contrast[ed] privacy in the democratic and the totalitarian state."[476] Whereas fascist and communist societies attack privacy as "part of the cult of individualism," he explained, "strong citadels of individual and group privacy" are a "prerequisite for liberal democracies."[477] Scholars since Westin have similarly regarded privacy as either necessary for, or highly conducive to, a vibrant democratic life. Law scholar Ruth Gavison stated that she sees privacy as "essential to democratic government because it fosters and encourages the moral autonomy of the citizen."[478] Privacy scholar Paul Schwartz has said that "strong rules for information privacy" are needed for deliberative democracy.[479] Privacy theorist Julie Cohen has argued that "conditions of diminished privacy" will shrink our "capacity for democratic self-government."[480]

In much of this literature, authoritarianism serves mainly to contrast how privacy works, or should work, in democratic societies. In explaining how "self-repression . . . could undermine the self-critical capacities of a polity," law scholar Jerry Kang described how "totalitarian regimes have maligned a desire for privacy as deviant . . . to sap an individual's ability to question the status quo."[481] Scholar Edward Bloustein has contrasted democracy's "deep-rooted respect for group privacy" with autocracies that try to "control the total social and political environment."[482] Legal scholar Jed Rubenfeld has based privacy in an "anti-totalitarian principle," the "freedom not to have one's life too totally determined by a progressively more normalizing state."[483]

---

[475] This is true both descriptively (autocracies lack privacy; democracies have them) and normatively (we need more privacy to ensure proper democratic life).

[476] WESTIN, *supra* note 39, at 23.

[477] *Id.* at 23–24.

[478] Gavison, *supra* note 1, at 455.

[479] Schwartz, *supra* note 1, at 1651.

[480] Cohen, *What Privacy Is For*, *supra* note 1, at 1912. Privacy theorists also see privacy as advancing other goods apart from democracy, like psychological well-being and intimate relationships. SOLOVE, *supra* note 27, at 79–80.

[481] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1993, 1217 & n.93 (1998).

[482] Edward J. Bloustein, *Group Privacy: The Right to Huddle*, 8 RUTGERS-CAMDEN L.J. 219, 279 (1977).

[483] Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 784, 787 (1989).

And legal scholar Spiros Simitis has argued that "considerations of privacy protection . . . determine the choice between a democratic and an authoritarian society."[484]

My purpose in referencing these works is not to detach privacy from its normative democratic underpinnings, but to set up two points of reflection. First, the concepts of "democracy" and "autocracy" envisioned in this literature are idealized ones that sit in tension with observed reality. Indeed, neoliberal democracies today have more in common with market-oriented autocracies than a diametric understanding of democracy and autocracy would predict. Cohen has described how "processes [in the United States] that have worked for centuries to foster deliberative dialogue and democratic self-government are revealed to be newly fragile and unthinkably vulnerable" in political economies dominated by information platforms.[485] In China, transformations in information technology have likewise produced ascendant forms of private economic power with risks to both political powerholders and ordinary individuals. Both countries are in the midst of an effort to contain these forces for a variety of reasons, only some of which are shared. Yet in both cases, privacy laws have emerged as an increasingly favored basis for regulation.

The second, more methodological point, is that the privacy-democracy nexus likely affects how we process privacy developments in the nondemocratic world. As William Alford has warned, "our efforts at engaging in broad theoretical work may unwittingly lead us to believe that we are considering foreign legal cultures in universal or value-free terms, when, in fact, we are examining them through conceptual frameworks that are products of our own values and traditions."[486] These frameworks can lead us to systematically overlook or oversimplify areas of both similarity and difference.[487]

---

[484] Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987). Authoritarian undertones also figure in two favorite metaphors in the privacy literature: philosopher Jeremy Bentham's panopticon and Orwellian dystopia. *See, e.g.*, RICHARDS, *supra* note 38, at 126–27 (invoking both metaphors to highlight "the stifling effects of surveillance on our expression").

[485] COHEN, BETWEEN TRUTH AND POWER, *supra* note 34, at 106; *cf.* Yochai Benkler, *Degrees of Freedom, Dimensions of Power*, DAEDALUS, Winter 2016, at 18, 20, 30–31 (discussing the democratic potential of the internet as it was originally designed in light of modern developments).

[486] William P. Alford, *On the Limits of "Grand Theory" in Comparative Law*, 61 WASH. L. REV. 945, 946 (1986).

[487] *See, e.g.*, Donald C. Clarke, *Puzzling Observations in Chinese Law: When Is a Riddle Just a Mistake*, *in* UNDERSTANDING CHINA'S LEGAL SYSTEM: ESSAYS IN HONOR OF

This Article hopes to have shown the existence of a more complex interplay between privacy, democracy, and autocracy than preexisting conceptual constructs might suggest. We have seen, for instance, how privacy law can advance not just democratic rights, but also authoritarian interests. Some of these interests have been more top-driven; others, I have argued, have been more reactive. But in either case, we see privacy law's appeal to the rational self-interest of authoritarian rulers. Indeed, autocrats may even face fewer barriers in implementing data privacy laws than democratic leaders, who have to contend with speech protections, or powerful industrial lobbies and civil society groups.

At this point, one might argue that China's laws aren't "real" privacy laws because they are more often enforced against private rather than state actors; legal scholar James Whitman has said that the "conceptual core" of the "American right to privacy . . . is the right to freedom from intrusions by the state."[488] But while there are critical differences between Chinese privacy laws and their foreign counterparts, privacy theorists here have also offered powerful critiques of private surveillance.[489] The "typical privacy claim is not a claim for noninterference by the state at all," noted Gavison. Rather, "[i]t is a claim *for* state interference in the form of legal protection against other individuals."[490] This is all the more true today, where, in the words of law scholar Jonathan Zittrain, the internet "puts private individuals in a position to do more to compromise privacy than the government and [traditional] commercial institutions."[491] China may not have a normatively attractive privacy regime, but it has one all the same.

This Article also highlights how even in authoritarian societies, there can also be quasi-democratic drivers of privacy law that we may be predisposed to overlook. There is a reflexive tendency to model China's privacy laws purely as the product of authoritarian instrumentalism. This is all the more tempting in the current political moment, with General Secretary Xi's now indefinite tenure as paramount leader, and in the current geopolitical moment, when U.S.-China competition is framed as a battleground

---

JEROME A. COHEN 93, 103–09 (C. Stephen Hsu ed., 2003) (discussing the flaws of interpreting the Chinese *Xianfa* through a Western constitutional framework).

488 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

489 *See, e.g.*, Cohen, *What Privacy Is For*, *supra* note 1, at 1906 (expressing concern over "both public and private systems of surveillance").

490 Gavison, *supra* note 1, at 438 (emphasis in original).

491 Jonathan L. Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 65.

between democracy and autocracy.[492] But while there is analytic utility to speaking of an authoritarian approach to privacy law, stereotypes about authoritarian societies can mislead more than they can inform.[493] By isolating foreign authoritarian nations as existing in a wholly different realm from our own, we are that much more likely to miss points of commonality.[494] China's citizens cannot elect their leaders, and so lack traditional modes of democratic accountability. But responsive policymaking continues to be a key source of regime legitimacy in China today, and there remain pressure points through which popular sentiment can influence public policies. Chinese citizens are not merely subjects that are surveilled or acted upon. They are also agents whose support is required to sustain party rule.

Lastly, I would merely observe that autocracies and democracies can be drawn to privacy laws for surprisingly similar reasons. Materials advocating for privacy legislation here in the United States evince familiar themes. Federal privacy law, we are told, would enhance our economy, improve our global positioning, protect our national security, and accord with popular demand.[495] To be sure, we have other more particular reasons for wanting a federal privacy law, including ones that would have little appeal to China's leaders. But there is enough that is shared to suggest that authoritarian privacy is part of a more universal story of technological change—one that is putting significant pressure on virtually every kind of actor in the modern world. While we do not know how this story will progress, we can hope that its shapers will be not just states or firms, but people too.

---

[492] *See* Mark Jia, *American Law in the New Global Conflict*, N.Y.U. L. REV. (forthcoming 2024) (manuscript at 12–14) (on file with author).

[493] *See* Mark Jia, *Illiberal Law in American Courts*, 168 U. PA. L. REV. 1685, 1722, 1724 (2020).

[494] *Cf.* TEEMU RUSKOLA, LEGAL ORIENTALISM: CHINA, THE UNITED STATES, AND MODERN LAW 9 (2013); Marlies Glasius, *What Authoritarianism Is . . . and Is Not: A Practice Perspective*, 94 INT'L AFFS. 515, 525–26 (2018) (introducing a practice-based definition of authoritarianism that locates authoritarian trends across various regime types).

[495] *See* Williams, *supra* note 94 (pointing to the security and geopolitical benefits of federal privacy law); *Federal Data Privacy Legislation*, *supra* note 141 (pointing to the economic benefits of federal privacy law); Chris Teale, *Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law*, MORNING CONSULT (June 15, 2022), https://perma.cc/ATM4-D26F (finding that over 80% of voters support major provisions of a draft privacy bill).