Co-Producing Surveillance: Technology, Law, and State–Society Relations in Asia

Ya-Wen Lei & Ching-Fu Lin

ABSTRACT

Amid the global intensification of surveillance through digital and biometric technologies, this review conceptualizes surveillance as the co-production of law, technology, and state–society relations. Examining cases from China, India, Singapore, Japan, South Korea, and Taiwan, it develops a spectrum of techno-legal co-production shaped by the degree of alignment or contestation between law and technology. At one end, authoritarian synergy integrates legal and technological systems to consolidate control; at the other, rights-bounded contestation in Japan, South Korea, and Taiwan constrains surveillance through legal safeguards, judicial oversight, and civic activism, while India and Singapore occupy hybrid middle positions. Across these contexts, surveillance emerges through dynamic interactions among state, corporate, and civic actors. Future research should extend this comparative framework to additional Asian contexts and explore the transnational dimensions of surveillance, including the diffusion and hybridization of legal norms, the circulation of technologies and governance models, and the emergence of transnational networks of resistance and accountability.

Keywords: Surveillance, law, technology, state–society relations, co-production, Asia

Ya-Wen Lei: Department of Sociology, Harvard University, Cambridge, MA, USA; email: yawenlei@fas.harvard.edu

Ching-Fu Lin: Institute of Law for Science and Technology, National Tsing Hua University, Hsinchu, Taiwan; email: chingfulin@mx.nthu.edu.tw

Acknowledgement:

Ching-Fu Lin gratefully acknowledges support from Taiwan's National Science and Technology Council and the research assistance of his PhD student, I-Ching Chen.

INTRODUCTION

Surveillance refers to the organized process of gathering, interpreting, and applying information about people, groups, or settings. It extends beyond state activity, encompassing a wider mechanism of social organization employed by governments, corporations, communities, and individuals to structure political, economic, and social life. As scholars of surveillance studies note, these practices are *janus-faced*: they can facilitate coordination and resource distribution, yet also enable control, exclusion, and inequality (Ball et al 2012). In this sense, surveillance operates both as a response to threats and as a threat itself (Marx 2015).

As elsewhere, surveillance has long been integral to governance and social organization in Asia (Murakami Wood et al 2007, Pei 2024). What distinguishes the current era is not the existence of surveillance but its intensification and acceleration through digital and biometric technologies that vastly expand the capacity to monitor, analyze, and intervene in everyday life (Lyon 2003). Promoted as tools of efficiency, security, and modernization, these systems also raise fundamental questions about legality, accountability, and power. Yet within this shared context of technological intensification, surveillance in Asia unfolds unevenly. It reflects distinct institutional arrangements and state–society relations that shape how digital infrastructures are built, governed, and contested. Attending to this variation reveals how global technological acceleration interacts with local legal and political contexts to produce different *varieties of surveillance*.

This review conceptualizes surveillance as the co-production of law, technology, and state–society relations (Jasanoff 2004). Technology and law function as interlocking mechanisms that both enable and constrain surveillance (Lei 2023, Marx 2015). Surveillance technologies—from foundational identification infrastructures to sectoral applications in policing, welfare, health, and urban management—shape governance through their material affordances: they render populations legible and intervene in social life. Law, in turn, authorizes, legitimizes, and constrains these practices, serving as an arena in which state power, corporate interests, and individual rights are continuously negotiated. State–society relations—the dynamic configurations linking the state, business actors, and civil society (Wolf 2008)—shape whether law and technology primarily serve to entrench coercion, enhance administrative efficiency, or safeguard rights. This relational perspective moves beyond static regime typologies by emphasizing the interactions among these actors. In short, state–society relations condition how law and technology are mobilized and to what ends.

These dynamics produce distinct configurations of surveillance across Asia, reflecting varying degrees of alignment and contestation between law and technology. At one end of the spectrum, in China, law and technology operate in concert under an authoritarian state, state-aligned firms, and a weak civil society, creating a techno-legal synergy that consolidates political control. At the other end, Japan, South Korea, and Taiwan exemplify rights-bounded contestation, where legal safeguards, judicial oversight, and civic activism discipline technological expansion. India and Singapore occupy an intermediate position, where law and technology are only partially aligned—enabling expanding surveillance while still preserving limited spaces for accountability and contestation. These cases reveal a continuum of techno-legal co-production shaped by

regime type, state and technological capacity, civic mobilization, and legal culture. They illustrate how the interplay of law, technology, and state–society relations gives rise to diverse forms of surveillance across Asia. Building on this comparative mapping, the review advances a relational framework of techno-legal co-production that explains how variation in state–society relations shapes the alignment between law and technology and, in turn, produces distinct surveillance regimes**.**

The article proceeds as follows. The next section maps the key actors in Asia's surveillance ecosystem, followed by an examination of technological architectures, from foundational identification systems to sectoral deployments. The subsequent section analyzes how legal frameworks authorize and constrain surveillance, highlighting courts as sites of contestation. Building on these analyses, the review develops a spectrum of techno-legal co-production and concludes with reflections on implications for law, technology, and governance in Asia and directions for future research.

MAPPING THE SURVEILLANCE ECOSYSTEM: STATE, CORPORATE, AND CIVIC ACTORS

Surveillance in Asia operates within a complex, interconnected ecosystem in which state agencies, private firms, public–private consortia, and civic actors interact through technology and law to co-produce distinct surveillance regimes—each with its own origins, designs, methods, processes, intermediaries, and outcomes.

State actors justify surveillance in the name of national security, public safety, and administrative efficiency, aiming both to preempt threats and to project political legitimacy through responsive governance. Such measures often resonate with public expectations that the state should ensure safety by preventing crime and terrorism, thereby reinforcing the social acceptance of expanded surveillance. Ministries of public security, intelligence services, and regulatory bodies advance these aims by deploying law to mandate data flows, retention, and identity linkage, while constructing foundational infrastructures that support applied uses (Balkin 2008, Johns 2021, Weller 2012). Crises such as social unrest, terrorist attacks, and pandemics frequently act as accelerators, providing governments with opportunities to introduce "exceptional" surveillance measures—ranging from counter-terrorism frameworks to digital health tracking—that later become normalized. Yet state actors differ across and within countries in their capacity to enact and implement surveillance (Liu 2022).

The private sector also plays a significant role, driven by the economic logic of profit-seeking. The model of "surveillance capitalism" depends on large-scale extraction, profiling, and commodification of user data for purposes such as targeted advertising (Zuboff 2019). Beyond data monetization, corporations serve as key intermediaries by building and maintaining infrastructures—cloud services, telecom networks, and identity authentication systems—that states routinely leverage. In China, firms such as Huawei and Alibaba exemplify this public–private symbiosis: they benefit from state contracts, subsidies, and market protections, while the government capitalizes on their technological innovations and infrastructures to expand its surveillance capacity (Huang & Tsai 2022, Lei 2023). This dynamic extends transnationally. Companies from the Global North historically supplied core surveillance technologies to China,

while today Chinese firms export such systems globally, including to certain Asian countries (Bernot 2022). These patterns suggest that surveillance capitalism functions not merely as a domestic economic logic but as a global political economy in which state imperatives and corporate profit-seeking are structurally intertwined, jointly driving the expansion and normalization of surveillance.

Finally, surveillance extends downward through community-based and participatory mechanisms. Driven by a logic of responsibilization, these practices enlist citizens as co-producers of order, diffusing the labor of surveillance. China's "grid management" system, for instance, institutionalizes neighborhood-level monitoring by equipping local cadres and volunteers with mobile apps to record and report on residents (Tang 2020). Such arrangements enable the population-level sorting of individuals into categories of eligibility or scrutiny, embedding surveillance into the routines of everyday life and linking grassroots practices to wider state and corporate systems of control. Yet community actors are not only conscripts into surveillance; they may also resist, subvert, or reinterpret these practices—through noncompliance, selective reporting, or collective opposition—revealing the contingent and contested nature of surveillance on the ground (Murakami Wood et al 2007).

TECHNOLOGIES OF SURVEILLANCE

Technologies of surveillance constitute and intensify Asia's surveillance regimes. These technologies can be understood through a layered lens that distinguishes between *foundational infrastructures of legibility* and *applied sectoral deployments*. Foundational technologies, as described by Bennett and Lyon (2008), render individuals and populations visible and linkable across systems, while applied technologies mobilize these foundations for specific governance purposes such as national security, policing, welfare, health, or urban management.

Foundational Infrastructures of Legibility

National identity systems are central to contemporary surveillance infrastructures in Asia. In China, the second-generation Resident Identity Card is mandatory for nearly all citizens aged sixteen and above. It serves as both a physical credential and a chip-embedded smart card containing an 18-digit ID number, photo, and—since 2013—fingerprint data, following an amendment to the Resident Identity Card Law. Closely tied to the *hukou* registration system and required across administrative and commercial services, the card underpins identification, authentication, and access to banking, travel, education, and telecommunications (Brown 2008).

India's Aadhaar system—initiated around 2009 and rolled out in 2010—is the world's largest biometric identification program. Each enrollee receives a 12-digit number linked to fingerprints, iris scans, and demographic data stored by the Unique Identification Authority of India. Although formally voluntary, Aadhaar has become *de facto* mandatory for many services. Initially designed to curb fraud and inefficiency in welfare distribution, it has since become an authentication mechanism used in banking, taxation, subsidies, and telecommunications. Scholars describe it as a "datafier" that transforms populations into machine-readable "coded citizens," enabling a platform for welfare and financial services—and, critics argue, serving as surveillance infrastructure in practice (Henne 2019, Rao & Nair 2019). Proponents emphasize

efficiency and financial inclusion, while critics warn of exclusion errors (e.g., biometric failures), privacy risks, and surveillance overreach.

In Japan, the My Number system assigns each resident a 12-digit number for administrative purposes, including taxation, social security, and disaster response. The My Number card—which includes a photo and IC chip—is voluntary, and although adoption has risen over time, full uptake remains incomplete. The government has sought to expand the card's use in financial institutions and other private sectors, but public skepticism persists, fueled by privacy concerns and documented data mishandling incidents (Matsui 2019).

In Taiwan, the national identification card has long been a mandatory document, embedded in the household registration system and required for voting, banking, telecommunications, and other administrative or commercial procedures. Efforts in the late 1990s and 2000s to add fingerprint databases and create multi-purpose smart cards encountered strong resistance. Alongside the ID system, Taiwan's national health insurance card, introduced in the 1990s, has become one of the most widely used identification tools (Kuo & Chen 2016).

Beyond national ID systems, SIM card registration has become a complementary tool of surveillance. Over 150 countries now mandate some form of SIM registration, typically justified on security grounds despite limited empirical evidence of its effectiveness (Krishnakumar 2021). In Asia, China links SIM cards to resident IDs (Lee & Liu 2016), while India requires ID verification and uses Aadhaar to link SIM cards (Henne 2019). By reducing anonymity in communications, SIM registration enables lawful interception, location tracking, and cross-database integration.

In tandem, national ID systems and SIM registration create the basic rails of visibility, interoperability, and traceability that make other forms of surveillance possible. In many cases—such as in China and India—these infrastructures incorporate biometric data. Biometric identifiers matter because they anchor identities to bodies, enabling real-time facial recognition, forensic matching, and routine authentication across services. More broadly, as foundational infrastructures of legibility, ID and SIM systems extend the reach of the state and provide the substrate upon which applied systems embed surveillance in everyday governance.

Applied Deployments by Domain

Building on these foundational systems, states deploy surveillance technologies for specific governance purposes, transforming technological and data infrastructures into instruments of administrative efficiency, social profiling, risk prediction, and state control.

Predictive Policing and Risk-Scoring

The rise of surveillance technologies in policing reflects a global shift toward predictive, data-driven security. Across Asia, governments deploy these tools to enhance efficiency and crime prevention, yet concerns about accuracy, bias, and civil liberties persist, and their scope and design vary widely.

China represents the most expansive case. Building on national ID and data infrastructures, platforms such as the Integrated Joint Operations Platform and Police Cloud aggregate biometric, travel, financial, and communication data to flag individuals for scrutiny (Sprick 2019). These systems operate alongside extensive CCTV networks under programs like Safe City and Sharp Eyes, which extend surveillance into both urban and rural areas and increasingly rely on facial recognition technologies (Hung & Yen 2021). Although officially framed as crime prevention or predictive policing, scholars argue that these tools serve selective repression—particularly targeting ethnic minorities in Xinjiang and political dissidents (Sprick 2019, Lei & Kim 2024).

India has pursued ambitious but uneven deployments. Delhi's Crime Mapping, Analytics, and Predictive System and Hyderabad's Integrated People Information Hub combine crime records, satellite imagery, and biometric or financial data to identify hotspots (Marda & Narayan 2020). The proposed Automated Facial Recognition System aims to integrate police databases nationwide, while several states are rapidly expanding CCTV coverage.[1] These initiatives are promoted as enhancing efficiency, but evaluations highlight accuracy problems and algorithmic bias, particularly against minorities (Basheer 2025).

Elsewhere in Asia, deployments are more limited or remain experimental. Singapore's PolCam 2.0 expands its dense camera network with video analytics and anomaly detection, reflecting a broader smart-city model (Mangkhalasiri & Poothakool 2025). South Korea's Smart Policing System pilots AI-enabled cameras and predictive tools, supported by robust digital infrastructure but facing public skepticism over privacy (Lee et al 2025, Moon et al 2017). Japan has issued formal guidelines for the use of facial recognition in airports through the One ID boarding system, while deployments in retail, transport, and advertising have faced criticism and, in some cases, modification or postponement (Ozaki 2020). Taiwan has largely confined AI policing to retrospective video analytics and targeted applications such as traffic enforcement, with little evidence of large-scale predictive policing programs.

Digital Welfare Systems

The integration of surveillance technologies into welfare systems reflects a global shift toward the *digital welfare state* (Van Toorn et al 2024). Governments employ data integration, automated eligibility checks, fraud detection, and biometric authentication to reduce costs and curb leakage. While automation promises speed and consistency, it also subjects low-income populations to intensified scrutiny. Critics caution that such systems risk reinforcing inequality by turning welfare recipients into highly monitored populations, while also producing exclusion and undermining privacy (Eubanks 2018, Zajko 2023).

Asian experiences illustrate both the ambitions and contradictions of welfare surveillance, though their scope and design vary considerably. In India, the Aadhaar program anchors welfare distribution through fingerprint and iris authentication (Rao & Nair 2019). Integrated into the Direct Benefit Transfer system and the broader JAM trinity—Aadhaar ID, Jan Dhan bank accounts, and mobile access—Aadhaar is credited with eliminating duplicate beneficiaries and streamlining delivery.[2] At the same time, biometric failures have excluded vulnerable populations, underscoring enduring tensions between efficiency and social rights (Rao & Nair 2019).

In China, welfare governance has become increasingly integrated with digital and AI-driven systems through large-scale data collection and automated decision-making. Pilot programs use AI to identify households for targeted poverty alleviation, detect healthcare fraud, and match job seekers with employment opportunities—often in conjunction with broader state surveillance infrastructures. While these initiatives are framed as enhancing efficiency and effectiveness, they raise concerns about privacy, algorithmic bias, and the lack of citizen oversight (Qiang 2025).

While India and China have expanded digital welfare through biometric authentication and AI-driven systems, other parts of Asia remain less extensive. Taiwan offers a contrasting example. Since 2012, it has operated the National Social Welfare Benefits Data Comparison System Database, which integrates tax and social assistance records. Designed primarily to reduce costs, streamline administration, and prevent double-dipping or fraud in welfare claims (Huang 2023), this narrower model contrasts with the more expansive, technology-intensive systems seen in India and China.

Public Health

The COVID-19 pandemic accelerated the adoption of digital surveillance for public health across Asia. Governments implemented app-based contact tracing, big-data integration, and biometric checkpoints, drawing on foundational infrastructures such as national ID systems and SIM registration. The urgency of effective crisis response legitimized expansive administrative powers and sidelined legislative and judicial oversight. Yet once emergency measures—particularly surveillance infrastructures—are adopted, they tend to persist and become normalized beyond their exceptional context (Lin et al 2020).

In China, the Health Code system emerged in early 2020 when Hangzhou and Shenzhen, working with Alibaba and Tencent, introduced QR-code apps to manage post-lockdown mobility. Embedded in Alipay and WeChat, the model spread rapidly nationwide, producing local variants until the State Council mandated integration through a national platform. Even then, local discretion persisted and interoperability remained uneven (Cong 2021, Yang et al 2021). Drawing on self-reports and telecom, transport, hospital, and public security data, the codes generated green, yellow, or red passes (Liang 2020). In practice, the system was effectively compulsory: a green code was required for travel, work, and access to public spaces. Promoted as "scientific epidemic control," it functioned less as contact tracing than as population management, relying on smartphones, networks, checkpoints, and the labor of community workers and police—revealing that surveillance was never fully automated. Contradictions soon emerged: officials overrode algorithmic outputs, misclassifications eroded trust, and citizens gamed the system through screenshots, false inputs, or lax enforcement (Liu 2022). Reliance on smartphones also deepened the digital divide, excluding the elderly, poor, and digitally marginalized (Yu 2022).

In 2020, India launched Aarogya Setu as both a contact-tracing tool and an experiment in participatory disease surveillance. Combining Bluetooth, GPS data, and self-reported symptoms, it generated risk scores and offered chatbot advice, ministry updates, and helplines (Garg et al 2020). Initially mandatory for government employees, many private workers, and travelers, it was made formally voluntary after legal and public pushback, though de facto requirements

persisted. By late 2020, downloads exceeded 150 million, with surveys showing high usage but lower uptake among women, students, and the less educated (Juneja et al 2021). Promoted as a model for digital health governance and linked to the National Digital Health Mission, the app drew criticism over privacy, transparency, and exclusion, as smartphone dependence further marginalized poorer and rural populations (Garg et al 2020).

Other states adopted intensive health surveillance but under stronger legal or social constraints. In South Korea, the Epidemic Investigation Support System integrated GPS, CCTV, credit card, immigration, and telecom data to reconstruct patient trajectories within hours. Framed as "virtuous surveillance," it emphasized transparency through text alerts and dashboards, but disclosures sometimes enabled re-identification and stigma, sparking privacy debates and policy revisions (Shaw et al 2020, Yang 2022, Yuan 2021). Singapore launched TraceTogether as a Bluetooth app, later extended to tokens and mandatory SafeEntry check-ins. Initially voluntary and framed as privacy-preserving, it gained traction only after mandates. Public trust declined when police access was revealed, prompting petitions, statutory limits on data sharing, and token redesigns (Lee & Lee 2022, Stevens & Haines 2020). At the same time, bottom-up civic initiatives complemented state systems, while outbreaks in migrant worker dormitories and the struggles of "digital outcasts" exposed persistent inequalities (Das & Zhang 2021). In Taiwan, authorities combined health insurance, border, and telecom data to operate an "Electronic Fence" for monitoring quarantined individuals—praised for effectiveness but criticized for privacy risks (Huang 2023).

In Japan, pandemic surveillance reflected strong privacy norms and institutional caution. Unlike South Korea, authorities avoided telecom and financial data, relying instead on interviews and cluster-based tracing (Shaw et al 2020). In June 2020, the government launched COCOA, an exposure-notification app based on the Apple–Google decentralized Bluetooth model, deliberately avoiding location tracking or personal identifiers (Ichihara 2020). While consistent with domestic privacy expectations, COCOA was hampered by major flaws: bugs left the Android version inoperative for months, health centers struggled to link notifications to timely PCR testing, and uptake was uneven. By early 2021, tens of millions had downloaded the app, but only a small fraction of positive cases were registered, limiting its epidemiological impact (Nakajima & Tsuji 2022).

Urban Governance and Smart Cities

The integration of surveillance infrastructures into urban governance reflects the rise of the smart city, where digital systems promise efficiency, coordination, and real-time oversight. Across Asia, governments and vendors have deployed platforms that combine CCTV, IoT sensors, and AI dashboards—marketed as neutral modernization while embedding governance priorities into contracts and technical standards. These systems render urban life newly legible and manageable, though their scope and design vary by country.

China has developed the most ambitious smart city programs, where national AI leadership converges with local experimentation. In Shanghai, designated a national AI pilot zone, authorities have rolled out applications in public security, waste management, housing, and transport, framing them as upgrades to the city's "urban operating system" (Marvin et al 2022).

Hangzhou illustrates a corporate-led model through Alibaba's City Brain, which integrates CCTV, GPS, and IoT data for traffic, fire, and policing. Initially aimed at congestion management, City Brain is now marketed to other Chinese and international cities. Together, these cases reveal a dual logic: AI serves simultaneously as an instrument of urban surveillance and social control, and as a commercial product within global capitalism (Marvin et al 2022).

Singapore has developed a highly integrated model of smart urbanism, exemplified by the Safe City Test Bed, which links cameras, facial recognition, and analytics across agencies in centralized control rooms. The Smart Urban Living pilot in Yuhua Estate embedded sensors in homes and neighborhoods, where residents variously embraced, ignored, or resisted the technologies (Yeo 2023). Scholars interpret these initiatives as part of a longer genealogy of "sedimented" surveillance, in which successive layers of governance and technology have normalized pervasive monitoring in everyday life (Woods et al 2025).

South Korea has advanced smart city development through projects such as Songdo and Sejong, built with dense IoT networks, CCTV integration, and centralized dashboards. Framed around environmental management, transport, and disaster response, these systems embed surveillance into daily urban operations. A national Smart City Data Hub further integrates municipal data for real-time monitoring. During the pandemic, this infrastructure was repurposed for epidemic control, revealing how tools designed for efficiency and safety can extend into population surveillance (Sonn & Lee 2020, Yang 2022). While broadly accepted, concerns persist over privacy, data exposure, and state overreach. The Korean model highlights both the technological ambition of ubiquitous smart cities and the dilemmas of transparency and oversight.

Taiwan's smart city development reflects a model that combines national coordination with local experimentation. Led by the Smart City Taiwan Project under the Industrial Development Bureau, the government promotes public–private partnerships linking central ministries, municipalities, and firms to pilot and scale digital solutions. This dual top-down and bottom-up strategy sets national priorities—such as mobility, healthcare, and sustainability—while allowing cities to design context-specific applications. Projects span smart policing, water management, and telemedicine, emphasizing service delivery and citizen participation (Leu et al 2021). Surveys indicate strong public support for initiatives improving safety, transport, and the environment, alongside concerns about privacy protection and equitable access to digital services, particularly for older or rural populations (Ji et al 2021).

Compared with its neighbors, Japan has adopted a more cautious approach to smart city development. Facial recognition pilots at Osaka Station and Osaka Metro were suspended following strong public criticism (Ozaki 2020), reflecting deep-seated privacy norms. Most Japanese smart city projects focus on energy efficiency, disaster resilience, and sustainable mobility rather than comprehensive data integration or large-scale surveillance (Ryu & Lim 2023). National initiatives such as the Society 5.0 vision promote technological innovation for social well-being, but implementation remains gradual and consensus-driven, emphasizing transparency, citizen trust, and environmental sustainability over data-driven control (Deguchi 2020). Japan thus represents a restrained and sustainability-oriented model of smart urbanism, where privacy concerns and civic values set clear boundaries on the adoption of surveillance technologies.

Cross-Sector Integration

While earlier cases show surveillance technologies operating within discrete domains such as policing, welfare, health, or urban management, recent developments highlight efforts to integrate these logics into more comprehensive governance regimes. Rather than remaining field-specific, such systems link diverse data sources and institutions to classify and govern populations holistically.

China's Social Credit System is the most ambitious example. Emerging from fragmented pilots in the early 2000s, it combines financial credit reporting, government blacklists and redlists, municipal scoring schemes, and commercial platforms into a hybrid regulatory regime. At its core, the Social Credit System quantifies trustworthiness across domains—from debt repayment and contract compliance to professional conduct and civic behavior—and ties these assessments to sanctions and rewards such as travel restrictions, loan eligibility, and access to public services (Liang et al 2018, Liu 2019). Scholars interpret the system both as regulatory infrastructure designed to address information asymmetries and as a disciplinary instrument that enforces state-defined norms of morality, loyalty, and order (Hou & Fu 2024, Liang & Chen 2022). Public opinion research suggests that popular support reflects not only demand for social trust but also the state's success in obscuring the system's coercive potential through propaganda and selective invisibility (Xu et al 2022). Yet a sharp gap persists between state ambitions and local realities, as implementation remains fragmented and uneven (Liu forthcoming).

Across Asia, surveillance technologies differ in scale and scope. In China, expansive digital infrastructures function as instruments of governance and social control. India and Singapore occupy a middle ground, where surveillance expands rapidly under developmental and security narratives but remains more uneven and contested than in China. By contrast, Japan, South Korea, and Taiwan adopt more restrained approaches shaped by strong privacy norms and democratic accountability. These cases reveal a continuum of surveillance intensity across the region.

THE LEGAL FRAMEWORK

This section examines the dual function of law in shaping surveillance across Asia. On the one hand, law enables and legitimizes the expansion of surveillance by granting actors statutory authority to monitor and collect information. On the other hand, it constrains state power by imposing limits and establishing venues and doctrines for rights-based contestation.

Law as Enabling Infrastructure

Legal frameworks across Asia provide both legitimacy and structure for surveillance. Beyond merely justifying surveillance, laws embed political and policy choices within technical systems, translating concepts such as national security, public order, and digital sovereignty into code and infrastructure. These legal vocabularies enable governments to securitize social and economic life and to justify exceptional technological interventions. However, the ways in which laws are enacted and applied to enable surveillance vary widely across different contexts.

In China—the most extensive case of state surveillance—legal and policy frameworks operate in tandem to institutionalize monitoring across everyday life. A dense set of national security laws provides the formal foundation for state control. The *Guarding State Secrets Law*, *Cybersecurity Law*, and *Data Security Law* collectively establish an expansive conception of national security that includes political stability, economic development, and technological self-sufficiency. These statutes authorize broad governmental discretion over data and digital infrastructure, allowing the state to regulate nearly all forms of information and socio-economic activity with minimal procedural safeguards. At the same time, China's surveillance landscape has evolved through policy experimentation often preceding legal authorization. The Social Credit System**,** for instance, began as fragmented local pilots governing social and economic behavior without a comprehensive national legal framework (Chen et al 2018). Subsequent regional regulations—such as those in Ningxia, Hubei, and Shanghai—partially formalized these initiatives, while recent central directives signal efforts toward nationwide codification (Werbach 2022). Similarly, the SkyNet Project, which integrates extensive CCTV and facial-recognition networks developed by firms such as Hikvision, SenseTime, Huawei, and ZTE, has expanded primarily through administrative policy rather than explicit legislative authorization (Qiang 2021).

India's legal framework grants the government broad authority to conduct surveillance through general-purpose statutes rather than dedicated legislation. The *Unlawful Activities (Prevention) Act (UAPA)* permits evidence obtained under the *Indian Telegraph Act* (1885) or the *Information Technology Act* (2000) to be admitted in court, creating a procedural incentive for interception (Horowitz 2023). The *Information Technology Act* further requires intermediaries to cooperate with state requests, effectively institutionalizing public–private censorship and extending colonial-era control over online speech (Anupam & Le 2015). Both laws have been invoked to justify the Central Monitoring System, which enables real-time interception and data access across platforms but lacks an explicit statutory basis (Litton 2015, Reddy 2014). Other initiatives, such as Aadhaar and the Smart Cities Mission—which installed extensive CCTV networks and partnered with private firms to integrate facial recognition (Jain et al 2021)—similarly operate without clear legislative grounding.

Singapore shares with China and India a reliance on broad enabling legislation and policy-led initiatives that authorize extensive surveillance without dedicated statutory mandates. Background laws such as the *Cybersecurity Act*, *Computer Misuse and Cybersecurity Act*, *Public Sector (Governance) Act*, and *Personal Data Protection Act* empower ministers to direct organizations to take "necessary measures" to address threats to national security, public order, or the economy, permit warrantless searches for certain computer-related offenses, and maximize government access to data. Although these statutes contain some procedural guardrails, their open-ended definitions of harm grant the executive wide discretion. This legal framework underpins programs such as the Risk Assessment and Horizon Scanning (RAHS) system, which allows authorities to "predict, model, and monitor" security threats across domains ranging from terrorism and disease to economic and policy risks (Hu 2017). Similarly, the Smart Nation initiative—launched in 2014 and expanded through Smart Nation 2.0, which incorporates extensive surveillance components—began as a policy blueprint without specific statutory authorization. Only later, in 2025, did the government announce plans for a *Digital Infrastructure Act* to enhance the security and resilience of national digital systems.

Although liberal democracies in Asia have not actively pursued expansive new forms of surveillance, recent security and public health concerns have prompted renewed debate over the boundaries of state power and the protection of individual rights. In Japan, strong privacy norms and a cautious legal tradition have long limited surveillance, yet growing anxieties about state-sponsored cyber intrusions and global cybercrime have led to gradual recalibration. The *Active Cyberdefense Law* (2025) authorizes the monitoring and interception of foreign internet traffic and even permits the preemptive disruption of hostile servers. Although nominally restricted to metadata and implemented in cooperation with private operators, the law marks a significant expansion of state power in cyberspace, raising concerns among civil society advocates about potential encroachments on privacy and freedom of expression.[3]

Taiwan and South Korea, both shaped by authoritarian pasts, operate within legal frameworks that explicitly and narrowly authorize surveillance. In Taiwan, the *Communication Security and Surveillance Act* limits interception to defined objectives and requires judicial warrants. A 2022 proposal to expand state oversight through the draft *Digital Intermediary Service Act* was withdrawn after public backlash, underscoring strong civic oversight and public sensitivity to government overreach.[4] South Korea has developed a comprehensive statutory framework that links surveillance to urban innovation. The *Protection of Communications Secrets Act* establishes safeguards for communications privacy, while the *Construction of Ubiquitous Cities Act* (2008), *Establishment and Promotion of Smart Cities Act* (2017), and *Promotion of Smart City Development and Industry Act* (2018) integrate digital infrastructure into city management under explicit legal authorization and well-defined procedural safeguards (Shin et al 2025).

Across these cases, law functions as an enabling infrastructure that confers legitimacy, institutional form, and regulatory capacity on surveillance, embedding it within broader bureaucratic routines and state machinery. Yet the scope of legal authorization varies widely—from expansive, open-ended mandates that empower executive discretion to narrowly circumscribed provisions that delineate the purposes and procedures of surveillance.

Law as Constraining Infrastructure

While law enables surveillance, it also establishes the boundaries within which surveillance may operate. Across Asia, these constraining mechanisms are uneven in scope, institutional strength, and normative orientation. Some democracies have developed robust legal safeguards and oversight, hybrid regimes retain broad administrative discretion, and authoritarian systems codify surveillance as an ordinary function of statecraft.

South Korea, Taiwan, and Japan exemplify rights-based approaches that embed procedural safeguards and institutional oversight within their legal frameworks (Greenleaf 2014). South Korea's *Protection of Communications Secrets Act* (PCSA) requires prior judicial authorization for communications interception, limits the duration of warrants, and excludes unlawfully obtained evidence. Even under national security exceptions, emergency surveillance must be swiftly ratified by a judge, preventing temporary exigencies from becoming permanent. Taiwan's *Communication Security and Surveillance Act* (CSSA) likewise enshrines judicial oversight and the principles of necessity and proportionality, reflecting the country's post-authoritarian commitment to procedural due process. All three democracies have also enacted comprehensive data protection laws—South Korea's *Personal Information Protection Act*

(PIPA), Taiwan's *Personal Data Protection Act* (PDPA), and Japan's *Act on the Protection of Personal Information* (APPI)—that regulate both public and private sectors. These statutes establish independent supervisory commissions, require transparency in data processing, and guarantee individuals the right to access, correct, and delete personal information. Together, they form a rights-based infrastructure in which surveillance is legally permissible only under defined conditions, subject to oversight, and open to judicial review.

India and Singapore, by contrast, represent hybrid regimes that combine formal privacy protections with expansive public-sector exemptions. Both countries have adopted comprehensive data protection legislation—Singapore's *Personal Data Protection Act* (PDPA) and India's *Digital Personal Data Protection Act* (DPDPA)—yet these laws preserve sweeping state discretion in the name of administrative efficiency and security. In Singapore, the *PDPA* explicitly excludes government agencies, while the *Public Sector (Governance) Act* authorizes inter-agency data sharing even when confidentiality provisions would otherwise apply (Wee & Findlay 2020). India's *DPDPA* adopts a comparable logic, granting blanket exemptions for public authorities processing personal data for broadly defined purposes such as sovereignty, national security, and public order. Both frameworks institutionalize a tension between the rhetoric of privacy and the practice of governance: law appears to protect data subjects while simultaneously insulating the state from meaningful accountability. Legal oversight exists largely at the discretion of the executive, and enforcement bodies have limited power to scrutinize state surveillance. In these hybrid systems, law functions less as a constraint than as a managerial instrument, justifying pervasive data collection as necessary for effective governance and development.

China stands apart in its authoritarian-legalist approach, where law itself serves to entrench and legitimize state surveillance. The *Personal Information Protection Law* (PIPL), along with the *Cybersecurity Law and Data Security Law*, establishes stringent obligations for private companies but grants public authorities broad and vaguely defined powers to collect, process, and analyze data in the "public interest" or for "national security" (Werbach 2022). Articles 13 and 18 of the PIPL permit state data use without consent and exempt government agencies from notification requirements. Complementary measures, such as the 2024 *Measures for the Security Management of the Application of Facial Recognition Technology* and the 2021 Supreme People's Court interpretation on facial recognition, nominally regulate misuse yet maintain wide exceptions for public security and state interests. These provisions create a dual structure: strict compliance for private actors and expansive discretion for state organs. In China, law functions less as a restraint on state power than as an instrument of legitimation, codifying surveillance as a lawful and institutionalized element of governance and social control.

The Judiciary as a Forum of Contestation

Gaps in statutory safeguards often leave courts as supplementary—yet sometimes decisive—sites of constraint. Across Asia, the judiciary has become a key arena where citizens and civil society actors contest the boundaries of state and corporate surveillance. Yet, as the cases below illustrate, the depth and effectiveness of judicial engagement remain uneven.

Taiwan has one of the most active constitutional jurisdictions in the region on issues of privacy and surveillance. The 2005 Constitutional Court ruling striking down compulsory fingerprinting for national ID cards marked an early assertion of judicial oversight over surveillance. In 2022, the Court addressed the secondary use of personal health data in the National Health Insurance Research Database, finding that the *National Health Insurance Act* lacked explicit authorization and sufficient safeguards. Reaffirming that privacy rights under Article 22 of the Constitution include control over personal information, the Court ordered the legislature to establish a clear statutory basis and an independent supervisory authority. The decision reshaped the governance of health data and articulated a constitutional framework for regulating data-driven administration (Huang 2023).

India's judiciary has played a pivotal but ambivalent role in defining privacy and surveillance. In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognized privacy as a constitutionally protected right under Article 21 of the Indian Constitution, which guarantees protection of life and personal liberty, overturning earlier precedent (Bhandari & Sane 2019). The case arose from challenges to the government's *Aadhaar* program, a centralized biometric database initially intended for welfare delivery but later expanded to financial, tax, and telecommunications uses without adequate safeguards (Guruswamy 2017). The Court upheld the *Aadhaar Act* (2016) but struck down mandatory linkages to private services, emphasizing proportionality and purpose limitation, and urged the enactment of a comprehensive data protection law. While affirming privacy as a fundamental right, the judgment also legitimized extensive state data collection, reflecting the judiciary's dual role as both guardian and enabler of India's surveillance infrastructure (Bhandari & Sane 2019).

China presents a different picture. Judicial challenges to state surveillance are rare, as courts remain subordinate to the executive. However, emerging cases on the private misuse of biometric data show nascent judicial engagement with data rights. In 2019, law professor Guo Bing successfully sued Hangzhou Safari Park over mandatory facial recognition, with the court ruling that biometric collection must be lawful, necessary, and proportionate (Luo & Guo 2021). The case spurred legal reforms, strengthening personal information protections in China's *Civil Code* (Chen & Wang 2023). In 2021, an appellate court held that residents could withdraw consent for facial recognition under Article 15 of the *PIPL*, citing the *Supreme People's Court's Provisions on the Use of Facial Recognition Technology in Civil Cases* (Chen & Wang 2023). Although such rulings remain confined to the private sector, they signal a gradual incorporation of privacy norms into China's legal reasoning.

VARIETIES OF SURVEILLANCE AND STATE–SOCIETY RELATIONS

Surveillance in Asia is co-produced through the interaction of law, technology, and state–society relations. These elements combine in varying ways, producing distinct configurations of surveillance best understood not as fixed categories but as positions along a spectrum of techno-legal co-production. This spectrum is defined by the degree of *alignment* or *contestation* between law and technology: at one end lies techno-legal synergy, where law and technology reinforce each other to strengthen surveillance; at the other, rights-bounded contestation, where legal institutions and civic actors constrain its reach. Between them are partial alignments, where

legality and technology intersect to consolidate surveillance capacity while leaving limited room for oversight and public scrutiny.

At the synergistic end of the spectrum stands China, where law and technology operate in concert under an authoritarian state, powerful technology firms aligned with state priorities, and a civil society offering limited resistance to surveillance. Legal and policy frameworks codify an expansive notion of national security, granting the state broad discretion while imposing strict compliance obligations on private firms, effectively enlisting them as extensions of the state's monitoring apparatus. Technology, in turn, materializes legal authority. The result is an authoritarian synergy in which law and technology co-produce control—law rationalizes, technology operationalizes—sustained by corporate dependence on state favor and a political environment that constrains civic oversight (Lei 2023).

At the middle are India and Singapore, where law and technology are partially aligned to strengthen surveillance. Legal frameworks invoke the language of privacy, accountability, and modernization while preserving broad state discretion in the name of efficiency, development, and security. In India, surveillance is justified through developmental governance: the *Digital Personal Data Protection Act and the Information Technology Act* coexist with expansive interception powers and weak oversight, enabling large-scale data integration through systems such as Aadhaar. Courts have affirmed privacy as a constitutional right yet largely upheld these infrastructures. Singapore follows a similar but more technocratic model. Broad statutes grant wide ministerial discretion and inter-agency data sharing, while the *Personal Data Protection Act* excludes government agencies. Programs such as Smart Nation and Risk Assessment and Horizon Scanning embed surveillance in everyday governance, framed as rational and forward-looking administration. Civil-society pushback, as in the TraceTogether controversy, has prompted modest legal adjustments but not structural constraint.

At the opposite end of the spectrum lies rights-bounded contestation, exemplified by Japan, South Korea, and Taiwan, where law and technology interact in a contested yet mutually shaping relationship. In these democracies, constitutional safeguards, judicial oversight, and civic activism constrain technological expansion. Japan maintains strong privacy norms and a cautious legal tradition, though cybersecurity concerns have prompted incremental extensions of surveillance, as seen in the *Active Cyberdefense Law* (2025). South Korea's *Protection of Communications Secrets Act* and Smart City statutes enable digital governance while requiring judicial warrants, proportionality, and transparency, amid active civic debates over privacy and data exposure. Taiwan's surveillance regime reflects post-authoritarian restraint: the *Communication Security and Surveillance Act* mandates judicial authorization, and Constitutional Court rulings have affirmed informational self-determination as a fundamental right. Public backlash has repeatedly forced the state to retreat from overreach. Across these democracies, surveillance remains legally permissible but continuously negotiated through judicial review, public deliberation, and civic oversight.

CONCLUSION

This review argues that surveillance in Asia is best understood as the co-production of law, technology, and state–society relations. Examining China, India, Singapore, Japan, South Korea,

and Taiwan along a spectrum of techno-legal co-production explains why distinct surveillance regimes have emerged within a shared context of technological intensification. Across these cases, the configurations linking the state, business actors, and civil society (Wolf 2008) illuminate not only how surveillance expands but also when and how it is disciplined. While much of the social science literature emphasizes technology and state or corporate power, this framework highlights the need to consider a wider range of actors and how legal institutions simultaneously enable and constrain surveillance across political and institutional contexts. In particular, civil actors and judicial institutions in Japan, South Korea, and Taiwan have been central to disciplining technological expansion through constitutional litigation, public backlash, and regulatory oversight that have curbed overreach and reshaped the legal frameworks governing surveillance.

Future research should extend this spectrum beyond the six core cases. Across Southeast and South Asia, countries such as Thailand, Indonesia, and Malaysia are experimenting with digital governance models that blend democratic and authoritarian features. Thailand's pilot crime databases and digital platforms remain fragmented and dependent on imported technologies (Mangkhalasiri & Poothakool 2025). Like India, Indonesia is moving toward a biometric digital welfare state by linking its national ID system to social assistance programs. Biometric registration is promoted to reduce fraud and duplication, and digital ID is increasingly required to access government subsidies. While these measures promise efficiency, they risk excluding citizens without reliable identification or digital access. A broader comparative inquiry into these cases can clarify how institutional contexts and state–society relations shape the co-production of law, technology, and surveillance.

Attention should also turn to the transnational dimensions of surveillance in Asia. Surveillance regimes are increasingly shaped by global flows of law, technology, and activism. The diffusion of legal norms—such as the European Union's General Data Protection Regulation (GDPR) and Digital Services Act (DSA)—has influenced reforms in Japan and South Korea. At the same time, regional initiatives promote inter-Asian legal learning, including the Association of Southeast Asian Nations (ASEAN) draft cross-border privacy rules, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) data-flow provisions (Erie & Lin 2025).

Yet these exchanges are not one-way diffusions of "Western" models. Asian jurisdictions increasingly reinterpret, hybridize, and project their own governance templates outward. Singapore's "Smart Nation" framework and Japan's data-governance standards are quietly shaping global debates on digital governance, cybersecurity, and AI regulation, challenging the view of Asia as a regulatory "follower" and underscoring its emerging role as a producer of global surveillance norms.

The geopolitical circulation of technology is equally significant. China's Digital Silk Road exports surveillance infrastructures through firms such as Huawei and Hikvision, seen in Thailand's reliance on imported technologies (Mangkhalasiri & Poothakool 2025) and Huawei-led Safe City projects in Kuala Lumpur and Dhaka (Feldstein 2021).[5] Finally, transnational networks of resistance and accountability—from regional digital rights coalitions to global

frameworks like the United Nations Guiding Principles on Business and Human Rights—are also beginning to challenge surveillance practices and corporate complicity across borders.

Taken together, these legal, technological, and civic flows underscore that the governance of surveillance in Asia is not only embedded in but also increasingly constitutive of transnational circuits of power, technology, regulation, and resistance. Understanding surveillance in Asia therefore requires moving beyond nationally bounded frameworks to account for these intersecting and evolving global dynamics.

[1] https://blogs.lse.ac.uk/humanrights/2021/04/16/predictive-policing-in-india-deterring-crime-or-discriminating-minorities/, retrieved October 17, 2025.

[2] A Jan Dhan account is a basic savings bank account opened for unbanked individuals under the Pradhan Mantri Jan Dhan Yojana. These accounts require no minimum balance.

[3] https://www.csis.org/analysis/norms-new-technological-domains-whats-next-japan-and-united-states-cyberspace#h2-legislative-shift-japan-s-active-cyber-defense-bill, retrieved October 17, 2025.

[4] https://www.ncc.gov.tw/english/files/24011/382_5865_240111_1.pdf; https://freedomhouse.org/country/taiwan/freedom-net/2022; https://jsis.washington.edu/nie/wp-content/uploads/2022/10/23_TF-JSIS_495D_Beyer_Final.pdf, retrieved October 17, 2025.

[5] https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en, retrieved October 17, 2025.

LITERATURE CITED

Anupam C, Le UP. 2015. Data nationalism. *Emory Law Journal* 64:677–739

Balkin JM. 2008. The constitution in the national surveillance state. *Minnesota Law Review* 93:1–26

Ball K, Haggerty K, Lyon D. 2012. Introducing surveillance studies. In *Routledge Handbook of Surveillance Studies*, eds. D Lyon, K Ball, K Haggerty, pp. 1–15. New York: Routledge

Basheer IP. 2025. Bias in the algorithm: Issues raised due to use of facial recognition in India. *J. Dev. Policy Pract.* 10:61–79

Bernot A. 2022. Transnational state–corporate symbiosis of public security: China's exports of surveillance technologies. *Int. J. Crime Justice Soc. Democr.* 11:159–73

Bhandari V, Sane R. 2019. A critique of the Aadhaar legal framework. *Natl. Law Sch. India Rev.* 31:72–97

Brown CL. 2008. China's second-generation national identity card: merging culture, industry, and technology. In *Playing the Identity Card*, ed. C Bennett, D Lyon, pp. 57–74. New York: Routledge

Chen W, Wang M. 2023. Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommun. Policy* 47:1–11

Chen Y-J, Lin C-F, Liu H-W. 2018. Rule of trust: The power and perils of China's social credit megaproject. *Colum. J. Asian Law* 32:1–36

Cong W. 2021. From pandemic control to data-driven governance: the case of China's health code. *Front. Polit. Sci.* 3:1–15

Das D, Zhang JJ. 2021. Pandemic in a smart city: Singapore's COVID-19 management through technology & society. *Urban Geogr.* 42:408–16

Deguchi A. 2020. From smart city to Society 5.0. In *Society 5.0: A People-Centric Super-Smart Society*, ed. Hitachi-UTokyo Laboratory, pp. 43–65. Singapore: Springer

Erie MS, Lin C-F. 2025. Introduction: The emergence of Inter-Asian law. In *Inter-Asian Law*, ed. MS Erie, C-F Lin, pp. 1–24. Cambridge: Cambridge Univ. Press

Eubanks V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* New York: St. Martin's Press

Feldstein S. 2021. *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance.* Oxford: Oxford Univ. Press

Garg S, Bhatnagar N, Gangadharan N. 2020. A case for participatory disease surveillance of the COVID-19 pandemic in India. *JMIR Public Health Surveill.* 6:1–5

Greenleaf G. 2014. *Asian Data Privacy Laws: Trade and Human Rights Perspectives.* Oxford: Oxford Univ. Press

Guruswamy M. 2017. Justice KS Puttaswamy (Ret'd) and Anr v. Union of India and Ors. *Am. J. Int. Law* 111:994–1000

Henne K. 2019. Surveillance in the name of governance: Aadhaar as a fix for leaking systems in India. In *Information, Technology and Control in a Changing World*, ed. B Haggart, K Henne, N Tusikov, pp. 223–45. Cham: Springer

Horowitz SI. 2023. A right to privacy under mass surveillance? *Hous. J. Int. Law* 46:331–45

Hou R, Fu D. 2024. Sorting citizens: governing via China's social credit system. *Governance* 37:59–78

Hu M. 2017. Horizontal cybersurveillance through sentiment analysis. *Wm. & Mary Bill Rights J.* 26:361–82

Huang J, Tsai KS. 2022. Securing authoritarian capitalism in the digital age: the political economy of surveillance in China. *China J.* 88:2–28

Huang Y-C. 2023. Applying privacy as trust in the emerging digital welfare state. *Natl. Taiwan Univ. Law Rev.* 18:97–124

Hung T-W, Yen C-P. 2021. On the person-based predictive policing of AI. *Ethics Inf. Technol.* 23:165–76

Ichihara M. 2020. Corona-tracking and privacy: the opposite approaches of South Korea and Japan. *Asian Democracy Issue Briefing*, pp. 1–5. http://adrnresearch.org/publications/list.php?cid=1&sp=%26sp%5B%5D%3D1%26sp%5B%5D%3D2%26sp%5B%5D%3D3&pn=1&st=&code=&at=view&idx=89

Jain R, Nagrath P, Thakur N, Saini D, Sharma N, Hemanth DJ. 2021. Towards a smarter surveillance solution: The convergence of smart city and energy-efficient unmanned aerial vehicle technologies. In *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, pp. 109–40. Cham: Springer

Jasanoff S. 2004. *States of Knowledge: The Co-Production of Science and the Social Order.* New York: Routledge

Ji T, Chen J-H, Wei H-H, Su Y-C. 2021. Towards people-centric smart city development: investigating citizens' preferences and perceptions about smart-city services in Taiwan. *Sustainable Cities and Society* 67:102691. https://doi.org/10.1016/j.scs.2020.102691

Johns F. 2021. Governance by data. *Annu. Rev. Law Soc. Sci.* 17:53–71

Juneja S, Singh S, Gupta S, Gupta R, Ray S, et al. 2021. "Aarogya Setu": India's COVID-19 contact-tracing mobile application. *Int. J. Community Med. Public Health* 8:1802–08

Krishnakumar T. 2021. Missed connections? Evaluating the global spread and legality of mandatory SIM registration in a modern national security context. *Denver J. Int. Law Policy* 49:57–94

Kuo Y-H, Chen P-L. 2016. Identity laws and privacy protection in a modern state: the legal history concerning personal information in Taiwan (1895–2015). *Wash. Int. Law J.* 25:223–26

Lee H, Kim E, Park DH. 2025. Insights from the Incheon Airport case in South Korea: balancing public safety and individual rights with global scalability analysis. *Humanit. Soc. Sci. Commun.* 12:1104

Lee HHH, Lee T. 2022. The TraceTogether matrix has you: surveillance, rationalisation and tactics of governance in Singapore's COVID-19 app. *Platform: J. Media Commun.* 9:77–91

Lee J-A, Liu C-Y. 2016. Real-name registration rules and the fading digital anonymity in China. *Wash. Int. Law J.* 25:1–35

Lei Y-W. 2023. *The Gilded Cage: Technology, Development, and State Capitalism in China.* Princeton, NJ: Princeton Univ. Press

Lei Y-W, Kim R. 2024. Automation and augmentation: artificial intelligence, robots, and work. *Annu. Rev. Sociol.* 50:251–72

Leu J-H, Lin B-C, Liao Y-Y, Gan D-Y. 2021. Smart city development in Taiwan. *IET Smart Cities* 3:125–41

Liang F. 2020. COVID-19 and health code: how digital platforms tackle the pandemic in China. *Social Media + Society* 6(3):1–4. https://doi.org/10.1177/2056305120947657

Liang F, Chen Y. 2022. The making of "good" citizens: China's social credit systems and infrastructures of social quantification. *Policy Internet* 14:114–35

Liang F, Das V, Kostyuk N, Hussain MM. 2018. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy Internet* 10:415–53

Lin C-F, Wu C-H, Wu C-F. 2020. Reimagining the administrative state in times of global health crisis: an anatomy of Taiwan's regulatory actions in response to the COVID-19 pandemic. *Eur. J. Risk Regul.* 11:256–72

Litton A. 2015. The state of surveillance in India: the Central Monitoring System's chilling effect on self-expression. *Wash. Univ. Global Stud. Law Rev.* 14:799–822

Liu C. 2019. Multiple social credit systems in China. *Econ. Sociol.* 21:22–32

Liu C. 2022. Seeing like a state, enacting like an algorithm: (Re)assembling contact tracing and risk assessment during the COVID-19 pandemic. *Sci. Technol. Hum. Values* 47:698–725

Liu C. Forthcoming. *Metricocracy: The Data and Bureaucratic Politics of a Chinese Social Credit Score System.*

Luo Y, Guo R. 2021. Facial recognition in China: current status, comparative approach, and the road ahead. *Univ. Pa. J. Law Soc. Change* 25:153–79

Lyon D. 2003. Surveillance technology and surveillance. In *Modernity and Technology*, ed. A Feenberg, P Brey, TJ Misa, pp. 161–83. Cambridge, MA: MIT Press

Mangkhalasiri P, Poothakool K. 2025. Data science in policing in Thailand: challenges and future directions. *J. Contemp. Soc. Sci. Humanit.* 12:18–34

Marda V, Narayan S. 2020. Data in New Delhi's predictive policing system. In *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, pp. 317–24. New York: ACM. https://doi.org/10.1145/3351095.3372865

Marvin S, While A, Chen B, Kovacic M. 2022. Urban AI in China: social control or hyper-capitalist development in the post-smart city? *Front. Sustain. Cities* 4:1–11

Marx GT. 2015. Surveillance studies. In *International Encyclopedia of the Social and Behavioral Sciences*, ed. JD Wright, pp. 733–41. Waltham, MA: Elsevier

Matsui S. 2019. Is "My Number" really my number?: national identification numbers and the right to privacy in Japan. *Syracuse J. Int. Law Commerce* 47:99–137

Moon H, Choi H, Lee J, Lee KS. 2017. Attitudes in Korea toward introducing smart policing technologies: differences between the general public and police officers. *Sustainability* 9:1921

Murakami Wood D, Lyon D, Abe K. 2007. Surveillance in urban Japan: a critical introduction. *Urban Stud.* 44:551–68

Nakajima I, Tsuji M. 2022. Issues on Japanese COVID-19 exposure notifications application (COCOA). In *Proceedings of the 4th International Conference on Computer Communication and the Internet (ICCCI)*, pp. 179–84. IEEE

Ozaki A. 2020. Governance framework for facial recognition systems in Japan. In *Human-Centric Computing in a Data-Driven Society*, ed. D Kreps, T Komukai, TV Gopal, K Ishii, pp. 52–63. Cham: Springer

Pei M. 2024. *The Sentinel State: Surveillance and the Survival of Dictatorship in China.* Cambridge, MA: Harvard Univ. Press

Qiang S. 2025. Intelligent social welfare: how AI optimizes social assistance, elderly care, and healthcare systems. *Digit. Soc. Virtual Gov.* 1:17–32

Qiang X. 2021. Chinese digital authoritarianism and its global impact. *Proj. Middle East Political Sci.* 43:35–40

Rao U, Nair V. 2019. Aadhaar: governing with biometrics. *South Asia: J. South Asian Stud.* 42:469–81

Reddy J. 2014. The Central Monitoring System and privacy: analysing what we know so far. *Indian J. Law Technol.* 10:41–62

Ryu H, Lim H. 2023. Linking smart city and urban sustainability issues: a comparative study of smart city services in Japan and Korea. *Urban Reg. Plan. Rev.* 10:263–93

Shaw R, Kim Y-K, Hua J. 2020. Governance, technology, and citizen behavior in pandemic: lessons from COVID-19 in East Asia. *Prog. Disaster Sci.* 6:1–11

Shin S-Y, Lee A, Chung C-S. 2025. Blueprints for tomorrow's smart cities in South Korea: conceptual definition and timeline forecast from a policy Delphi study. *Journal of Policy Studies* 40(3):43–69

Sonn JW, Lee JK. 2020. The smart city as time-space cartographer in COVID-19 control: the South Korean strategy and democratic control of surveillance technology. *Eurasian Geogr. Econ.* 61:482–92

Sprick D. 2019. Predictive policing in China: an authoritarian dream of public security. *NAVEIÑ REET: Nord. J. Law Soc. Res.* 1:299–364

Stevens H, Haines MB. 2020. TraceTogether: pandemic response, democracy, and technology. *East Asian Sci. Technol. Soc.* 14:523–32

Tang B. 2020. Grid governance in China's urban middle-class neighbourhoods. *China Q.* 241:43–61

Van Toorn G, Henman P, Soldatić K. 2024. Introduction to the digital welfare state: contestations, considerations, and entanglements. *J. Sociol.* 60:507–22

Wee A, Findlay M. 2020. AI and data use: surveillance technology and community disquiet in the age of COVID-19. *SMU Centre for AI & Data Governance Research Paper No. 2020/10.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715993

Weller T. 2012. The information state: an historical perspective on surveillance. In *Routledge Handbook of Surveillance Studies*, ed. K Ball, K Haggerty, D Lyon, pp. 57–63. New York: Routledge

Werbach K. 2022. Orwell that ends well? Social credit as regulation for the algorithmic age. *Univ. Ill. Law Rev.* 4:1417–75

Woods O, Lim A, Kong L. 2025. Sedimented surveillance in Southeast Asia's "smart" city-state: the case of Singapore. In *Handbook on Cities and Crime*, eds. D Oberwittler, R Wickes, pp. 468–82. Cheltenham: Edward Elgar

Xu X, Kostka G, Cao X. 2022. Information control and public support for social credit systems in China. *J. Polit.* 84:2230–45

Yang C. 2022. Digital contact tracing in the pandemic cities: problematizing the regime of traceability in South Korea. *Big Data & Soc.* 9:1–13

Yang F, Heemsbergen L, Fordyce R. 2021. Comparative analysis of China's Health Code, Australia's COVIDSafe, and New Zealand's COVID Tracer surveillance apps. *Media Int. Aust.* 178:182–97

Yeo SJI. 2023. Smart urban living in Singapore? Thinking through everyday geographies. *Urban Geogr.* 44:687–706

Yu H. 2022. Living in the era of codes: a reflection on China's health code system. *BioSocieties* 19: 1–18

Yuan EJ. 2021. Governing risk society: the socio-technological experiences of China and South Korea in the COVID-19 pandemic. *Asian J. Commun.* 31:322–36

Zajko M. 2023. Automated government benefits and welfare surveillance. *Surveill. Soc.* 21:246–58

Zuboff S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs