Journal of Chinese Political Science
https://doi.org/10.1007/s11366-025-09918-5

RESEARCH ARTICLE

When Does Surveillance Trigger Resistance? Public Response to Escalating Digital Control in China

Dakeng Chen[1] · Jing Vivian Zhan[1]

Accepted: 13 May 2025

Abstract

Digital technologies have revolutionized authoritarian states' capacity for social control through mass surveillance. However, how citizens perceive and react to escalating digital control remains understudied. This research proposes a risk-benefit analytical framework to explain how awareness of state control intentions shapes public reactions to digital surveillance in conjunction with surveillance intrusiveness. Using two independent survey experiments with over 2000 respondents, we examine the public acceptance of four digital control measures with increasing intrusiveness: CCTV cameras in public areas, CCTV cameras in residential communities, smartphone location tracking, and smartphone usage monitoring. We find that awareness of the state's mass monitoring and targeted repression intentions significantly decreases public support, especially for more intrusive measures. Our findings suggest that while digital innovations expand authoritarian states' surveillance capabilities, technological overreach may backfire by evoking public resistance.

Keywords China · Digital surveillance · Intrusiveness · Public opinion · State control

Introduction

Digital technologies have fundamentally transformed authoritarian governance, with China leading the global deployment of sophisticated surveillance systems [37, 48, 72]. From ubiquitous CCTV cameras to advanced smartphone tracking, the Chinese government has leveraged information and communication technology (ICT) to bolster its monitoring capabilities and suppress potential threats to regime stability [16,

✉ Jing Vivian Zhan
zhan@cuhk.edu.hk

Dakeng Chen
chendakeng@link.cuhk.edu.hk

[1] School of Governance and Policy Science, the Chinese University of Hong Kong, Shatin, New Territories, Hong Kong, SAR, China

Published online: 10 June 2025

35, 76]. This digital transformation of authoritarian control reached new heights during the COVID-19 pandemic, as the state deployed unprecedented levels of surveillance in the name of public health [27, 75].

However, the effectiveness of digital control hinges on public acceptance and cooperation [17, 33, 74]. This raises a critical yet unaddressed question: *how do citizens perceive and respond to escalating digital control?* Existing scholarship offers mixed answers. While conventional wisdom holds that state repression breeds resentment and resistance [2, 7, 8], more recent studies find that citizens may well support state repression [32, 81]. In the Chinese context, where digital tools have been increasingly deployed to surveil citizens, studies have found wide public support for the state's use of digital surveillance [38, 61].

To address this puzzle, we propose a risk-benefit framework that explains public responses to authoritarian digital control through the interplay of perceived risks and benefits. Focusing on the perceived risks, we argue that citizens' risk assessments are shaped by their awareness of state control intentions, including mass monitoring and targeted repression, which allow the state to weaponize collected information for political control. While authoritarian regimes justify escalating digital surveillance through benefits such as public safety and pandemic control, citizens who recognize these technologies as instruments of political control are more likely to perceive heightened threats to personal freedom and security. Specifically, when realizing surveillance's mass monitoring function, citizens become aware that their personal information is being systematically collected; when realizing surveillance' targeted repression function, citizens are alerted to how the state can utilize the collected information against individual citizens. This risk assessment is further intensified by the technological intrusiveness of surveillance tools. As surveillance penetrates deeper into private spheres to collect increasing volume and granularity of personal information and enable more precise state control, it drives up citizens' perceived risks. When perceived risks outweigh benefits, public acceptance of surveillance transforms into opposition.

This risk-benefit framework reconciles seemingly contradictory findings in existing literature: Citizens may embrace certain surveillance measures when benefits seem to dominate, while rejecting others when risks become more salient. The key lies not in whether citizens categorically accept or reject surveillance, but in how they evaluate the balance of risks and benefits across different contexts and technologies.

We test our theoretical framework through two independent online survey experiments in China, each with over 1000 respondents drawn from distinct pools of internet users. Our experimental design probes the core elements of risk-benefit calculations through random assignment to one control and three treatment groups. While all groups received information about surveillance benefits, treatment groups were exposed to varying information about state control intentions behind digital surveillance: 1) mass monitoring of citizens, 2) targeted repression of dissidents, and 3) both mass monitoring and targeted repression simultaneously. This manipulation allows us to examine how awareness of these state control intentions influences public acceptance of surveillance. All participants then evaluated their support for four increasingly intrusive digital control measures prevalent in China: 1) CCTV cameras in public areas, 2) CCTV cameras in residential communities, 3) smartphone location tracking, and 4) smartphone usage monitoring. This graduated scale of surveillance intrusiveness enables us to identify variations in public acceptance of different surveillance measures, especially in conjunction with citizens' awareness of state control intentions.

Our findings strongly support the risk-benefit framework, revealing how awareness of state control intentions shapes public acceptance of digital control along with varying degrees of technological intrusiveness. Awareness of both mass monitoring and targeted repression intentions significantly erodes acceptance across all surveillance measures, with stronger effects for more intrusive technologies. This pattern demonstrates how heightened risk perception, driven by awareness of state control intentions, can override perceived benefits and trigger resistance, especially to more intrusive surveillance measures. In general, citizens largely accept both public and residential area surveillance cameras, but support plummets when monitoring extends to smartphones. This sharp decline indicates a critical threshold between static, undifferentiating surveillance and individualized surveillance that is omnipresent and hard to evade.

This research contributes to the growing literature on digital authoritarianism in three ways. First, it proposes a risk-benefit analytical framework to reconcile citizens' seemingly contradictory attitudes toward digital control in previous studies. We show how awareness of state control intentions shapes perceived risks and reveal the boundaries of public tolerance for digital control in authoritarian contexts. Second, by disaggregating and comparatively examining a spectrum of digital control measures, we draw attention to the distinction among different surveillance technologies and divergent societal reactions. The findings challenge monolithic interpretations of digital surveillance and highlight a resistance threshold between public cameras and intimate smartphone monitoring. Finally, our results expose a central paradox of digital authoritarianism: As regimes deploy increasingly intrusive surveillance to strengthen control, they risk triggering public resistance that may ultimately undermine regime stability. This insight enriches debates about authoritarian resilience in the digital age by showing that technological overreach could backfire.

The paper proceeds as follows: Section Two reviews the existing literature and develops our analytical framework and hypotheses regarding public acceptance of digital control. Section Three examines the escalation of digital control in China and illustrates state access to surveillance data facilitated by state-corporate collaboration and supported by legal frameworks and institutional arrangements. Sections Four and Five present the experimental design and empirical findings, respectively. Section Six offers additional support through robustness checks. The final section concludes.

Public Response to Digital Surveillance: Theoretical Analysis

Digital surveillance technologies have fundamentally transformed the relationship between the state and the citizenry. While earlier scholarship centered on privacy-security tradeoffs when explaining public attitudes toward digital surveillance in democratic contexts [9, 49], the unprecedented reach of digital surveillance in authoritarian regimes has created a qualitatively different reality. The increasing intrusion of digital control into citizens' private lives raises critical questions: Under what conditions do citizens acquiesce to or resist digital surveillance? Where lies the threshold between public acceptance and opposition? These questions are not merely theoretical; they cut to the heart of regime stability and state-society relations in contemporary authoritarian regimes.

Existing literature on public attitudes toward surveillance has developed primarily in democratic contexts, where privacy-security tradeoffs dominate the theoretical discussion. Studies find that citizens evaluate surveillance by weighing perceived benefits such as public safety and crime reduction [1, 63] against risks of privacy loss and fears of data misuse [13, 71]. The acceptance typically declines for more intrusive technologies that collect sensitive personal data [10, 25], with online surveillance and biometric data collection viewed as more concerning than traditional CCTV monitoring [18].

China, as an authoritarian regime, presents an intriguing case. Although living under the world's most extensive surveillance systems [5], Chinese citizens are found to widely support the state's surveillance practices, ranging from CCTV cameras [61], to facial recognition technology [29] and the social credit system [26]. The support appears particularly strong when surveillance is justified by public benefits like security enhancement [28] and pandemic control [27], and when citizens trust the benevolence of implementing institutions [80]. Yet, this support shows important signs of conditionality - when citizens learn about surveillance systems' punitive potential, their approval declines significantly [77].

The existing studies suggest that citizens' attitudes toward digital surveillance in both democratic and authoritarian contexts hinge on the perceived benefits and risks, but the risk calculations may differ fundamentally in different political settings. Compared with democracies, authoritarian states tend to have stronger incentives to collect information about citizens for control purposes [16]. When states deliberately deploy surveillance technologies for political control and repression, citizens must evaluate more complicated political risks and personal consequences that go beyond privacy concerns [53]. Moreover, as surveillance penetrates private spheres, it creates mechanisms for precise political control through the weaponization of intimate personal data [11]. These distinctive features necessitate a more nuanced understanding of citizens' risk calculations that underpin their attitudes toward digital surveillance in authoritarian settings.

To address this gap, we propose a risk-benefit analytical framework to explain citizens' attitudes toward digital surveillance in authoritarian contexts. While authoritarian regimes often justify escalating digital surveillance with such benefits as public safety and pandemic control [6, 63], we argue that citizens' acceptance hinges on their perceived political risks – namely, how the state may exploit collected information for control purposes. Central to the risk assessment is citizens' awareness of state control intentions, including mass monitoring and targeted repression.

Specifically, mass monitoring involves broad data collection and analysis that enable comprehensive state oversight of the population [55, 70]. This creates an Orwellian sense of being watched, imposing psychosocial pressure that prompts citizens to self-regulate their behaviors in conformity with the regime's rules [40]. For example, awareness of online surveillance can generate a chilling effect, leading individuals to self-censor their expressions [50, 59]. Such pressure can evoke aversion and resistance to digital surveillance, especially more intrusive measures that collect increasingly granular data.

Meanwhile, targeted repression involves the state's concrete actions to weaponize collected information against specific individuals or groups [16, 76]. It generates tangible and relatable threats to individual citizens [11, 46], thereby undermining their support for digital surveillance, especially more intrusive measures that enable more precise targeting. Whereas the threat of mass monitoring stems from pervasive surveillance of all citizens, targeted repression presents personalized threats of state coercion against individuals. Recognizing these distinct control mechanisms significantly heightens citizens' risk perceptions of digital surveillance.

The risk calculus is further amplified by technological intrusiveness. As surveillance penetrates deeper into private spheres, increasing volume and granularity of personal information can be collected for state use. In authoritarian contexts, more intrusive surveillance enables greater state control [11] and more precise targeting of dissidents [51]. This transformation of personal data into potential political weapons can drive up citizens' perceived political risks. Taking smartphone surveillance as an example, location tracking, although facilitating pandemic control during the COVID-19 pandemic [75], can be used to track petitioners and prevent them from traveling across administrative regions, demonstrating how granular personal data enables targeted repression [44]. The escalation of digital control with growingly intrusive data collection thus creates a more severe threat to personal security.

The analysis above suggests that citizens' acceptance of surveillance can be shaped by their awareness of how the state utilizes collected information for control purposes, with technological intrusiveness serving as an amplifying factor. The interaction between state control intentions and technological intrusiveness shapes what we call the "resistance threshold," a critical point at which the perceived risks outweigh perceived benefits, transforming public acceptance into resistance. Based on this analytical framework, we propose the following hypotheses and test them in the empirical sections:

Hypothesis 1: *Awareness of state intentions of mass monitoring and targeted repression will decrease public acceptance of digital surveillance, with greater declines for more intrusive measures.*

Hypothesis 2: *Public acceptance of digital surveillance will decrease as technological intrusiveness increases.*

Escalating Digital Control and State Data Collection in China

China's digital control capabilities have evolved dramatically over the past two decades [22, 36], demonstrating a clear progression towards increasingly intrusive surveillance technologies that provide more granular data about citizens' lives. In the early 2000 s, China's digital control focused primarily on monitoring public spaces through CCTV camera networks and ID tracking systems under the "Golden Shield

Project" [56, 67]. These surveillance systems allowed authorities to monitor activities in public areas like transport hubs and internet cafes via cameras and ID scanners [56]. By the late 2000 s, these CCTV networks had proliferated to provide comprehensive coverage of urban communities [34]. While advanced technologies like facial recognition and AI-powered alert systems were integrated, enabling authorities to identify and track specific individuals of interest, CCTV surveillance was still largely restricted to open spaces [45].

The widespread use of smartphones in the mid-2010s marked a pivotal escalation in digital surveillance [39]. Unlike CCTV cameras, smartphones are not devices stationed in fixed locations but are intimately intertwined with individuals' everyday lives and are ever-present. They enabled far more intrusive digital control measures [69]. Authorities began employing location tracking via GPS and cellular data to continuously monitor citizens' movements and map their social connections [46]. Additionally, smartphone usage data like calls, messages, social media, and browsing histories were harvested to construct detailed digital profiles of personal behaviors [44]. These practices represented a profound intrusion into personal lives and private domains, allowing unprecedented state visibility into citizens' daily activities and social networks for control intentions.

More recently, the COVID-19 pandemic catalyzed the rapid escalation of digital control through the implementation of invasive health code systems. Leveraging 5G networks of state-owned telecommunications enterprises and e-governance platforms by tech giants such as Tencent and Alibaba, these apps enabled real-time location tracking and monitoring of citizens' behaviors [75]. By categorizing people's virus exposure risk, the system facilitated stringent control over citizen mobility and social interactions in unprecedented ways [44, 58].

The state collection of personal data was facilitated by state-corporate collaborations [3, 4]. While much of this data collection is executed by corporate platforms, China's political system and legal framework enable comprehensive state access to and sharing of the collected information [22, 70]. State-owned telecommunications enterprises like China Mobile, China Unicom, and China Telecom provide direct access to call records, SMS data, and location information in response to government requests. For data collected by private enterprises, the 2017 Cybersecurity Law and 2021 Data Security Law mandate that technology companies store user data domestically and share it with authorities when requested. Major surveillance technology providers like Hikvision and Dahua operate under national standards that ensure data integration with public security networks, while social media platforms establish standardized protocols that enable data sharing with the government.

At local levels, our fieldwork interviews with police officers in command centers[1] and frontline police stations reveal a tiered system of data access authorization.[2] For

[1] Command centers function as intelligence hubs for public security organs, coordinating digital surveillance, analysis, and police dispatch [56].

[2] During our fieldwork in a prefectural-level city in South China between August and October 2022, we conducted semi-structured interviews with police officers from the city-level and district-level command centers and frontline police stations in three administrative districts.

surveillance cameras installed in residential communities and apartment complexes, public security bureaus can access the footage either through direct requests or via city-level integrated systems that link these cameras to command centers. Access to social media data like WeChat requires authorization by provincial command centers, but telecommunications data like base station location tracking, SMS, and phone records can be obtained directly through city-level authorities. In fact, location tracking data, accessible with city-level permission, has become police officers' preferred surveillance tool due to its convenience and accuracy. This tiered system of data access and sharing creates a comprehensive surveillance infrastructure that enables state access to personal information ranging from basic communications to sophisticated behavioral patterns [44, 45].

Overall, the Chinese state has progressively adopted more invasive digital technologies to extend its social control from public spaces into more intimate spheres of private life. The new systems represent escalating digital control, allowing the state to achieve increasingly granular visibility and regulation over citizen behaviors and daily activities. The evolution of digital control in China thus provides an opportune context to examine citizens' attitudes to escalating surveillance.

Research Design

Survey Data Collection

To empirically test our hypotheses, we employ an independent-samples design with two online survey experiments independently conducted between March 7 and April 19, 2023.[3] The first sample was drawn from a pool of over 6.2 million registered internet users managed by Wenjuanxing Survey Company, one of China's largest survey platforms.[4] The second sample was drawn from a pool of over 1 million registered internet users managed by Diaoyanjia Survey Company, a leading survey platform widely used for professional market studies and academic research.[5] By leveraging two distinct sampling pools (see Appendix A for demographic details of the two sampling pools), we aim to mitigate potential biases associated with a single data source and enhance the representativeness and robustness of our results.

The same questionnaire was distributed among all registered users in both sampling pools, who are active internet users, primarily consisting of young netizens (under the age of 40) across China. Participants were offered monetary rewards of 5 CNY (approximately 0.7 USD) for completing the questionnaire. Table 1 presents the key demographic characteristics of our two samples. Participants in Sample 2

[3] Before conducting data collection, we pre-registered our research design, including hypotheses, treatment assignments, and questionnaires, on the Open Science Framework (OSF). Pre-registration helps us avoid data-driven bias and enhances the reliability of this research.

[4] The Wenjuanxing sampling pool can be found at https://www.wjx.cn/sample/service.aspx. Last accessed on April 28, 2025.

[5] The Diaoyanjia sampling pool can be found at https://www.surveyplus.cn/panel.html. Last accessed on April 28, 2025.

Table 1 Sample Demographic Characteristics

Variables	Sample 1	Sample 2
Male	.46 (.50)	.39 (.49)
Age	31.37 (7.17)	29.77 (9.33)
Education Level	2.80 (.49)	2.41 (.75)
Urban Hukou	.57 (.49)	.50 (.50)
Married	.68 (.47)	.40 (.49)
CCP Member	.16 (.37)	.10 (.30)
Observations	1049	1084

The number in each cell and that in the brackets indicate the mean and standard deviation, respectively

were generally younger than those in Sample 1, had lower educational attainment, fewer urban residents, fewer married individuals, and fewer Chinese Communist Party (CCP) members. By examining these demographically diverse samples, we aim to strengthen the robustness and generalizability of our findings. Figure 1 illustrates the geographic distribution of the respondents based on their primary residential areas.

Though our samples may not perfectly represent China's general population demographics, they capture a significant segment of the country's internet-savvy youth. This demographic group is particularly relevant to our research question, as they are more likely to be aware of and have direct experiences with various surveillance systems. The diversity of regional representation in our samples also helps to capture a broad range of perspectives and experiences related to escalating digital control across China.

To ensure data quality, we excluded low-quality or dubious responses using criteria such as attention checks, response consistency, and completion time (see Appendix B for details). After applying these exclusion criteria, our final dataset includes 1049 respondents in Sample 1 and 1084 respondents in Sample 2.

The anonymous survey experiment ensures the privacy and safety of our respondents and mitigates self-censorship by respondents. The conversion rate, i.e. the percentage of survey participants who completed the entire questionnaire, is 56% and 48% in the two samples respectively. These conversion rates fall within the typical range for online surveys and are comparable to other studies that focus on non-politically sensitive topics, such as marketing and educational research [20, 42, 47, 54].

In summary, by employing two independent samples and ensuring survey data quality, our data collection process tries to maximize the robustness, representativeness, and validity of our findings.

Treatment and Measures

In our experimental survey design, participants were required to complete a 10-minute-long survey questionnaire, which collected information on the respondents' demographic background, technology affinity, privacy concerns, political attitudes,

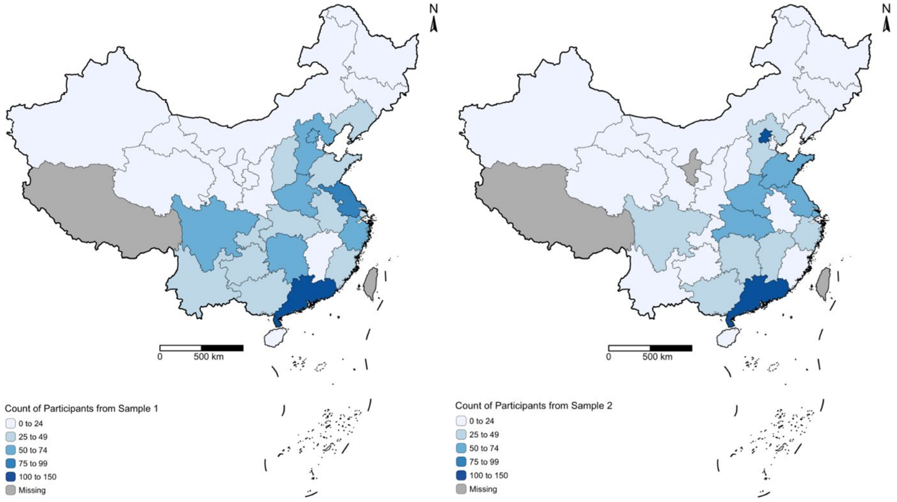


Fig. 1 Sample Geographical Distribution. Source: Authors' compilation based on survey respondents' residential locations

and acceptance of digital surveillance measures. In the survey experiment section, we randomly assign respondents to one control and three treatment groups. As shown in Table 2, all four groups were informed of the benefits of digital surveillance including public safety and pandemic control. In the control group, respondents received no information about state control motives underlying digital surveillance. In treatment scenarios, respondents received additional information revealing the state's underlying control intentions, either mass monitoring (i.e., collecting personal data on citizens), targeted repression (i.e., suppressing potential threats to regime stability), or both control intentions concurrently.

To ensure information authenticity and mitigate the risk of censorship, all treatment scenarios were constructed based on real cases reported by state media outlets such as People's Daily, China National Radio, China News, and Beijing News. The reports cover various surveillance systems and widely known incidents of coercive behaviors by Chinese local governments, such as using surveillance cameras to suppress villagers' petitions, using health codes to prevent citizens from withdrawing money from their bank accounts, or using health codes to prevent proprietors from engaging in collective actions to defend their property rights. At the end of the survey, the links to these media reports are provided for the respondents' reference (see Appendix C for the full survey questionnaire design).

This between-group experimental design allows us to test our hypotheses by comparing the public acceptance of digital control measures across different treatment groups. We expect that citizens' awareness of the state's control intentions (both mass monitoring and targeted repression) will decrease public acceptance across all digital control measures. Table 3 shows the treatment assignments in both samples. As detailed in Appendix D, the randomization is successful, and the four groups are well-balanced.

Table 2 Treatment Information

Assignments	Treatment Information
Control	We are living in a digital era: CCTV cameras are ubiquitous on the streets; facial recognition is often required to access certain public areas[a]; smartphones and mobile payments have also become prevalent. With the help of big data, it is difficult for criminals to evade the "Sky Net" surveillance, thus contributing to social order maintenance. In addition, digital tracking technologies like "health code" can accurately locate infected individuals and their close contacts, contributing to pandemic control in the past three years.
Monitoring Intention	We are living in a digital era … in the past three years. However, these advancements have enabled the state to collect and analyze citizens' daily activities and behavior patterns through extensive camera surveillance and smartphone tracking.
Repression Intention	We are living in a digital era … in the past three years. However, the state has exploited these tools to suppress dissent and target individuals perceived as threats. For example, health codes were used to impose mobility restrictions to prevent citizens from withdrawing money from their bank accounts, while CCTV cameras were used to monitor property owners who participated in collective rights-defending activities.
Both Intentions Concurrently	We are living in a digital era … in the past three years. However, these advancements have enabled the state to collect and analyze citizens' daily activities and behavior patterns through extensive camera surveillance and smartphone tracking. Furthermore, the state has exploited these tools to suppress dissent and target individuals perceived as threats. For example, health codes were used to impose mobility restrictions to prevent citizens from withdrawing money from their bank accounts, while CCTV cameras were used to monitor property owners who participated in collective rights-defending activities.

[a] Facial recognition systems are widely deployed as automatic entrance checks at public spaces like transportation hubs and office buildings. During COVID-19, these practices were amplified through integration with health code verification via "electronic sentinels" (*dianzi shaobing*) - checkpoint machines installed at high-traffic locations including hospitals, schools, residential communities, and office buildings to mandatorily verify individuals' personal information, health status, and travel history [15, 41]

Table 3 Treatment Assignments

	Group 1	Group 2	Group 3	Group 4
Assignments	Control	Monitoring Intention	Repression Intention	Both Intentions Concurrently
N in Sample 1	263	262	257	267
N in Sample 2	275	274	269	268

After reading the assigned information, participants were asked to indicate their support for four types of digital control measures with escalating intrusiveness and data granularity. We focus on four types of commonly used digital control methods:

1) CCTV cameras in public areas represent the initial form of digital control, offering limited data granularity and intrusion into private spheres [67]. 2) CCTV cameras in residential communities represent a step further into semi-private spaces to obtain more detailed information about citizens' daily routines and social interactions [52]. 3) Smartphone location tracking through GPS or cellular signal provides visibility about citizens' movements and social networks and offers a higher level of data granularity [46]. 4) At the most intrusive level, smartphone usage analysis harvests vast amounts of personal data, including calls, messages, social media usage, browsing histories, etc. It allows for the construction of highly granular digital profiles that map intimate personal behaviors [44]. Public acceptance of the four digital control measures was measured using a 4-point Likert scale, ranging from "1 strongly oppose", "2 oppose", "3 support", to "4 strongly support" (see Table 4 for details).[6]

Statistical Models

We employ OLS regression to estimate how state control intentions affect public acceptance of digital control. Our statistical model is as follows:

$$Y_i = \beta_0 + \beta_1 Treatment_i + \alpha_1 x_{1i} + \cdots + \alpha_k x_{ki} + \varepsilon$$

where Y_i indicates the individual i's acceptance for the four digital control measures discussed earlier; $Treatment_i$ refers to the treatment scenarios of varied state control intentions that individual i is randomly assigned to ("0″ for the control group, "1″ for monitoring intention, "2″ for repression intention, and "3″ for both intentions concurrently); β_0 is the intercept, and ε is the error term; x_{1i} to x_{ki} represent individual-level characteristics that may influence how individual i responds to different digital control tools.

The control variables include the respondents' demographics, political attitudes, privacy and security concerns, and technology affinity collected in the survey questionnaire (see Appendix C for the detailed survey questions). They are selected based on our theoretical framework and existing literature on public opinions about state control.

First, we incorporate basic demographic characteristics, such as gender, age, education level, hukou status, marital status, and CCP party membership, as they may shape individuals' attitudes toward state control and digital technologies [68].

Second, we control for citizens' political attitudes, specifically political trust and social trust, as they are closely associated with public support for state policies [62] including digital control [49]. Existing studies have found that trust in the government and inter-personal trust are positively related to support for digital control

[6] We deliberately chose a 4-point scale over the conventional 5-point scale [14, 23]. As research suggests that the neutral option in a 5-point scale often does not reflect true neutrality but allows respondents to circumvent sensitive questions that they are reluctant to answer [30, 60], the 4-point scale allows us to more accurately gauge the respondents' attitudes toward the surveillance measures.

Table 4 Measuring Public Acceptance of Digital Surveillance

To what extent do you support the following different big data management approaches?
Options: Strongly oppose/Oppose/Support/Strongly support

Degree of Intrusiveness Lower→ Higher	CCTV Cameras in Public Areas	Install CCTV cameras in public places (e.g., streets, intersections, subway stations) to monitor citizen activities.
	CCTV Cameras in Residential Areas	Install CCTV cameras in residential communities (e.g., entrances, corridors, elevators) to monitor citizen activities.
	Smartphone-based Location Tracing	Trace smartphone GPS and cell tower signals (e.g., the “travel itinerary code” used for pandemic control) to monitor citizens’ daily travel history.
	Smartphone-based Behavior Analysis	Collect and analyze smartphone usage data (e.g., conversations and posts on WeChat, “likes” on TikTok and Kwai, search keywords on Baidu, consumption patterns on Taobao, etc.) to monitor citizen behaviors.

measures in China including facial recognition [29], the social credit system [26], and close contact tracing for COVID-19 containment [27].

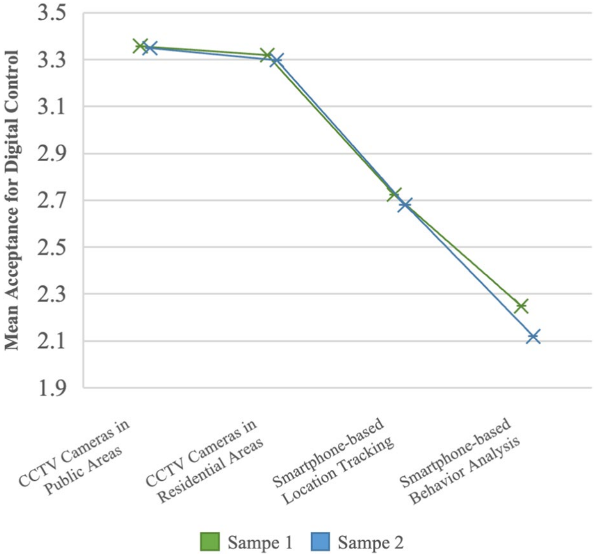
Third, we account for privacy concerns and concerns about personal safety and social stability, which are important factors influencing public support for digital control [9, 49]. Individuals more concerned about personal safety and social stability may embrace stricter digital control. Conversely, those who prioritize their privacy may be more cautious about the state overstepping into the personal realm.

Last, drawing on existing studies on public responses toward digital systems [64–66], past experience and knowledge of digital technologies will influence citizens' decisions on future adaptation [24, 28, 68]. We control for citizens' affinity towards CCTV cameras and smartphones (i.e., smartphone usage frequency and CCTV camera installation habits), the key digital control measures under this study.

Empirical Results

The analysis of the two independent samples consistently supports our hypothesis that public acceptance of digital control decreases as the level of intrusiveness increases. Figure 2 shows the average levels of public acceptance for the four control measures. CCTV cameras installed in public areas receive the highest acceptance rate, and that of CCTV cameras in residential areas is slightly lower but still relatively high (around 3.35 and 3.30, respectively, out of 4). However, public acceptance drops dramatically for smartphone monitoring, which is far more intrusive and collects more detailed personal data. The acceptance rate for location tracking drops to around 2.7, and smartphone usage analysis drops even further to around 2.2, which is in the "oppose" range in the survey response.

Fig. 2 Average Public Acceptance for Digital Surveillance



These findings provide important context for understanding how citizens evaluate surveillance risks. The sharp decline in acceptance between CCTV camera surveillance and smartphone monitoring suggests a critical threshold in public tolerance. When digital surveillance escalates from camera surveillance at fixed locations to individualized monitoring that enables more precise targeting, citizens become significantly more resistant, despite the propagated benefits of public safety and health. This pattern sets the stage for examining how awareness of state control intentions further shapes public acceptance.

We hypothesize that informing Chinese citizens of the state's monitoring and repressive intentions would reduce public acceptance of digital control, with greater effects for more intrusive control measures. Table 5 presents the t-test results of the two independent samples, comparing the mean differences in public acceptance between the treatment and control groups.

The results reveal statistically significant differences in almost all cases. From top to bottom rows in Table 4, we observe that revealing state intentions of massing monitoring, targeted repression, and both to the respondents leads to increasing declines in their acceptance of all the digital control measures. Meanwhile, from left to right columns in each sample, the effect of awareness about state control intentions on public acceptance is also larger for the more intrusive cellphone surveillance than for CCTV cameras. These findings indicate that awareness of state control intentions significantly shapes public responses to digital control in China, with stronger effects observed for more intrusive technologies that enable more granular data collection and more precise targeting of citizens.

To examine the empirical findings more thoroughly, we conduct OLS regressions utilizing the model specifications outlined in Section 4.3. Since the discussion above shows highly similar and stable patterns between our two samples, to enhance readability, we merge them into one dataset in the subsequent analyses. To ensure the robustness of our findings, we also run regressions on the two samples respectively, and the results are highly consistent (see Appendix E for details). In addition to OLS regression, we also conduct ordinal logistic regression, treating the dependent variables as ordinal variables. The statistical results remain robust (see Appendix F for details).

Table 6 presents the regression results on the combined samples. Models 1–4 show the baseline results with only the treatment variables as the predictors. Models 5–8 are the full models incorporating individual-level covariates. The treatment effects remain stable and statistically significant in almost all the models, with targeted repression consistently showing stronger negative effects than mass monitoring. This pattern could be because Chinese citizens are more aware of and accustomed to the state's mass monitoring, whereas less familiar with how surveillance can be weaponized against specific individuals. When they realize the state's repressive motives can pose a substantial threat to personal autonomy and rights, their acceptance of digital control measures declines more strongly. The effects are particularly pronounced for smartphone surveillance, suggesting that the effects of state control intentions become more salient when surveillance enables more precise tracking of individuals.

Table 5 T-test between Treatment and Control Groups (Separate Samples)

	Sample 1				Sample 2			
Mean Diff. of Support	Public CCTV	Residential CCTV	Location Tracking	Behavior Analysis	Public CCTV	Residential CCTV	Location Tracking	Behavior Analysis
Mass Monitoring vs Control	−.017	−.060	−.157**	−.155*	−.080*	−.102**	−.131**	−.140**
Targeted Repression vs Control	−.134***	−.135**	−.186***	−.178**	−.091**	−.110**	−.138**	−.180**
Both vs Control	−.138***	−.141***	−.242***	−.178**	−.094**	−.143***	−.303***	−.265***

*** $P <.01$, ** $P <.05$, * $P <.1$

Table 6 OLS Regression Results for Public Acceptance

	Baseline Model				Full Model			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Acceptance for Public CCTV	Acceptance for Residential CCTV	Acceptance for Location Tracking	Acceptance for Behavior Analysis	Acceptance for Public CCTV	Acceptance for Residential CCTV	Acceptance for Location Tracking	Acceptance for Behavior Analysis
Treated: Mass Monitoring	**−.049**	**−.081****	**−.144*****	**−.148*****	**−.067***	**−.123*****	**−.219*****	**−.207*****
	(.034)	**(.036)**	**(.046)**	**(.051)**	**(.038)**	**(.039)**	**(.05)**	**(.057)**
Treated: Targeted Repression	**−.112*****	**−.122*****	**−.161*****	**−.179*****	**−.152*****	**−.174*****	**−.252*****	**−.251*****
	(.034)	**(.036)**	**(.047)**	**(.052)**	**(.037)**	**(.039)**	**(.05)**	**(.057)**
Treated: Both	**−.115*****	**−.142*****	**−.272*****	**−.222*****	**−.133*****	**−.177*****	**−.315*****	**−.275*****
	(.034)	**(.036)**	**(.046)**	**(.051)**	**(.037)**	**(.039)**	**(.05)**	**(.056)**
Male					−.038	−.062**	−.128***	−.025
					(.027)	(.029)	(.036)	(.042)
Age					.002	−.002	−.005*	−.003
					(.002)	(.002)	(.003)	(.003)
Education: Vocational					.003	−.028	−.108	.036
					(.053)	(.056)	(.071)	(.081)
Education: University					.011	−.059	−.288***	−.137*
					(.05)	(.052)	(.067)	(.076)
Urban Hukou					−.025	−.022	−.138***	−.18***
					(.029)	(.03)	(.039)	(.044)
Married					.026	.042	.074	.061
					(.034)	(.036)	(.046)	(.052)
CCP Member					−.135***	−.121***	−.057	−.057

Table 6 (continued)

	Baseline Model				Full Model			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Acceptance for Public CCTV	Acceptance for Residential CCTV	Acceptance for Location Tracking	Acceptance for Behavior Analysis	Acceptance for Public CCTV	Acceptance for Residential CCTV	Acceptance for Location Tracking	Acceptance for Behavior Analysis
					(.04)	(.042)	(.054)	(.061)
Political Trust					.126***	.116***	.225***	.195***
					(.014)	(.015)	(.018)	(.021)
Social Trust					−.02	−.018	.014	.018
					(.016)	(.016)	(.021)	(.024)
Concerns: Personal Safety					.174***	.124***	−.039	−.167***
					(.034)	(.036)	(.046)	(.052)
Concerns: Social Stability					.102***	.12***	.014	−.122**
					(.034)	(.036)	(.046)	(.052)
Concerns: Privacy					.023	−.011	−.044**	−.084***
					(.015)	(.016)	(.02)	(.023)
Smartphone Usage Freq.					.041**	.015	−.035	−.081***
					(.017)	(.017)	(.022)	(.025)
Install CCTV at Home					.044	.09***	.05	.068
					(.027)	(.029)	(.036)	(.041)
_cons	3.427***	3.406***	2.869***	2.869***	2.245***	2.612***	3.688***	4.126***
	(.027)	(.028)	(.037)	(.037)	(.164)	(.172)	(.219)	(.249)

Table 6 (continued)

	Baseline Model				Full Model			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Acceptance for Public CCTV	Acceptance for Residential CCTV	Acceptance for Location Tracking	Acceptance for Behavior Analysis	Acceptance for Public CCTV	Acceptance for Residential CCTV	Acceptance for Location Tracking	Acceptance for Behavior Analysis
Control for Sample 1/2	Y	Y	Y	Y	Y	Y	Y	Y
Observations	2133	2133	2133	2133	1652	1652	1652	1652
R-squared	.007	.009	.017	.017	.139	.115	.151	.118

*** $p<.01$, ** $p<.05$, * $p<.1$ (Standard errors are in parentheses)

Specifically, the full models show that for CCTV cameras in public areas, revealing the state's mass monitoring intentions and repression intentions both lead to statistically significant decreases in public acceptance, while their combination leads to a 4% reduction from the average support level. For CCTV cameras in residential communities, which represent a step towards more intrusive surveillance, revealing monitoring and repression intentions both lead to significant decreases, while their combination leads to a 5.4% reduction from the average support level. These patterns are similar to those observed for public CCTV surveillance, but the larger magnitudes of the coefficients suggest that as cameras penetrate the semi-private realm, citizens' perceived threats from state control are amplified. For smartphone location tracking, revealing monitoring and repression intentions also leads to significant decreases in public acceptance, while their combination leads to a larger 11.6% decline from the average support level. Similarly, for smartphone behavior analysis, monitoring and repression intentions both decrease support, while their combination results in an even steeper 12.6% decline from the average support level.

Interestingly, revealing the state's control intentions generates the largest magnitudes of decline in public support for smartphone location tracking, although it is less intrusive than smartphone behavior analysis. This trend likely stems from Chinese citizens' recent negative experiences with location tracking surveillance during the COVID-19 pandemic, including the "travel tracer" system and mobility constraints [75]. Revealing the state's control intentions during the survey may have brought respondents' negative experiences to the forefront [78], thus leading to a more significant decline in public acceptance of location tracking.

Regarding the covariates, political trust is significantly and positively associated with public acceptance of digital control, with a more substantial impact on the acceptance level of intrusive smartphone monitoring. This echoes existing studies that link political trust with public approval of surveillance, such as the social credit system [26, 38]. But the association between social trust and public acceptance is negligible and statistically insignificant. Personal safety and social stability concerns show a consistent pattern: both positively predict acceptance of CCTV surveillance but turn negative for smartphone monitoring, suggesting that citizens' evaluation of security benefits versus control risks shifts as surveillance becomes more capable of precise targeting, indicating that citizens may view the latter more as risks than benefits due to the potential abuse of intimate data collected from cellphones. Privacy concerns are negatively associated with support for smartphone monitoring but have a negligible impact on support for camera surveillance. This finding suggests that Chinese citizens' lack of privacy concerns, as some earlier studies argue [79, 80], mainly applies to less intrusive surveillance technologies, but once surveillance invades the personal sphere via cellphone, privacy concerns will manifest and undermine public approval.

Citizens' affinity for CCTV cameras, especially their choice to install cameras at home, has a positive effect on all four digital control measures. In contrast, citizens' affinity to smartphones has a small and insignificant effect on their acceptance level for less intrusive CCTV systems, but the coefficient turns negative for smartphone location tracking and becomes negative and significant for smartphone behavior analysis. This suggests that frequent smartphone users tend to perceive greater threats associated with the intrusion of smartphone-based control measures, as smartphone surveillance can be omnipresent and hard to evade, making it a powerful weapon for state control over individuals.

As for the demographic controls, female participants tend to express higher acceptance of digital control, possibly due to their prioritization of perceived security benefits over potential threats. Individuals with higher levels of education are less accepting of digital control, particularly for intrusive smartphone monitoring. This can be attributed to their greater concern about personal rights and more critical attitudes toward state control. Urban residents also exhibit lower acceptance for digital surveillance, possibly because they have previously experienced or witnessed more severe consequences of digital controls during the COVID-19 pandemic than their rural counterparts. CCP party members exhibit lower acceptance of digital control, which can be attributed to their higher level of political awareness and understanding of the digital control systems. They may also be more concerned about the potential exposure of sensitive activities by digital surveillance. However, these demographic factors are not statistically significant in all models.

To further examine variations in the effects of state control intentions on digital surveillance perceptions across citizen subgroups, we also conduct heterogeneity analysis (see Appendix G for details). Using subsample analysis with the full model specification, we find that CCP members demonstrate a distinctive pattern of relative tolerance of the state's monitoring intentions across surveillance forms, yet exhibit heightened resistance when informed of the state's repressive intentions, suggesting that even for political elites, surveillance acceptance has critical boundaries. Privacy emerges as a moderating factor, with individuals reporting high privacy concerns displaying more negative responses, especially to more intrusive surveillance technologies.

Taken together, our statistical results reveal a stark pattern: awareness of state intentions of mass monitoring and targeted repression significantly reduces public acceptance across all surveillance measures. The negative impact proves particularly pronounced for smartphone surveillance that enables precise identification and tracking of individuals. The findings suggest that as regimes deploy more intrusive technologies to gather granular data, they risk crossing the resistance threshold and catalyzing public opposition. This dynamic underscores fundamental constraints on digital authoritarianism: regimes must balance their surveillance ambitions against the risk of public resistance when citizens recognize how collected information can be exploited for control purposes.

Robustness Checks and Textual Analysis

This section presents additional checks to ensure the reliability of our findings.

First, to address the challenge of preference falsification, where respondents may intentionally conceal their true attitudes when answering politically sensitive questions [21, 31], we construct a "self-censorship" index to control for the extent to which respondents obscure their genuine views toward the regime due to social desirability concerns. This index, inspired by the approach of Shen and Truex

[57], measures the difference in item non-response rates (i.e., “Don’t Know” and “Hard to Say” responses) between politically sensitive questions (e.g., political trust, regime compliance) and non-sensitive questions (e.g., demographics). A higher value indicates greater self-censorship, as respondents are more likely to refuse to answer sensitive questions than non-sensitive ones. After including this self-censorship index as a control variable in our statistical models, our key findings remain highly stable and consistent across different model specifications (see Appendix H for details). These robust results mitigate concerns that our findings may be biased by respondents’ tendency to provide socially desirable responses on sensitive political topics related to the regime, especially in the authoritarian context.

Second, to address the issue of missing values in our survey data, which may lead to biased estimation, we use multiple imputations to estimate the missing values (see Appendix I for details). Specifically, we use Amelia’s EMB (expectation-maximization with bootstrapping) algorithm, which applies the EM algorithm on bootstrapped samples of the incomplete data to draw complete-data parameters and then uses these parameters to generate imputed values for missing data [19]. This approach maximizes statistical power while minimizing bias when data are not missing completely at random – a common scenario in survey research. After recovering the full sample, our key findings remain stable. This consistency bolsters confidence that our conclusions are not influenced by the missing values in the original data, further reinforcing the robustness of our empirical results.

Third, to gain additional insights into citizens’ perceptions, we analyzed over 2000 open-ended responses collected through our survey. Participants across different treatment groups were asked about their general feelings about digital control practices in China. They offered a plethora of answers showing divergent attitudes, such as “I support digital control, which is inevitable in the digital age,” “Big data is very useful for social management, but the government should manage the data responsibly,” and “Big data analysis is going too far now.” Given the large volume of textual data, we leverage advanced large language models (LLMs) to conduct sentiment analysis [82]. We deploy multiple open-source LLM models locally to determine the sentiment underlying each open-ended response about digital control perceptions on a scale from 0 (very negative) to 1 (very positive). Higher scores (> 0.7) emphasize the benefits of digital surveillance such as governance efficiency, moderate scores (0.4–0.6) recognize both risks and benefits, while lower scores (< 0.3) express strong reservations about digital control and loss of autonomy (see Appendix J for details).

The textual analysis reveals patterns that align with our theoretical arguments. Respondents express more negative sentiments regarding digital control in general when informed about state control intentions. Specifically, we observe a 5% decrease in sentiment scores for awareness of monitoring intentions, a 7% decrease for repressive intentions, and a 10% decrease when both monitoring and repressive intentions are presented concurrently (see Fig. 3). The sentiment analysis of the open-ended responses provides additional evidence that corroborates our main findings: As citizens become more aware of state control intentions, their general attitude toward digital control turns more negative.

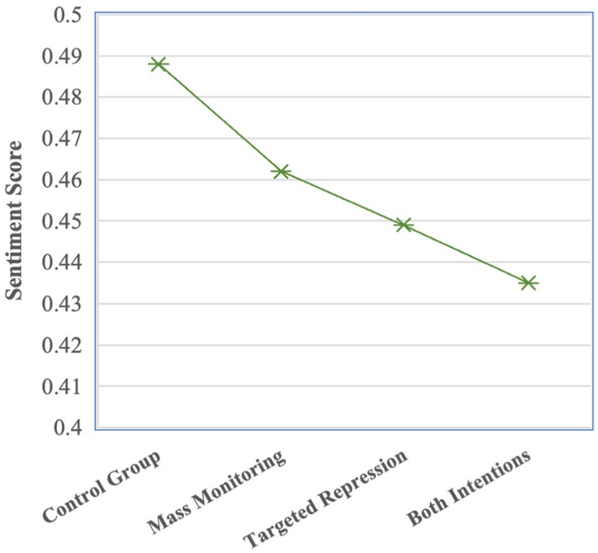


Fig. 3 Sentiments in Open-ended Responses

Discussion and Conclusion

This study proposes and empirically tests a risk-benefit analytical framework that transcends traditional privacy-security trade-offs to explain public perceptions of digital surveillance in authoritarian contexts. We argue that public acceptance or resistance to surveillance technologies is conditional on the perceived risks versus benefits, which can accommodate more factors than just privacy versus security. While the benefits are widely believed to lie in public security and health, the perceived risks are far beyond the privacy concerns emphasized in existing literature. In authoritarian contexts, citizens' risk assessments reflect a more complex political calculus due to the state's control intentions, including mass monitoring and targeted repression. Whereas the threat of mass monitoring stems from pervasive surveillance of all citizens, targeted repression presents personalized threats of state coercion against individuals. These political risks are further amplified by technological intrusiveness, as surveillance systems that penetrate deeper into private spheres enable more granular collection of personal data and more precise targeting of individuals. The awareness of state control intentions and technological intrusiveness collectively shape citizens' risk perceptions of digital surveillance.

We test these theoretical arguments through a survey experiment on two independent samples. The survey results demonstrate that revealing the state's control intentions - both mass monitoring and targeted repression - significantly reduces public acceptance of digital surveillance, with stronger effects for the more intrusive measures. The statistical results are robust to regression analyses on both independent samples and the combined samples and stand a series of robustness tests. The empirical findings thus strongly support our arguments that citizens become significantly more alert and resistant when they are aware of surveillance's potential for political control and repression.

Contrary to earlier findings suggesting widespread acquiescence to digital surveillance [26–29, 61], we find that Chinese citizens respond differently to various digital control measures. By disaggregating surveillance across a spectrum of intrusiveness, our study helps reconcile the seemingly contradictory findings in existing research. For relatively unintrusive measures like CCTV cameras, citizens exhibit high acceptance. However, acceptance levels decrease significantly for more invasive technologies of smartphone monitoring that intrude into private spheres to collect more granular data and enable more precise state control. This pattern of varying acceptance becomes particularly pronounced when combined with awareness of state control intentions - citizens show stronger resistance to intrusive technologies when their potential for mass monitoring and targeted repression is revealed.

Our findings highlight the existence of a "resistance threshold," a point at which the perceived risks outweigh the benefits of digital surveillance and trigger a sharp decline in public acceptance. As regimes push surveillance measures in pursuit of more granular data and when citizens become aware of how the collected data can be weaponized for political control, they risk crossing the threshold and encountering significantly increased public resistance.

Such dynamics are not unique to China. Comparative studies reveal that intrusive surveillance, such as spyware in Middle Eastern regimes, has encountered stronger opposition than less advanced systems [12]. The expanding surveillance in Russia has prompted growing skepticism, particularly when it targets political activists rather than criminals [12, 43]. Autocrats have learned that for sophisticated information control to succeed, it's better to keep citizens unaware of their control intentions [17]. These observations suggest that even in different institutional contexts, public perception is similarly shaped by the awareness of state control intentions and the intrusiveness of surveillance. Our risk-benefit framework thus offers analytical leverage for understanding surveillance dynamics across authoritarian systems.

This research generates important implications for authoritarian resilience and state-society relations in the era of digital authoritarianism [11, 51, 73]. While technological innovations enhance state surveillance capabilities, our findings suggest that public opposition can heighten when citizens recognize how collected information might be weaponized for political control. This resistance is likely to grow as surveillance technology increasingly intrudes into citizens' private lives for more precise monitoring and repression. To prevent such intrusion from provoking public revolt, authoritarian regimes may need to promote added benefits, such as national security and governance efficiency, to justify tighter digital control. They are also motivated to conceal the political risks that citizens face by implementing more secretive surveillance and discreet repression to decrease public awareness and aversion.

Finally, we acknowledge the limitations of this study. While our sample captures a significant segment of China's internet-savvy youth, it may not perfectly represent the demographic composition of the general Chinese population. Younger, urban, and more educated individuals may be more aware of digital control compared to older, rural, and less educated segments of the population. How different socioeconomic and regional groups perceive digital control warrants further examination. Moreover, our study provides a snapshot of public attitudes but cannot capture potential long-term shifts as digital control systems dramatically expand and routinize. Initial resistance could give way to resigned acceptance, or societal opposition could intensify over time if the state continuously escalates digital control. Longitudinal analysis is needed to understand the long-term patterns.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s11366-025-09918-5.

Authors' Contributions The two authors make equal contributions to this research.

Funding The authors acknowledge the funding support from CUHK Direct Grant 4052279.

Data Availability The data used in this manuscript are available upon request.

Declarations

Ethics Approval and Consent to Participate This research has received ethics approval from the Survey and Behavioural Research Ethics Committee of the Chinese University of Hong Kong and consent from participants to the surveys.

Consent for Publication Not applicable.

Conflict of interest The authors declare no competing interests.

References

1. Ardabili, B. R., A. D. Pazho, G. A. Noghre, V. Katariya, G. Hull, S. Reid, and H. Tabkhi. 2023. *Exploring public's perception of safety and video surveillance technology: A survey approach*. https://doi.org/10.48550/arXiv.2312.06707.
2. Aytac, S. E., L. Schiumerini, and S. Stokes. 2018. Why do people join backlash protests? Lessons from Turkey. *Journal of Conflict Resolution* 62 (6): 1205–1228. https://doi.org/10.1177/0022002716686828.
3. Beraja, M., A. Kao, D. Y. Yang, and N. Yuchtman. 2023. AI-tocracy. *The Quarterly Journal of Economics* 138 (3): 1349–1402. https://doi.org/10.1093/qje/qjad012.
4. Beraja, M., D. Y. Yang, and N. Yuchtman. 2023. Data-intensive innovation and the state: Evidence from AI firms in China. *The Review of Economic Studies* 90 (4): 1701–1723. https://doi.org/10.1093/restud/rdac056.
5. Bischoff, P. 2022. *Surveillance camera statistics: Which City has the Most CCTV cameras?* Comparitech https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. Accessed October 3, 2022.
6. Cayford, M., W. Pieters, and P. H. A. J. M. van Gelder. 2019. Wanting it all – Public perceptions of the effectiveness, cost, and privacy of surveillance technology. *Journal of Information, Communication and Ethics in Society* 18 (1): 10–27. https://doi.org/10.1108/JICES-11-2018-0087.

7. Curtice, T. 2021. How repression affects public perceptions of police: Evidence from a natural experiment in Uganda. *Journal of Conflict Resolution* 65 (10): 1680–1708. https://doi.org/10.1177/00220027211013097.
8. Davenport, C. 2007. *State repression and the domestic democratic peace*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511510021.
9. Davis, D. W., and B. D. Silver. 2004. Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science* 48 (1): 28–46. https://doi.org/10.1111/j.0092-5853.2004.00054.x.
10. Degli Esposti, S., K. Ball, and S. Dibb. 2021. What's in it for us? Benevolence, National Security, and digital surveillance. *Public Administration Review* 81 (5): 862–873. https://doi.org/10.1111/puar.13362.
11. Diamond, L., R. J. Deibert, S. Feldstein, and Q. Xiao. 2019. The road to digital unfreedom. *Journal of Democracy* 30 (1): 20–67. https://doi.org/10.1353/jod.2019.0001.
12. Feldstein, S. 2021. *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford, New York: Oxford University Press.
13. Friedewald, M., M. van Lieshout, S. Rung, M. Ooms, and J. Ypma. 2015. Privacy and security perceptions of European citizens: A test of the trade-off model. In *Privacy and identity Management for the Future Internet in the age of globalisation*, ed. J. Camenisch, S. Fischer-Hübner, and M. Hansen, 39–53. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-18621-4_4.
14. Garland, R. 1991. The mid-point on a rating scale: Is it desirable. *Marketing Bulletin* 2 (1): 66–70.
15. Germanò, M. A., A. Liu, J. Skebba, and B. Jili. 2023. Digital surveillance trends and Chinese influence in light of the COVID-19 pandemic. *Asian Journal of Comparative Law* 18 (1): 91–115. https://doi.org/10.1017/asjcl.2022.31.
16. Gohdes, A. R. 2020. Repression technology: Internet accessibility and state violence. *American Journal of Political Science* 64 (3): 488–503. https://doi.org/10.1111/ajps.12509.
17. Guriev, S., and D. Treisman. 2020. A theory of informational autocracy. *Journal of Public Economics* 186:104158. https://doi.org/10.1016/j.jpubeco.2020.104158.
18. Gurinskaya, A. 2020. Young citizens attitudes towards CCTV and online surveillance in Russia. In *Digital transformation and global society*, ed. D.A. Alexandrov, A.V. Boukhanovsky, A.V. Chugunov, Y. Kabanov, O. Koltsova, and I. Musabirov, 61–74. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-65218-0_5.
19. Honaker, J., G. King, and M. Blackwell. 2011. Amelia II: A program for missing data. *Journal of Statistical Software* 45:1–47. https://doi.org/10.18637/jss.v045.i07.
20. Ilieva, J., S. Baron, and N. M. Healey. 2002. Online surveys in marketing research. *International Journal of Market Research* 44 (3): 1–14. https://doi.org/10.1177/147078530204400303.
21. Jiang, J., and D. L. Yang. 2016. Lying or believing? Measuring preference falsification from a political purge in China. *Comparative Political Studies* 49 (5): 600–634. https://doi.org/10.1177/0010414015626450.
22. Jin, X., and Y. Dai. 2024. Data-driven technology, organizational structure, and interdepartmental data sharing: The case of government-led digital projects in Guangzhou. *Chinese Political Science Review* 1–18. https://doi.org/10.1007/s41111-024-00257-z.
23. Kalton, G., J. Roberts, and D. Holt. 1980. The effects of offering a middle response option with opinion questions. *Journal of the Royal Statistical Society: Series D (The Statistician)* 29 (1): 65–78. https://doi.org/10.2307/2987495.
24. Kim, S. S., and N. K. Malhotra. 2005. A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena. *Management Science* 51 (5): 741–755. https://doi.org/10.1287/mnsc.1040.0326.
25. Kokkoris, M. D., and B. Kamleitner. 2020. Would you sacrifice your privacy to protect public health? Prosocial responsibility in a pandemic paves the way for digital surveillance. *Frontiers in Psychology* 11. https://doi.org/10.3389/fpsyg.2020.578618.
26. Kostka, G. 2019. China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society* 21 (7): 1565–1593. https://doi.org/10.1177/1461444819826402.
27. Kostka, G., and S. Habich-Sobiegalla. 2024. In times of crisis: Public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States. *New Media & Society* 26 (4): 2256–2294. https://doi.org/10.1177/14614448221083285.
28. Kostka, G., L. Steinacker, and M. Meckel. 2021. Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United

States. *Public Understanding of Science* 30 (6): 671–690. https://doi.org/10.1177/09636625211001555.

29. Kostka, G., L. Steinacker, and M. Meckel. 2022. Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*101761. https://doi.org/10.1016/j.giq.2022.101761.
30. Krosnick, J. A. 2018. Questionnaire Design. In *The Palgrave handbook of survey research*, 439–455. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-54395-6_53.
31. Kuran, T. 1997. *Private truths, public lies: The social consequences of preference falsification*. Cambridge: Harvard University Press https://www.hup.harvard.edu/books/9780674707580.
32. Lachapelle, J. 2022. Repression reconsidered: Bystander effects and legitimation in authoritarian regimes. *Comparative Politics* 54 (4): 695–716. https://doi.org/10.5129/001041522X16317396828722.
33. Li, H., and L. Gu. 2025. Smart interaction vs. face-to-face? Evidence from a survey experiment on perceived government responsiveness in China. *Journal of Chinese Political Science*1–33. https://doi.org/10.1007/s11366-024-09900-7.
34. Li, Y. 2015. The history and prospects of Safe City. *China Public Security* 9:88–92.
35. Li, Y., D. Liu, and L. Shao. 2024. Propaganda with subculture: A resource for internet control in China. *Journal of Chinese Political Science*1–25. https://doi.org/10.1007/s11366-024-09897-z.
36. Liao, X., J. Zhao, and Y. Cheng. 2025. Party-led digitalization: The CCP'S role in steering China's E-government transformation. *Chinese Political Science Review*1–29. https://doi.org/10.1007/s41111-024-00274-y.
37. Lin, X. 2025. A model of big data-based governance: China's National Government big Data Platform and an analysis of its governance competence. *Chinese Political Science Review*1–40. https://doi.org/10.1007/s41111-025-00279-1.
38. Liu, C. 2022. Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems. *International Sociology* 37 (3): 391–412. https://doi.org/10.1177/02685809221084446.
39. Liu, J., and X. Wang. 2017. In your face: China's all-seeing state. *BBC News*. https://www.bbc.com/news/av/world-asia-china-42248056. Accessed May 22, 2023.
40. Lyon, D. 2013. *The electronic eye: The rise of surveillance society - computers and social control in context*. New York: John Wiley & Sons.
41. Mahr, D., and M. Bloch. 2022. Digital risk distribution and COVID-19: How contact tracing is promoted as a solution to equilibrate public health and economic prosperity during pandemics. *Digital Health* 8:20552076221085068. https://doi.org/10.1177/20552076221085068.
42. Manfreda, K. L., M. Bosnjak, J. Berzelak, I. Haas, and V. Vehovar. 2008. Web surveys versus other survey modes: A Meta-analysis comparing response rates. *International Journal of Market Research* 50 (1): 79–104. https://doi.org/10.1177/147078530805000107.
43. Maréchal, N. 2017. Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and Communication* 5 (1): 29–41. https://doi.org/10.17645/mac.v5i1.808.
44. Mozur, P., C. Fu, and C. A. Chang. 2022. How China's police used phones and faces to track protesters. *The New York Times* https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html. Accessed May 22, 2023.
45. Mozur, P., and A. Krolik. 2019. A surveillance net blankets China's cities, giving police vast powers. *The New York Times*. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html. Accessed May 22, 2023.
46. Mozur, P., M. Xiao, and J. Liu. 2022. 'An invisible cage': How China is policing the future. *The New York Times* https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html. Accessed August 20, 2023.
47. Nulty, D. D. 2008. The adequacy of response rates to online and paper surveys: What can be done? *Assessment & Evaluation in Higher Education* 33 (3): 301–314. https://doi.org/10.1080/02602930701293231.
48. Papageorgiou, M., M. Can, and A. Vieira. 2024. China as a threat and balancing behavior in the realm of emerging technologies. *Chinese Political Science Review* 9 (4): 441–482. https://doi.org/10.1007/s41111-024-00248-0.
49. Pavone, V., and S. D. Esposti. 2012. Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science* 21 (5): 556–572. https://doi.org/10.1177/0963662510376886.

50. Penney, J. W. 2017. Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review* 6 (2): https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case. Accessed December 1, 2024.
51. Polyakova, A., and C. Meserole. 2019. Exporting digital authoritarianism: The Russian and Chinese models. *Foreign Policy at Brookings* 8:1–22.
52. Qian, I., M. Xiao, P. Mozur, and A. Cardia. 2022. Four takeaways from a times investigation into China's expanding surveillance state. *The New York Times* https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html. Accessed July 3, 2023.
53. Roberts, M. E. 2018. *Censored: Distraction and diversion inside China's great firewall*. Princeton: Princeton University Press https://press.princeton.edu/books/hardcover/9780691178868/censored?srsltid=AfmBOoqvL3facmBgCzWyeODQqfHlL_uiV7ChW0YXNMgxKMmfc7dqocZ1.
54. Sax, L. J., S. K. Gilmartin, and A. N. Bryant. 2003. Assessing response rates and nonresponse Bias in web and paper surveys. *Research in Higher Education* 44 (4): 409–432. https://doi.org/10.1023/A:1024232915870.
55. Schlund, R., and E. M. Zitek. 2024. Algorithmic versus human surveillance leads to lower perceptions of autonomy and increased resistance. *Communications Psychology* 2 (1): 1–9. https://doi.org/10.1038/s44271-024-00102-8.
56. Schwarck, E. 2018. Intelligence and informatization: The rise of the Ministry of Public Security in intelligence work in China. *The China Journal* 80 (1): 1–23. https://doi.org/10.1086/697089.
57. Shen, X., and R. Truex. 2021. In search of self-censorship. *British Journal of Political Science* 51 (4): 1672–1684. https://doi.org/10.1017/S0007123419000735.
58. Shih, V. C. 2021. China's Leninist response to COVID-19: From information repression to Total mobilization. In *Coronavirus politics*, ed. S.L. Greer, E.J. King, E.M. da Fonseca, and A. Peralta-Santos, 67–85. University of Michigan Press https://www.jstor.org/stable/10.3998/mpub.11927713.6. Accessed April 7, 2023.
59. Stoycheff, E., J. Liu, K. Xu, and K. Wibowo. 2019. Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society* 21 (3): 602–619. https://doi.org/10.1177/1461444818801317.
60. Sturgis, P., C. Roberts, and P. Smith. 2014. Middle alternatives revisited: How the neither/nor response acts as a way of saying "I Don't know"? *Sociological Methods & Research* 43 (1): 15–38. https://doi.org/10.1177/0049124112452527.
61. Su, Z., X. Xu, and X. Cao. 2022. What explains popular support for government monitoring in China? *Journal of Information Technology & Politics* 19 (4): 377–392. https://doi.org/10.1080/19331681.2021.1997868.
62. Tang, W. 2016. *Populist authoritarianism: Chinese political culture and regime sustainability*. New York, NY: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190205782.001.0001.
63. van Heek, J., K. Arning, and M. Ziefle. 2017. The surveillance society: Which factors form public acceptance of surveillance technologies? In *Smart cities, green technologies, and intelligent transport systems*, ed. M. Helfert, C. Klein, B. Donnellan, and O. Gusikhin, 170–191. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-63712-9_10.
64. Venkatesh, V., and F. D. Davis. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science* 46 (2): 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926.
65. Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS Quarterly* 27 (3): 425–478. https://doi.org/10.2307/30036540.
66. Venkatesh, V., J. Y. L. Thong, and X. Xu. 2012. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly* 36 (1): 157–178. https://doi.org/10.2307/41410412.
67. Walton, G. 2001. *China's Golden shield: Corporations and the development of surveillance Technology in the People's republic of China*. Hanover: Rights & Democracy.
68. Wang, K., Z. Wang, Y. Hu, and D. Chen. 2025. Digital forgotten people?: decomposing digital divide in urban China. *Journal of Chinese Governance* 10 (1): 57–79. https://doi.org/10.1080/23812346.2024.2408497.
69. Wang, Y., P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor. 2013. Privacy nudges for social media: An exploratory Facebook study. In *Proceedings of the 22nd international conference on world wide web*, 763–770. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2487788.2488038.

70. Wang, Y., and H. Pan. 2024. Information collection, public attitudes, and supportive behavior tendencies in the urban digital transformation: A survey experiment in a facial recognition scenario. *Journal of Chinese Governance* 9 (4): 483–510. https://doi.org/10.1080/23812346.2024.2378395.
71. Westerlund, M., D. A. Isabelle, and S. Leminen. 2021. The acceptance of digital surveillance in an age of big data. *Technology Innovation Management Review* 11 (3): 32–44. https://doi.org/10.22215/TIMREVIEW/1427.
72. Woods, D. 2025. Stag hunt in the digital wilds: Legitimizing global AI governance amidst diverse terrains. *Fudan Journal of the Humanities and Social Sciences*1–32. https://doi.org/10.1007/s40647-025-00438-3.
73. Woods, D. 2025. AI as a tool for surveillance: China's concave trilemma. *Journal of Chinese Political Science*1–35. https://doi.org/10.1007/s11366-025-09907-8.
74. Xiao, H., Y. He, and W. Ge. 2024. Living with digital government: Effects of technology anxiety on public support for policy in China. *Journal of Chinese Political Science*1–26. https://doi.org/10.1007/s11366-024-09898-y.
75. Xu, F., and Q. Liu. 2021. China: Community policing, high-tech surveillance, and authoritarian durability. In *Covid-19 in Asia: Law and policy contexts*, ed. V.V. Ramraj, 27–42. Oxford University Press. https://doi.org/10.1093/oso/9780197553831.003.0002.
76. Xu, X. 2021. To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science* 65 (2): 309–325. https://doi.org/10.1111/ajps.12514.
77. Xu, X., G. Kostka, and X. Cao. 2022. Information control and public support for social credit Systems in China. *The Journal of Politics* 84 (4): 2230–2245. https://doi.org/10.1086/718358.
78. Zaller, J. R. 1992. *The nature and origins of mass opinion*. Cambridge: Cambridge university press. https://doi.org/10.1017/CBO9780511818691.
79. Zhang, B., H. M. Peterson Jr., and W. Sun. 2017. Perception of digital surveillance: A comparative study of high school students in the U.S. and China. *Issues in Information Systems* 18 (1): https://doi.org/10.48009/1_iis_2017_98-108.
80. Zhang, H., J. Guo, C. Deng, Y. Fan, and F. Gu. 2019. Can video surveillance systems promote the perception of safety? Evidence from surveys on residents in Beijing, China. *Sustainability* 11 (6): 1595. https://doi.org/10.3390/su11061595.
81. Zhu, J., S. Bai, S. Kang, J. Wang, and K. Liu. 2024. Authoritarian cue effect of state repression. *American Journal of Political Science*. https://doi.org/10.1111/ajps.12916.
82. Ziems, C., W. Held, O. Shaikh, J. Chen, Z. Zhang, and D. Yang. 2024. Can large language models transform computational social science? *Computational Linguistics* 50 (1): 237–291. https://doi.org/10.1162/coli_a_00502.

Dakeng Chen is a Postdoctoral Fellow in the School of Governance and Policy Science, the Chinese University of Hong Kong. His research encompasses comparative politics, contemporary Chinese politics, and computational methods, with a particular interest in digital control and state-society relations in authoritarian contexts.

Jing Vivian Zhan is a professor in the School of Governance and Policy Science, the Chinese University of Hong Kong. Her research interests span comparative political economy, contemporary Chinese politics, and research methodology, with a focus on post-Mao reforms, intergovernmental relations, local governance, and development studies.