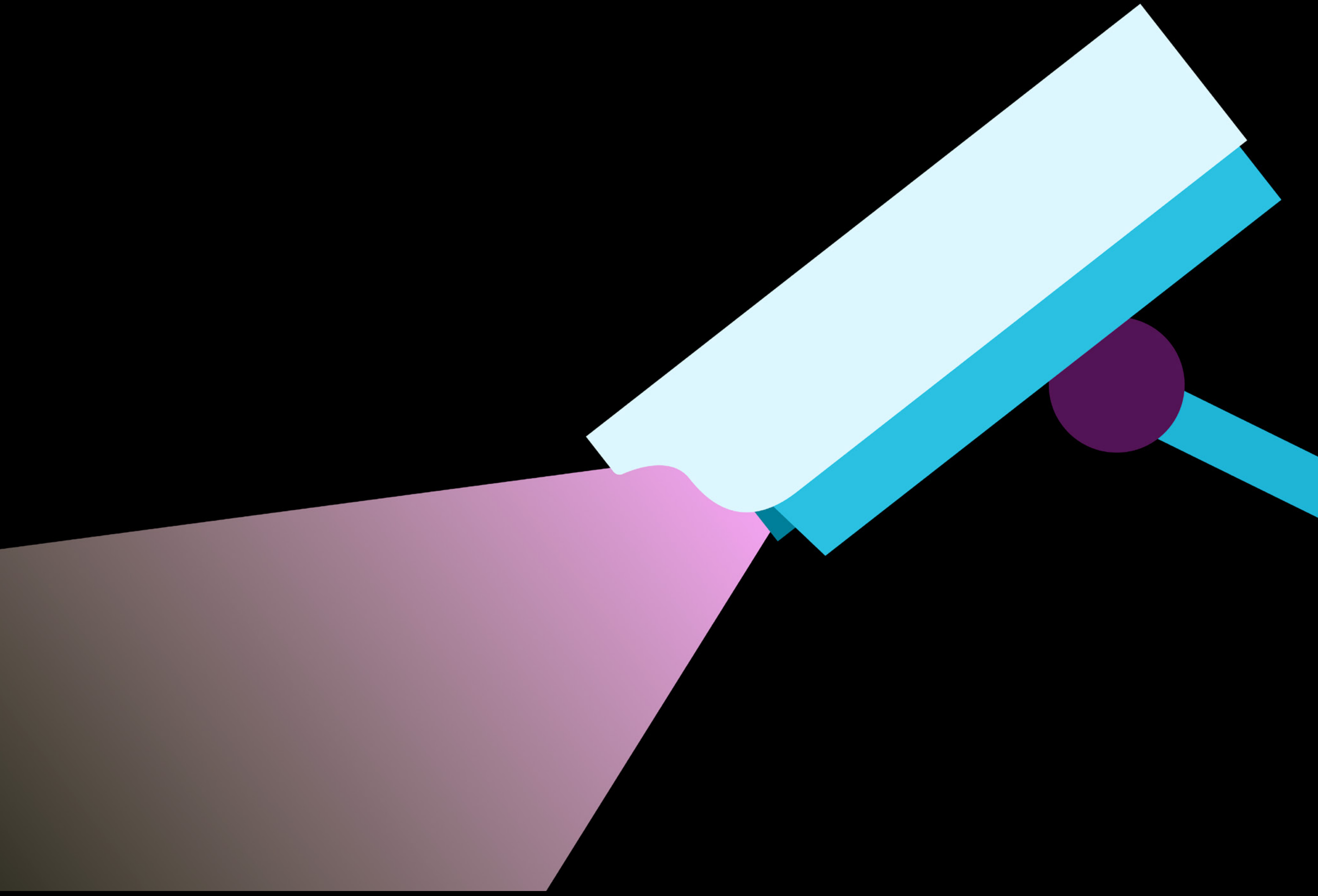
Surveillance, privacy and agency

Insights from China

Daria Impiombato, Yvonne Lau and Luisa Gyhn



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief
Report No. 74/2023

About the authors

Daria Impiombato is an analyst at ASPI's Cyber, Technology and Security Centre.

Yvonne Lau is a researcher at ASPI's Cyber, Technology and Security Centre.

Luisa Gyhn is a research intern at ASPI.

Acknowledgements

ASPI acknowledges the Ngunnawal and Ngambri peoples, who are the traditional owners and custodians of the land upon which this work was prepared, and their continuing connection to land, waters and community. We pay our respects to their cultures, country and elders past, present and emerging.

The authors would like to thank Dr Alexandra Caples, Fergus Ryan and Stephan Robin for all their work on this project. Thank you also to all of those who peer-reviewed the work and provided valuable feedback that improved it, including Mike Bareja, Ausma Bernot, Danielle Cave, Emile Dirks and Jacinta Keast.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI Cyber, Technology and Security

ASPI's Cyber, Technology and Security (CTS) analysts aim to inform and influence policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS remains a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and Internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity building team that conducts workshops, training programs and large-scale exercises for the public, private and civil society sectors. Current projects are focusing on capacity building in Southeast Asia and the Pacific Islands region, across a wide range of topics. CTS enriches regional debate by collaborating with civil society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on. If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

ASPI

Tel Canberra: +61 2 6270 5100
Tel Washington DC: +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_CTS

First published October 2023.

ISSN 2209-9689 (online).
ISSN 2209-9670 (print).

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

Surveillance, privacy and agency

Insights from China

Daria Impiombato, Yvonne Lau and Luisa Gyhn

Policy Brief
Report No. 74/2023

Contents

Executive summary 3

Key findings 3

Introduction 4

Project details and methodology 6

Online survey 6

Media analysis 7

Research Platform 7

Comfort with surveillance 10

Latent class analysis 12

Receptivity to state messaging on surveillance 14

Conclusions and recommendations 20

Appendix 1: Survey questions and translations 21

Appendix 2: Breakdown of survey respondents 22

Notes 23

Acronyms and abbreviations 25

Executive summary

ASPI and a non-government research partner[1] conducted a year-long project designed to share detailed and accurate information on state surveillance in the People's Republic of China (PRC) and engage residents of the PRC on the issue of surveillance technology. A wide range of topics was covered, including how the party-state communicates on issues related to surveillance, as well as people's views on state surveillance, data privacy, facial recognition, DNA collection and data-management technologies.

The project's goals were to:

- improve our understanding of state surveillance in China and how it's communicated by the Chinese party-state
- develop a nuanced understanding of PRC residents' perceptions of surveillance technology and personal privacy, the concerns some have in regard to surveillance, and how those perceptions relate to trust in government
- explore the reach and potential of an interactive digital platform as an alternative educational and awareness-raising tool.

This unique project combined extensive preliminary research—including media analysis and an online survey of PRC residents—with data collected from an interactive online research platform deployed in mainland China. Media analysis drew on PRC state media to understand the ways in which the party-state communicates on issues of surveillance. The online survey collected opinions from 4,038 people living in mainland China, including about their trust in government and views on surveillance technologies. The interactive research platform offered PRC residents information on the types and capabilities of different surveillance technologies in use in five municipalities and regions in China. Presenting an analysis of more than 1,700 PRC Government procurement documents, it encouraged participants to engage with, critically evaluate and share their views on that information. The research platform engaged more than 55,000 PRC residents.

Data collection was led and conducted by the non-government research partner, and the data was then provided to ASPI for a joint analysis. The project details, including methodology, can be found on page 6.

Key findings

The results of this research project indicate the following:

- Project participants' views on surveillance and trust in the government vary markedly.
  - Segmentation analysis of survey responses suggests that respondents fall into seven distinct groups, which we have categorised as dissenters, disaffected, critics, possible sceptics, stability seekers, pragmatists and endorsers (the segmentation analysis is on page 12).
- In general, PRC state narratives about government surveillance and technology implementation appear to be at least partly effective.
  - Our analysis of PRC state media identified four main narratives to support the use of government surveillance:

        1. Surveillance helps to fight crime.
        2. The PRC's surveillance systems are some of the best in the world.
        3. Surveillance is commonplace internationally.
        4. Surveillance is a 'double-edged sword', and people should be concerned for their personal privacy when surveillance is handled by private companies.
    - Public opinion often aligns with state messaging that ties surveillance technologies to personal safety and security. For example, when presented with information about the number of surveillance cameras in their community today, a larger portion of Research Platform participants said they would prefer the same number (39%) or more cameras (38.4%).
    - PRC state narratives make a clear distinction between private and government surveillance, which suggests party-state efforts to 'manage' privacy concerns within acceptable political parameters.
- Project participants value privacy but hold mixed views on surveillance.
    - Participants expressed a preference for consent and active engagement on the issue of surveillance. For example, over 65% agreed that DNA samples should be collected from the general population only on a voluntary basis.
    - Participants are generally comfortable with the widespread use of certain types of surveillance, such as surveillance cameras; they're less comfortable with other forms of surveillance, such as DNA collection.

Introduction

It's important for non-government organisations, governments and human rights advocates combating the misuse of surveillance technologies to assess people's perceptions of those technologies, especially in the realms of privacy, freedom of expression, movement and assembly, and equal access to public services.[2] Gauging the perceptions of populations living with such technologies can support local and international advocacy efforts to improve online and privacy rights by better understanding local views on privacy, security and governance and by shaping effective messaging that raises awareness or resonates with existing concerns.

The threats that surveillance technology poses to human rights are on the rise globally. In August 2022, the UN Human Rights Council published a report on privacy in the digital age, highlighting the abuse of hacking tools, restrictions on encryption, and the extensive monitoring of public spaces, including online monitoring, as the three main areas of concern. Specifically citing freedom of expression and peaceful assembly, participation and democracy, the report stated:

> Systematic surveillance of people in the public space online and offline, in particular when combined with additional ways to analyse and connect the obtained information with other data sources, constitutes an interference with the right to privacy and can have highly detrimental effects on the enjoyment of other human rights.[3]

The Chinese Communist Party (CCP) operates a society-wide system of tech-enhanced authoritarian governance, facilitated by a sophisticated online censorship apparatus and internet-linked physical surveillance devices. In addition to online repression and surveillance, the PRC has become the world's primary case study of so-called 'techno-authoritarianism',[4] as the CCP increases its grip on power through an expanding and near-ubiquitous physical and digital surveillance apparatus. Chinese cities are covered by the highest number of CCTV surveillance cameras in the world.[5] Police agencies make intensive use of facial recognition to monitor human behaviour, link people's digital identities with their physical movements through specific devices, and collect DNA, voice prints and iris scans into large-scale databases. Efforts are underway to centralise and better analyse all the data collected.[6]

The surveillance apparatus now blankets the whole country, but there are differences in intensity and deployment between regions.[7] For example, the Xinjiang Uyghur Autonomous Region in western China has long been subject to party-state authorities' crackdowns aimed at repressing and culturally assimilating the local Muslim minorities. That has included a brutal arbitrary detention system[8] and the institution of a more intense surveillance system across the region.[9]

Surveillance has become integral to the way the party-state operates and governs. As surveillance and China experts Ausma Bernot and Susan Trevaskes put it, 'to lead everything, the Party needs to see everything.'[10] In their work, they highlight how ideology permeates all aspects of the PRC's tech-surveillance systems, and how increasingly, under PRC leader Xi Jinping, tech-enhanced (or 'smart') governance has become central to social, political and ideological control. Legislation and regulations that limit companies' use of surveillance frequently include loopholes that allow the government to use the technology in national- and public-security settings, with limited oversight from PRC citizens. This imbalance hurts transparency and accountability and deprives PRC citizens of avenues to push back against the government's misuse of technology.

Some Chinese legal experts and others *have* raised concerns about state surveillance.[11] However, the general lack of strong and independent media or a civil society free to investigate and critique government surveillance, as well as restrictions placed on researchers looking to explore these and other topics,[12] means that it's difficult to assess the impact of surveillance technology on people in China. It's highly unlikely that Chinese residents have access to comprehensive and detailed information on the surveillance technologies currently being deployed by the PRC Government, what they're used for, and, most importantly, what impact the expanding surveillance has on individuals.

The Chinese domestic information space is dominated by state media, the broader propaganda apparatus and affiliated, nationalist voices; therefore, much of the available information about state surveillance in the PRC reflects party narratives that stress the importance of surveillance for public security and social stability. Another noticeable trend in state narratives is the amplification and, at times, exaggeration of the government's technology capabilities, which gives an idealised depiction of the surveillance apparatus. This glorification of surveillance tech as the ultimate conduit to social stability serves the party-state as a constant reminder that people are being monitored at all times and promotes self-censorship.[13]

Project details and methodology

Obtaining reliable public-opinion data from mainland China is increasingly difficult, given the party-state's almost total control of information flows.[14] That makes it necessary to use alternative means to engage with the public in spaces that aren't fully censored and controlled. Deploying interactive online platforms is an emerging technique designed to surface opinions from the general population.

While China's huge population and local differences make it difficult to make any generalised assessment based on the datasets obtained, deployed platforms can nonetheless add to our understanding of the Chinese population's views on important and complex issues. For this project, an interactive digital platform provided PRC residents with an alternative pathway to express individual opinions on surveillance technologies, ultimately enabling direct information sharing with PRC residents and facilitating high levels of engagement. The Research Platform engaged more than 55,000 individuals over four months.

The data collection for this research project occurred through three mechanisms: first, an online survey to unpack the relationship between perceptions of surveillance and trust in government; second, a media analysis to understand how the party-state communicates on the implementation of its surveillance apparatus; and third, a Research Platform, which was a website designed to promote access to uncensored information about the capabilities and use of surveillance technologies in the PRC. This report conveys results from the media analysis, as well as survey respondents, and platform participants' perceptions of surveillance technologies, and it provides analysis of those perceptions.

In any context, public-opinion data comes with the caveat that participants might not respond completely truthfully to every question. That risk is higher in contexts in which expressing dissenting opinions carries personal risks, and perhaps even more so for a sensitive issue such as surveillance. Notwithstanding those limitations, which must be taken into consideration when examining our findings, this report furthers our understanding of the expansion of surveillance in the PRC, how the implementation of those technologies is communicated by the PRC Government, and what types of concerns those technologies raise.

Online survey

The online survey engaged 4,038 adults living in mainland China between 7 October and 2 November 2022. It was conducted through the Real-Time Interactive World-Wide Intelligence (RIWI) online survey tool.[15] The survey was distributed at the start of the project to assess the level of interest in and receptivity to information on surveillance and to inform strategies for effectively communicating research findings about the capabilities of surveillance technologies. The findings helped to shape the development of content for the Research Platform described below.

RIWI's survey methodology allows respondents to remain anonymous.[16] The data was weighted through 'raking'[17] to ensure that the sample matched China's demographic composition according to age and gender. Respondents were spread across a total of 28 provinces, administrative regions, autonomous regions and municipalities; however, the data wasn't weighted across geographical areas during the analysis. A breakdown of the survey respondents is provided in Appendix 2 at page 22. The survey's margin of error was +/– 1.54, with a degree of confidence of 95%.

Media analysis

As a complement to the findings from the online survey, the media analysis shed light on the way that surveillance is characterised in public discourse. In particular, the analysis identified common messages that PRC state media use to communicate and justify the use of surveillance technologies.

Using simplified Chinese Boolean search queries to examine publicly accessible content from a variety of Chinese sources, including Baidu, state media, blog sites and others, queries were initially informed by researching previously published reports on surveillance technology in China and were iteratively updated to remove irrelevant content on the basis of returned results.

The media analysis was conducted at the outset of the project over a 12-month period from 2021 to 2022. The goal of this activity was to inform our understanding of how state media currently describe the use of surveillance and to measure alignment between project participants' views and state narratives, as well as to develop content that addressed them. The analysis identified more than 4,000 mentions of surveillance, where 'mentions' refer to single articles, videos, press releases or posts—each of which may contain multiple or repeated uses of keywords. The mentions returned by the search queries were further categorised based on a list of keywords related to surveillance to identify common themes in the way that surveillance was described and discussed online. Using a qualitative approach, samples of state-media articles and videos as well as government press releases were selected from each category and analysed in greater detail to identify state narratives on the topic of surveillance.

The systematic and quantitative approach allowed for greater expediency in collecting a large dataset of public references to surveillance in the Chinese online landscape. That dataset was then unpacked by examining specific articles returned by each query. As a result, the findings provide an indication of common themes and patterns in the way that surveillance is presented in state media. These results should be considered in context with other studies that leverage similar approaches to develop a view of state narratives in China comprehensively. The results were used principally as a reference for comparing identified state messaging on surveillance with PRC residents' views on surveillance and privacy, derived both from the online survey and Research Platform data.

Research Platform

The Research Platform was an online interactive website that included five modules, each focusing on a different type of surveillance technology. Every module offered information on one of five surveillance technologies and was designed to encourage participants to engage with, critically evaluate and share their views on the information provided. To that end, every module included knowledge-testing and opinion questions, providing participants with the correct answers after they completed each question. The Research Platform also included infographics for users who wished to deepen their understanding of how surveillance technologies are purchased and deployed, and by which government actors.

Research Platform information was drawn from analysis of government procurement documents exclusively provided by *ChinaFile*, a digital magazine published by the Asia Society.[18] The documents consisted of more than 1,700 procurement notices related to surveillance technologies from central- and local-government offices across the country.

The PRC is an opaque system: understanding the actual surveillance technologies that are deployed and where they're deployed can often be difficult to differentiate from aspirational capability or propaganda. The large set of procurement documents offered a clear indication of some of the types of surveillance technologies that various levels of PRC government have intended to purchase and deploy. Our dataset primarily reflected technologies that were procured at the local rather than the central level.

To better understand the current reality of surveillance in local communities, research prioritised procurement notices awarded between 2012 and 2022 from five locations: Shanghai, Beijing, Guangdong,[19] Suzhou, and Hangzhou (Table 1).

Table 1: Number of procurement documents collected, by location and year

	Beijing	Shanghai	Guangdong	Suzhou	Hangzhou	Total
Notices	498	217	552	207	242	1,716
2012	0	3	0	0	38	41
2013	2	0	7	5	48	62
2014	2	3	2	9	21	37
2015	7	2	23	1	16	49
2016	16	16	29	14	13	88
2017	22	8	23	7	12	72
2018	93	29	45	17	25	209
2019	135	41	109	59	9	353
2020	107	62	142	48	25	384
2021	78	48	124	32	27	309
2022	32	4	48	3	7	94
Unspecified year	4	1	0	12	1	18

The number of procurement documents across the five locations shouldn't be directly compared. The locations have varying population sizes, so the amount of surveillance technology procured and the amount spent varied.

We note also that the sample included in this analysis is based only on publicly accessible documents, and that the figures and monetary amounts represent an unknown fraction of total spending on surveillance. Some procurement documents show joint procurement by different areas of government. Similarly, some notices procured multiple technologies at once. Therefore, the number of procuring agencies and the amount of technology procured exceed the number of procurement notices analysed for each location. Despite those limitations, a large procurement dataset offers a good indication of capability 'on the ground'.

Selection of the five technologies as the focal point for this analysis (Table 2) was based on preliminary research investigating findings from previous reports on the application of surveillance in China. The Research Platform therefore focused on providing information on—and seeking participants' views on—those five technologies.

Table 2: Five technologies analysed for this project

Surveillance technology	Description	Research findings
1. Facial recognition	Facial recognition is the ability to match a human face from a digital image or video to a database. PRC companies have widely developed this technology to successfully match faces that are obstructed with coverings (such as face masks) and to determine demographic information on the individual.	The analysis shows that facial-recognition cameras currently deployed have a range of capabilities, including: • accurate image capture, even when people are wearing hats, sunglasses, headphones or masks • tracking licence-plate information • determining the gender, age group and ethnicity of individuals captured by the camera.[20]
2. Wi-Fi probes	Wi-Fi probes, or 'sniffers', are used to track mobile devices and are able to access information from devices. They collect this information even if the device isn't connected to Wi-Fi through automatic Wi-Fi requests. Wi-Fi probes can collect device identification numbers (IMSI numbers) and have the potential to collect information about the apps and content on a device. Wi-Fi probes are often implemented alongside facial-recognition cameras.	For example, one of the notices we analysed requested more than 1,500 units of Wi-Fi probe technologies in Qingpu District in Shanghai alone.[21] The same notice also requested more than 16,000 units of high-definition surveillance cameras that are either fixed, remote-controlled, or mounted on a mobile vehicle or a drone. It suggests the capturing of both physical and digital tracks for more comprehensive surveillance or, as the procurement document titles it, creating a 'city image surveillance system'.[22]
3. DNA surveillance	DNA surveillance is the general collection, storage and use of genomic data from a large sample of the population. DNA collected from an individual has potential implications for them and their extended family.	Most of the notices related to DNA testing and analysis in Guangdong, for example, are issued by public-security bureaus across the province. Research on DNA-collection policies suggests that DNA samples are often collected from the general public without people's informed consent. A previous ASPI report found no evidence that Chinese authorities sought people's consent prior to collecting DNA samples, and that people who gave their samples are unlikely to understand how that may subject them and their families to greater state surveillance.[23] Citizens often have very little information about why their DNA is collected, where it will be stored, and how it will be used.[24] Notices from Guangdong related to DNA collection and analysis reveal how the PRC Government is expanding biometric surveillance. Often, those notices referenced the creation of DNA databases. One notice stated that DNA samples from across Guangdong would contribute to a 'national DNA library' of genetic information on ordinary citizens.[25]

4. Database management	Database management is the collection of various surveillance data into one location for public-security purposes. For example, data from public and private locations such as residential complexes may be connected with the local public-security bureau's big-data system. Apart from the information obtained via the technologies mentioned in this table, other data, such as entry and exit records and facial-recognition photos, is shared with the precinct's facial-recognition database for secondary analysis. Street offices have issued procurement documents for database management, which indicates that the local districts are connecting and integrating information into the police system.	One of the records from Suzhou, for example, suggests that data gathered from entry gates in residential areas needs to be seamlessly connected with the local public-security bureau's big-data system.[26] This includes facial-recognition photos, entry and exit records, and warnings that can be shared automatically with the precinct's facial-recognition big-data platform for secondary analysis.[27] The specific procurement notice was issued by a street office (街道办事处), which suggests that local districts are connecting and integrating information about ordinary citizens' daily lives into the police system.
5. Surveillance cameras	Surveillance cameras are video cameras with the purpose of observing a geographical area. They can be fixed, remote-controlled or mounted on a mobile vehicle or a drone. Feeds from surveillance cameras are often connected to a database that combines other surveillance data and contains analysis capabilities such as facial-recognition technology.	Records from Hangzhou, for example, suggest that there's a growing level of surveillance on university and college campuses through a project called 'Safe Campus' (平安校园).[28] This effort seems to be led by public-security bureaus in addition to educational institutions, which is notably different from our analysis of other cities, where the educational institutions procured their own surveillance equipment. Records from Hangzhou also suggest that the government expands surveillance systems in the lead-up to major events. A procurement notice issued prior to the G20 Summit in 2016, for example, states that 'surveillance at ethnic and religious venues relates to the safety of the summit'.[29]

This information was then provided to Research Platform participants, explaining use cases and capabilities of the key surveillance technologies in use across the PRC. The platform was made available on the Chinese internet. Over four months, more than 55,000 individuals from mainland China interacted with the platform, and more than 32,000 completed either one or multiple modules.[30]

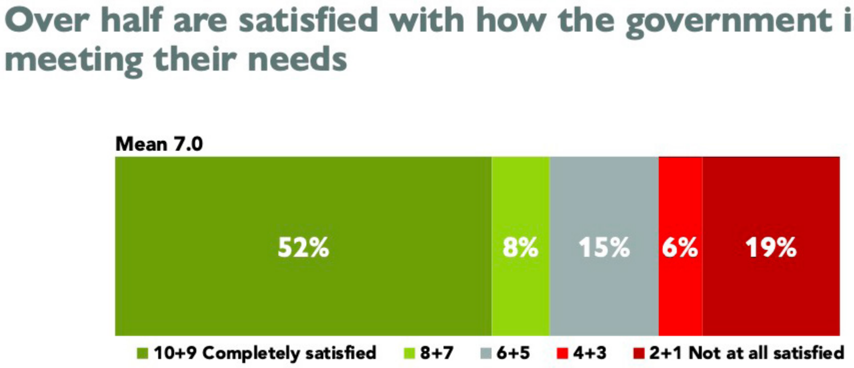
To ensure both the security of participants and ongoing research opportunities, the exact methodology for distributing the Research Platform to participants isn't explained in this report. We note that the distribution method is effective but has inherent limitations for which it can be difficult to control, such as limited means to scale and promote engagement through diverse digital channels. Furthermore, participation on the platform appeared to be skewed towards young, male and highly educated respondents—the most active internet-using population in the country.

Comfort with surveillance

The survey asked respondents about different forms of video surveillance, facial-recognition systems, audio recording devices in public spaces, internet and social-media monitoring, and other more generic questions. Selected questions are featured below and in Appendix 1.

Our findings show that most respondents ranked the government's performance favourably. On whether respondents felt that the government was meeting their needs, on a scale from 1 (least satisfied) to 10 (most satisfied), 60% of respondents gave a positive answer at 7 and above, 15% stayed neutral at 6–5, and 25% gave a more negative answer of under 5 (Figure 1).

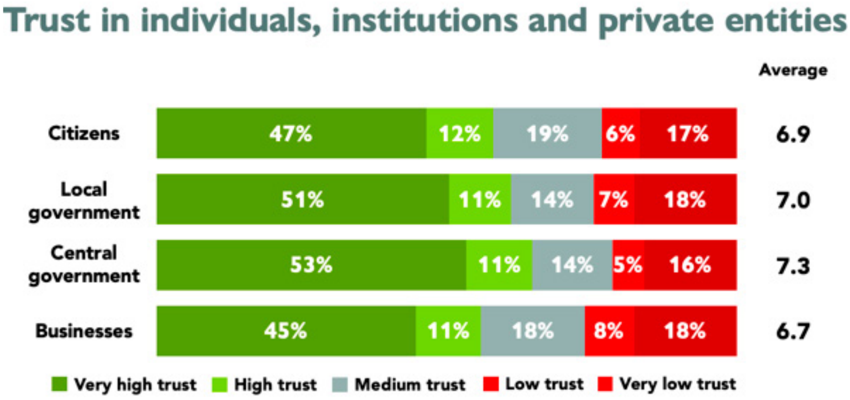
Figure 1: Online survey results: 'How satisfied are you with how the government is meeting your needs these days? On the scale of 1 to 10 below, 1 means not satisfied at all and 10 means completely satisfied.'



Source: ASPI's non-government research partner.

Respondents were also asked to rate their trust in different levels of government, as well as in citizens and private entities, ranging from very low trust to very high trust. The results indicate a comparatively higher degree of trust in the central government (Figure 2). This is consistent with earlier surveys with larger respondent groups.[31]

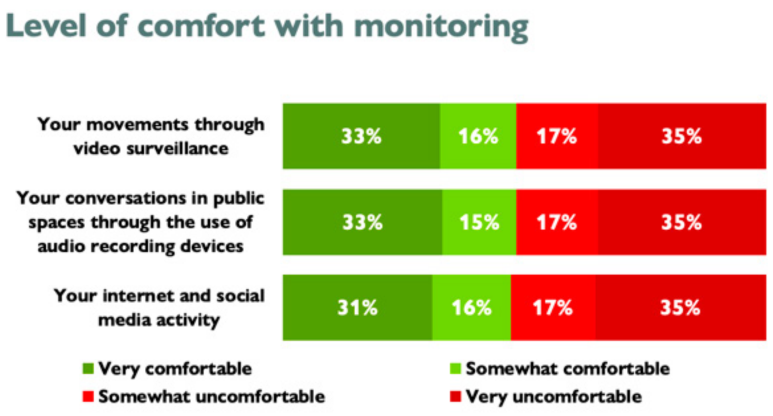
Figure 2: Online survey results: 'Using a point scale where 1 is no trust and 10 is a very high level of trust, how much do you trust the following?'



Source: ASPI's non-government research partner.

Views on surveillance, however, are more split (Figure 3). Just over half of respondents expressed discomfort about being monitored (52%). That level of discomfort was constant across three different types of monitoring: video surveillance; audio recording devices in public spaces; and internet and social-media activity. Those three forms of monitoring were selected to provide an insight into respondents' level of comfort with more traditional forms of surveillance, such as video, compared to what could be perceived as more intrusive, such as audio, and compared to surveillance in the digital space. Ultimately, the data showed that levels of comfort are consistent across all three.

Figure 3: ‘How comfortable are you with the government monitoring the following?’



Source: ASPI’s non-government research partner.

To describe how trust in the government and attitudes towards surveillance interact, a segmentation analysis was conducted using latent class analysis (LCA). LCA identifies latent subgroups within a sample based on a set of variables (see box). The purpose of this analysis was to develop more effective messaging systems by better understanding the different nuances of public opinion on this issue and avoiding homogenous and stereotyped assessments. This helped to finetune the approach to public education on surveillance more effectively.

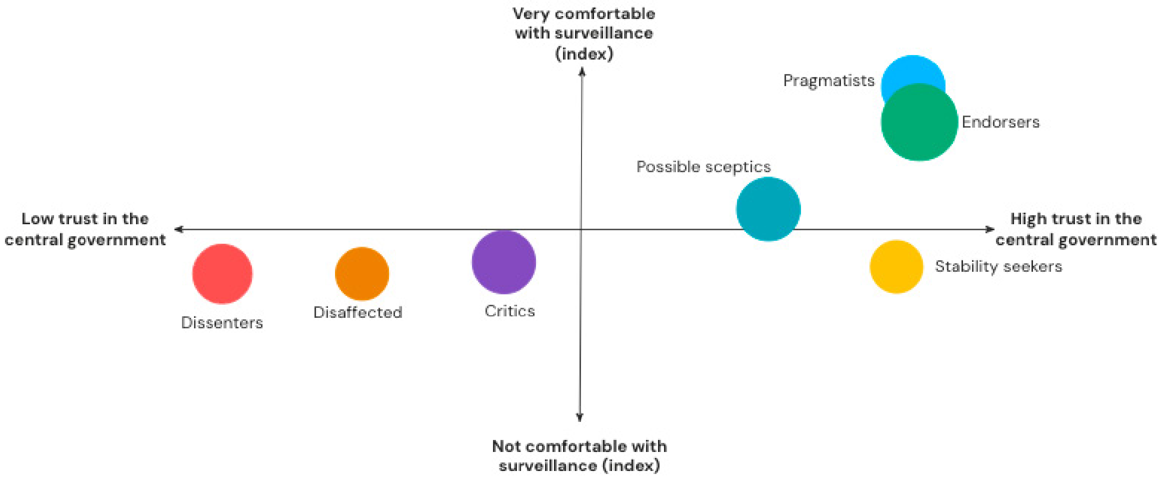
Latent class analysis

For this analysis, responses from all survey questions were included, producing a set of seven distinct groups of respondents. The characteristics of each group and the proportion of the sample represented are outlined here and are shown in Figure 4.

- *Dissenters* (13%): With very low government-satisfaction and trust scores, this group fundamentally mistrusts the government. These participants have a low level of comfort with surveillance; they notice it often and want limits imposed on government surveillance. Anger and anxiety are the top emotions expressed by this group about surveillance.
- *Disaffected* (9%): This group has lower-than-average trust and satisfaction levels. Government surveillance primarily provokes anxiety, but this group doesn’t notice surveillance as much as the Dissenters do. They aren’t sure whether the government has the capacity to monitor them everywhere, and whether there should be limits on government surveillance. Their expectations for the future of the economy are low.
- *Critics* (15%): With moderately low trust and satisfaction, this group shares much in common with the Disaffected and Dissenters. Their comfort with surveillance is low. While not likely to notice surveillance, they think there should be limits to government surveillance. Compared to the Dissenters, they downplay the government’s capacity to surveil but acknowledge the potential for inappropriate use of surveillance.
- *Possible sceptics* (15%): Participants in this group share a generally positive view of the state and are middle of the road when it comes to comfort with surveillance. They don’t really notice surveillance and generally say that government surveillance makes them feel safe or that they have mixed feelings about it.

- *Stability seekers* (10%): Like Endorsers and Pragmatists, Stability seekers have a high level of trust in, and satisfaction with, the central government. What distinguishes them is a lack of comfort with surveillance and an awareness of its ubiquity. This group recognises that surveillance is sometimes used inappropriately but values order and social stability. This group has the most positive expectations for the economy.
- *Pragmatists* (15%): Pragmatists are mostly comfortable with surveillance but approach the question with low levels of engagement. Most of them don't have an opinion on whether there are, or should be, limits to government surveillance. In fact, this group is the least likely to notice surveillance and doesn't think it's used inappropriately. Despite their high levels of support for the central government, participants in this group value personal privacy over social stability.
- *Endorsers* (23%): Endorsers are the most comfortable with surveillance and have the highest level of trust in the central government. 'Safe' is the top word that comes to mind when they think about government surveillance. Many (42% above average) think that there are already limits on government surveillance and generally agree that there should be limits. The group places a very high value on social stability, as opposed to personal privacy.

Figure 4: Comfort with surveillance and trust in government



Source: ASPI's non-government research partner.

This analysis indicates that, while trust in the central government and comfort with surveillance are strongly correlated, there are other dimensions that should be considered to construct an informed assessment of public perspectives in China. For example, some of the respondents who declared the highest level of trust in the central government and comfort with surveillance also hold values that contradict government narratives about surveillance, such as expressing a strong preference for personal privacy over public order. By contrast, there are also respondents who express distrust towards the government but are more likely to value public order over personal privacy.

Receptivity to state messaging on surveillance

As part of this project, the research team analysed articles in PRC state media to understand how the implementation of surveillance is communicated to the public. The analysis resulted in the identification of four common messages:

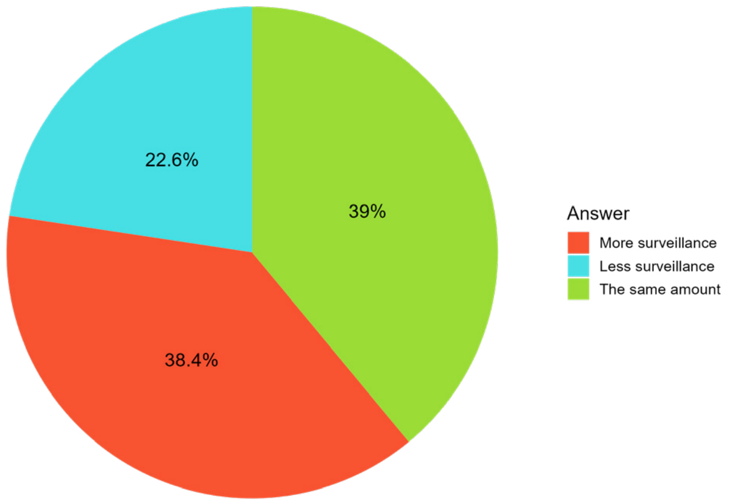
1. Surveillance helps to fight crime.[32]
2. The PRC's surveillance system is one of the best in the world.[33]
3. Surveillance is commonplace internationally.[34]
4. Surveillance is a 'double-edged sword', and people should be concerned for their personal privacy when surveillance is handled by private companies.[35]

On the last point, state-media articles that acknowledge citizens' concerns often also draw attention to the protections embedded in current privacy-protection legislation and the government's desire to better regulate vendor and platform data management.[36] Those points are accompanied by a reinforcement of citizens' complaints against the private sector's handling of data.[37]

At the same time, issues and concerns related to the collection, storage and handling of large datasets, including hacks and leaks (an example being the hacking of police databases in 2022), are often censored.[38] If concerns about companies are amplified, while those about the government are censored, that creates the impression that the public supports measures taken by the government to surveil the population for security purposes while being sceptical of private companies. This narrative positions 'the state and citizens on the same side of the privacy battle against private companies',[39] providing a 'legitimate' outlet for concerns about surveillance.

Data collected over the course of this project indicates that state narratives have been at least partly effective in generating public acceptance of the use of surveillance and trust in the central government as the implementer of those technologies. When asked to reflect on the prevalence of surveillance cameras in their community, a larger portion of Research Platform participants would prefer there to be the same number (39.0%) or more (38.4%). A smaller, but substantial, portion (22.6%) supported having less surveillance (Figure 5).

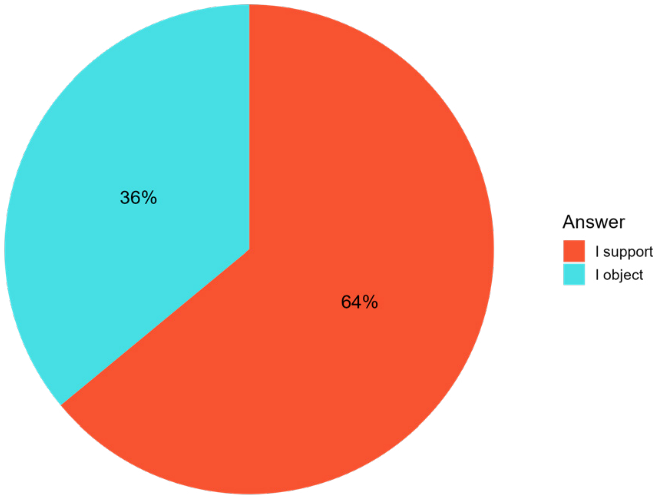
Figure 5: Research Platform results: 'Thinking about the number of surveillance cameras in your community today. Ideally, would you prefer for your community to have less surveillance, the same amount, or more surveillance?'



Note: Numbers rounded for clarity.
Source: ASPI.

Research Platform results also suggest that participants largely have a positive perception of social credit systems (SCSs).[40] Sixty-four percent of respondents said they would support rewarding and punishing citizens' behaviour through an SCS (Figure 6). We didn't ask the respondents their reason for supporting SCSs; nor did we give more specificity about the different types of SCSs and their purposes. However, one hypothesis that could explain the strong support is that respondents see tangible benefits in implementing the system, such as institutionalisation and social stability, and that the government has effectively communicated social credit via cultural and moral concepts, as well as Confucian norms that are strongly rooted in the Chinese society and therefore more easily accepted.[41]

Figure 6: Research Platform results: 'Do you support rewarding and punishing citizens' behaviour through a social credit system?'



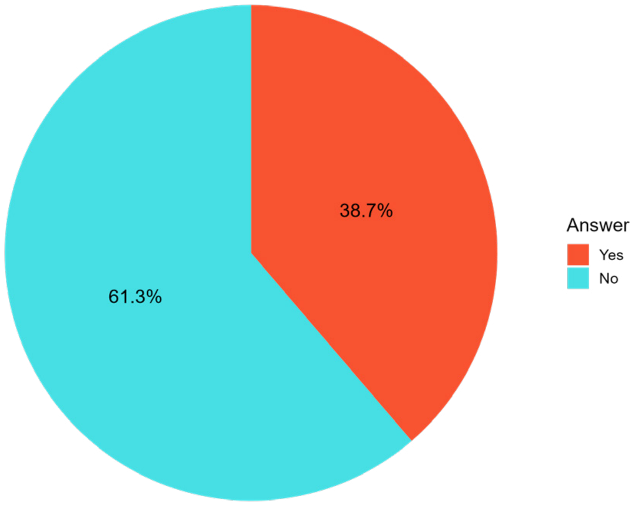
Note: Numbers rounded for clarity.
Source: ASPI.

Personal agency and privacy

Facial-recognition technologies

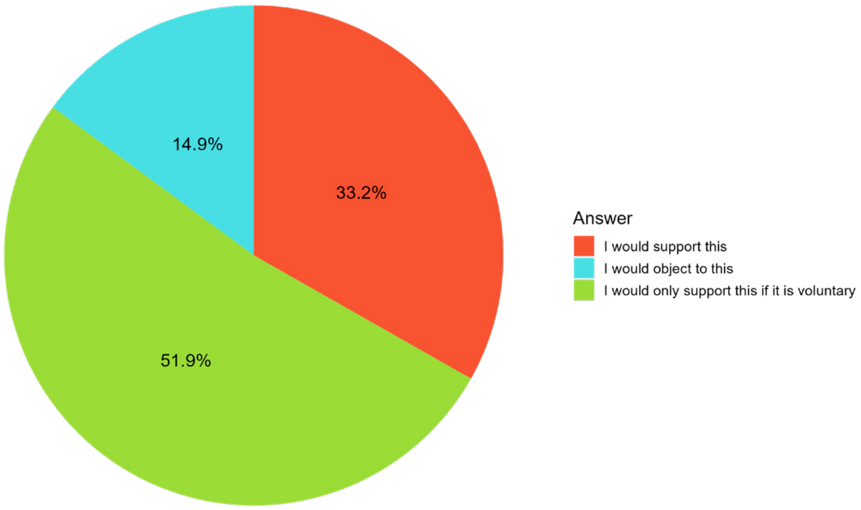
While there's broad support among Research Platform participants for the government to use surveillance, participants hold nuanced views that demonstrate preferences for privacy-preserving policies. When asked about whether facial-recognition technology (FRT) surveillance systems should be allowed to automatically record information such as age, gender or ethnicity, the majority (61.3%) said 'no' (Figure 7). A large number of participants also had concerns regarding the implementation of FRT at their apartment complexes: just over half (51.9%) support this only if it's voluntary (Figure 8). This suggests that PRC residents aren't passive participants in FRT systems and prefer to have a choice to opt out.

Figure 7: Research Platform results: 'Should facial recognition surveillance systems be allowed to automatically record information like age, gender, or ethnicity?'



Note: Numbers rounded for clarity.
Source: ASPI.

Figure 8: Research Platform results: 'How would you feel about the local public security office implementing facial recognition technology at your apartment complex?'



Note: Numbers rounded for clarity.
Source: ASPI.

These findings are particularly noteworthy, considering that there are already laws and regulations that supposedly give the public more control over their biometric information. The 2021 Personal Information Protection Law states that 'separate consent is required when processing sensitive personal information', and that there should be protection rules and standards for 'sensitive personal information processing, and new technologies and applications such as face recognition and artificial intelligence'.[42]

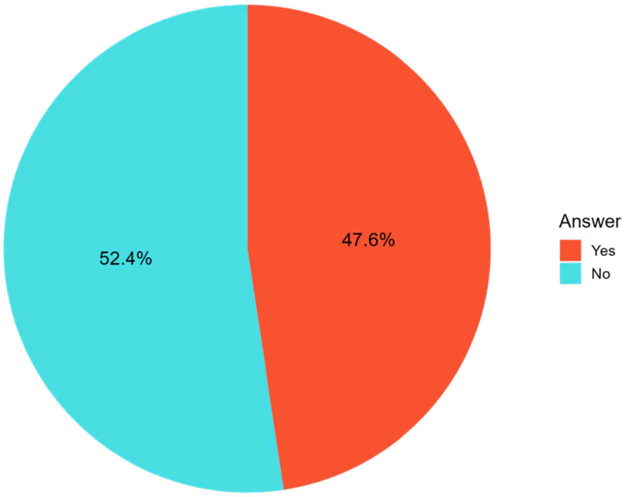
More recently, the draft rules on FRT released by the Cyberspace Administration of China in August 2023 appear to provide individuals with more rights to opt out.[43] According to the draft rules, FRT would require individual approval or written consent. The draft rules also state that, in cases in which non-biometric identification solutions are equally effective, they should be favoured over facial recognition.[44] The proposed measures would also stop organisations or individuals from creating profiles based on attributes such as 'race, ethnic group, religion, health, social class, or other sensitive information', except when 'protecting national security, public security, or in other emergency situations'.[45]

This new draft law highlights how most regulations apply predominantly to the private use of surveillance technology, and that loopholes are included for the government to use the technology in national- and public-security settings with limited oversight from PRC citizens. That imbalance hurts transparency and accountability and deprives PRC citizens of avenues to push back against the government's misuse of technology.

DNA collection

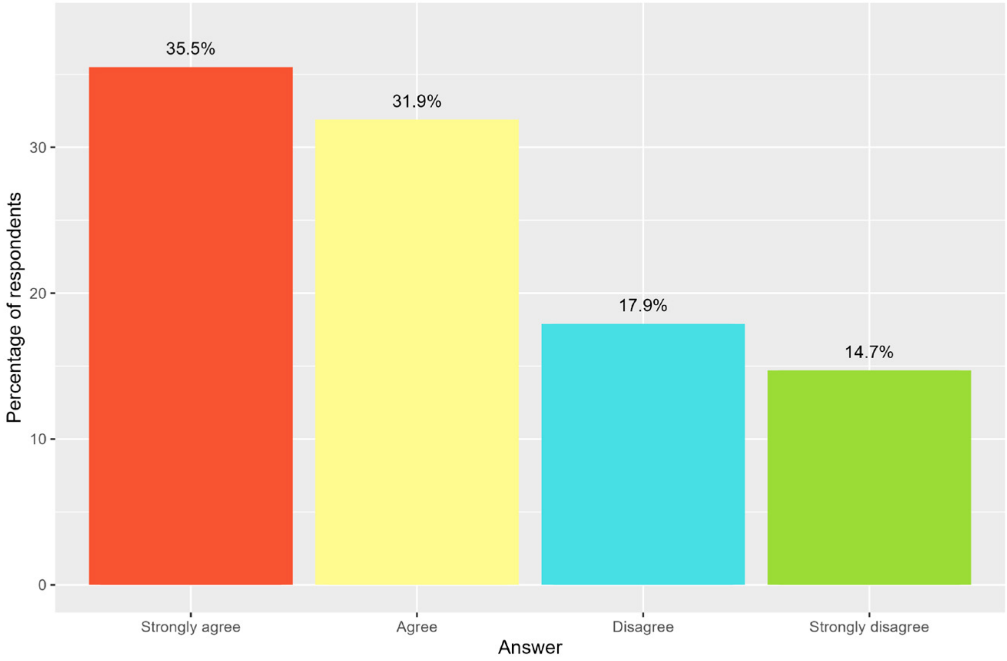
Participants are less comfortable about having their DNA information collected and stored compared to the application of other types of surveillance. While the split is almost even between participants feeling comfortable with the government collecting and storing DNA information about them or their families (Figure 9), a majority (67.4%) agree that DNA samples should be collected from the general population only on a voluntary basis (Figure 10). Uncertainty about DNA technology, the invasive nature of DNA collection and the lack of any visible or immediate personal benefits associated with DNA testing—as opposed to the 'security dividend' that a security camera might be seen to provide, for example—may explain the less welcoming responses regarding its collection.

Figure 9: Research Platform results: 'Would you be comfortable with the government collecting and storing DNA information about you or people in your family?'



Note: Numbers rounded for clarity.
Source: ASPI.

Figure 10: Research Platform results: 'Do you agree with the statement "DNA samples should only be collected from the general population on a voluntary basis. People should have the choice to not participate."'

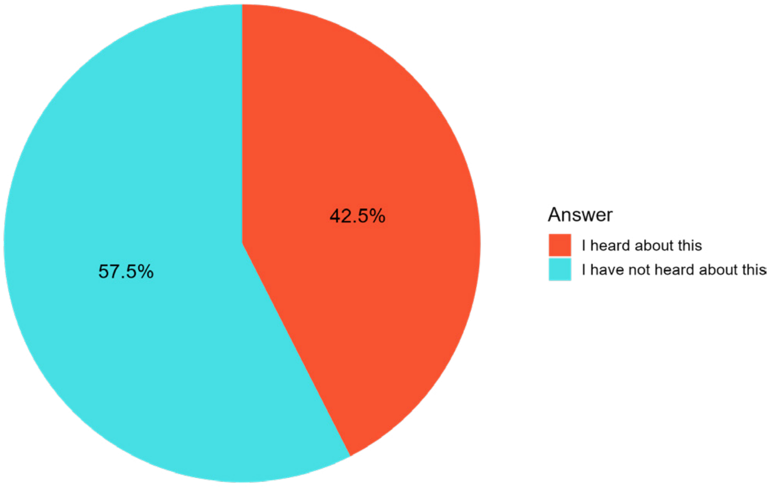


Note: Numbers rounded for clarity.
Source: ASPI.

Data management

In addition to showing preferences for personal agency related to the use of FRT and DNA collection, project data shows that participants have concerns about the security of their personal information and digital privacy. Over half of the Research Platform participants (57.5%) hadn't heard of the July 2022 hack into the Shanghai police database that contained the personal information of more than 1 billion PRC citizens (Figure 11).[46] One reason may be that the participants haven't had access to the news due to heavy government censorship.

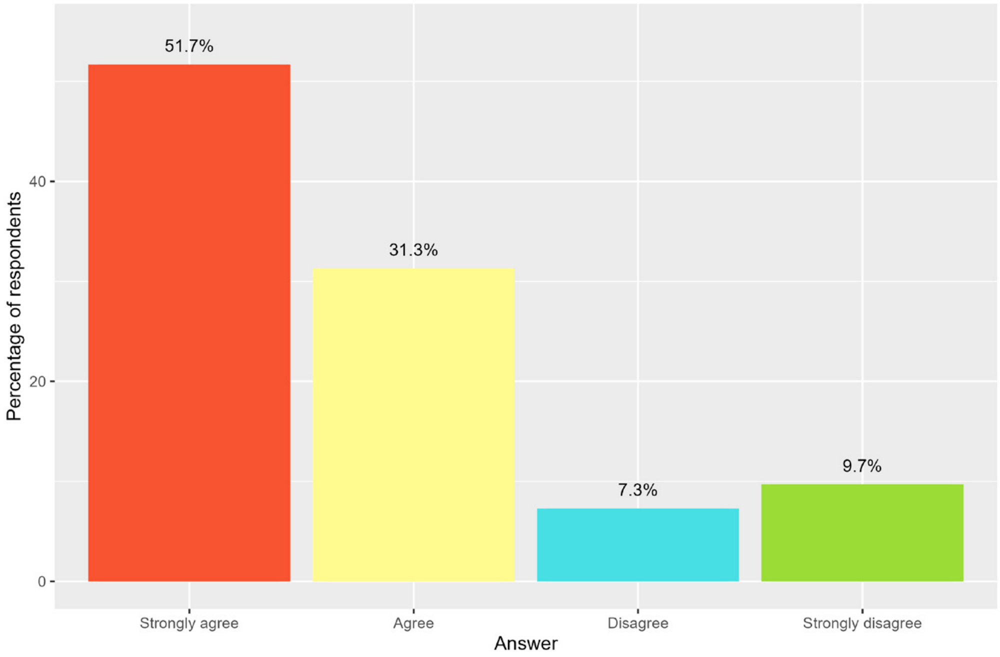
Figure 11: Research Platform results: 'Have you heard about the hacker claiming on an online forum to have gained access to a Shanghai police database containing the personal information of more than 1 billion PRC citizens?'



Note: Numbers rounded for clarity.
Source: ASPI.

When asked whether the government should have a duty to inform the public when data leaks involving personal information happen, an overwhelming majority (83%) agreed (Figure 12).

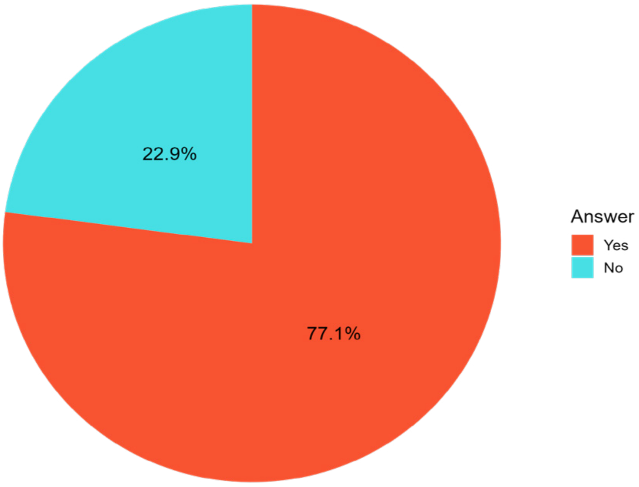
Figure 12: Research Platform results: 'Do you agree that the government should have a duty to inform the public when data leaks involving personal information happen?'



Note: Numbers rounded for clarity.
Source: ASPI.

A question on whether PRC citizens should have the option to remain anonymous on social media also resulted in the majority of participants answering 'yes' (Figure 13). These findings run counter to China's strict real-name registration policies, implemented in 2012. Those policies mandate that all internet users in China register using their real names and personal identification details, with the aim of increasing online surveillance capabilities, maintaining government control over information and addressing social unrest. However, those measures have sparked significant debate within Chinese society, centring around concerns related to free speech, privacy and law enforcement.[47]

Figure 13: 'Should you have the option to remain anonymous online?'



Note: Numbers rounded for clarity.
Source: ASPI.

Conclusions and recommendations

Project results indicate that, although the party-state's messaging on surveillance has been largely effective in persuading PRC residents to accept the widespread use of certain types of surveillance technology, most would still prefer the option to consent to surveillance rather than be passively subjected to it. Equally, although participants strongly support the idea of an SCS that punishes or rewards citizen behaviours, most also have concerns about the arbitrary collection of personal information, and they're particularly uncomfortable with the collection of DNA. Support for an SCS doesn't preclude a desire for greater online privacy, including the option to remain anonymous on social media.

Together, the data collected over the course of the project generated new insights on:

- PRC residents' perceptions of surveillance technologies and privacy
- the complexity of public opinion on policy issues such as surveillance, and the importance of examining how trust and values help to shape the diversity of perspectives in the country
- the ways in which the PRC Government differentiates between state and private surveillance, and how that's received by residents.

Leveraging the lessons learned from this project, similar approaches could be applied and expanded on in the future in order to:

- explore where and how PRC residents access news and information, including news or information from outside China, and how that information resonates with different target audiences
- support human-rights research and education, particularly in other closed and closing online information spaces, through novel empirical methods to collect data
- develop engaging education campaigns on other human-rights issues, such as health care or gender equality.

Appendix 1: Survey questions and translations

Question	English translation	Simplified Chinese
Q 1	How satisfied are you with how the government is meeting your needs these days?	您觉得政府能够满足您近来的需要吗？
	1 (not at all satisfied)	1 完全不满意
	10 (completely satisfied)	10 完全满意
Q 2	What is your level of trust towards the following groups? Citizens	请问您对以下群体的信任程度? 普通群众
	1 (no trust)	1 毫不信任
	10 (complete trust)	10 非常信任
Q 3	What is your level of trust towards the following groups? Local government	请问您对以下群体的信任程度? 地方政府
	1 (no trust)	1 毫不信任
	10 (complete trust)	10 非常信任
Q 4	What is your level of trust towards the following groups? Central government	请问您对以下群体的信任程度? 中央政府
	1 (no trust)	1 毫不信任
	10 (complete trust)	10 非常信任
Q 5	What is your level of trust towards the following groups? Businesses	请问您对以下群体的信任程度? 商家
	1 (no trust)	1 毫不信任
	10 (complete trust)	10 非常信任
Q 6	How comfortable are you with the government monitoring the following: Your movements through video surveillance	请问您放心政府采取以下行为吗 通过视频监控追踪你的行踪
	Very uncomfortable	非常不放心
	Somewhat uncomfortable	有些不放心
	Somewhat comfortable	大体放心
	Very comfortable	非常放心
Q 7	How comfortable are you with the government monitoring the following: Your conversations in public spaces through the use of audio recording devices	请问您放心政府采取以下行为吗 通过录音设备监听你在公共场合的对话
	Very uncomfortable	非常不放心
	Somewhat uncomfortable	有些不放心
	Somewhat comfortable	大体放心
	Very comfortable	非常放心
Q 8	How comfortable are you with the government monitoring the following: Your internet and social media activity	请问您放心政府采取以下行为吗 监控你在网络和社交媒体上的个人行为
	Very uncomfortable	非常不放心
	Somewhat uncomfortable	有些不放心
	Somewhat comfortable	大体放心
	Very comfortable	非常放心

Appendix 2: Breakdown of survey respondents

Region	Number of respondents	Percentage of sample
Anhui	125	3.10%
Beijing	221	5.47%
Chongqing	74	1.83%
Fujian	78	1.93%
Gansu	38	0.94%
Guangdong	629	15.58%
Guangxi	105	2.60%
Guizhou	29	0.72%
Hainan	14	0.35%
Hebei	170	4.21%
Heilongjiang	53	1.31%
Henan	350	8.67%
Hubei	78	1.93%
Hunan	119	2.95%
Jiangsu	342	8.47%
Jiangxi	106	2.63%
Jilin	44	1.09%
Liaoning	95	2.35%
Ningxia Hui Autonomous Region	11	0.27%
Qinghai	9	0.22%
Shaanxi	98	2.43%
Shandong	303	7.50%
Shanghai	136	3.37%
Shanxi	77	1.91%
Sichuan	130	3.22%
Tianjin	75	1.86%
Yunnan	76	1.88%
Zhejiang	247	6.12%
Not disclosed	206	5.10%
Total	**4,038**	**100.00%**

Gender	Number of respondents	Percentage of sample
Female	800	19.81%
Male	3,238	80.19%
Total	**4,038**	**100.00%**

Age group	Number of respondents	Percentage of sample
18–24	1,515	37.52%
25–34	1,461	36.18%
35–44	638	15.80%
45–54	173	4.28%
55–64	83	2.06%
65 and over	168	4.16%
Total	**4,038**	**100.00%**

Notes

[1] ASPI supported this project with an undisclosed research partner. That institution remains undisclosed to preserve its access to specific research techniques and data and to protect its staff.

[2] ‘The right to privacy in the digital age’, Office of the UN High Commissioner for Human Rights, 4 August 2022, online; Joss Wright, Valentin Weber, Gregory Finn Walton, ‘Identifying potential emerging human rights implications in Chinese smart cities via machine-learning aided patent analysis’, *Internet Policy Review*, 28 July 2023, 12(3), online.

[3] ‘The right to privacy in the digital age’, UN Human Rights Commission, 7 October 2022, online.

[4] Samantha Hoffman, ‘China’s tech-enhanced authoritarianism’, testimony before the Congressional Executive Commission on China, 17 November 2021; Samantha Hoffman, *Engineering global consent: the Chinese Communist Party’s data-driven power expansion*, ASPI, Canberra, 14 October 2019, online.

[5] Paul Bischoff, ‘Surveillance camera statistics: which cities have the most CCTV cameras?’, *Comparitech*, 23 May 2023, online.

[6] Isabelle Qian, Muyi Xiao, Paul Mozur, Alexander Cardia, ‘Four takeaways from a Times investigation into China’s expanding surveillance state’, *The New York Times*, 21 June 2022, online.

[7] Josh Chin, Liza Lin, *Surveillance state: inside China’s quest to launch a new era of social control*, St Martin’s Press, 2022.

[8] *The Xinjiang Data Project*, ASPI, Canberra, online.

[9] Darrey Byler, *In the camps: life in China’s high-tech penal colony*, Atlantic Books, London, 2022, online; Lindsay Maizland, China’s repression of Uyghurs in Xinjiang, Council on Foreign Relations, 22 September 2022, online.

[10] Ausma Bernot, Susan Trevaskes, ‘Smart governance, smarter surveillance’, in *China Story yearbook 2021: Contradiction*, Australian Centre for China in the World, online; Susan Trevaskes, Ausma Bernot, ‘Surveillance infrastructure in China: key concepts and mechanisms enhancing the party-state’s governance ambitions’, *Global Media and China*, September 2023, 8(3):327–342, online.

[11] For examples, see ‘Be alert to the risk of information leakage in the era of “facial recognition”’ [警惕“刷脸”时代的信息泄露风险], Yulin Internet Police [榆林网警], 3 July 2023, online; Yan Shi [石晏], ‘Preventing facial recognition from being misused, new regulations proposed to push for stricter controls’ [防止人脸识别被滥用 新规拟推严监管举措], *China Securities Journal* [中国证券网], 10 August 2023, online; Yi Ni [倪弋], ‘Regulate the application of facial recognition and guard personal information security’ [规范人脸识别应用，护航个人信息安全], *People’s Daily* [人民日报], 21 June 2023, online; ‘The age of information technology: monitoring system network faces security risks’ [信息化时代 监控系统网络化面临的安全隐患], China Security and Protection Industry Association [中国安全防范产品行业协会], 3 July 2019, online.

[12] Dyani Lewis, ‘China’s souped-up data privacy laws deter researchers’, *Nature*, 25 May 2023, online.

[13] Paul Mozur, ‘Inside China’s dystopian dreams: AI, shame and lots of cameras’, *The New York Times*, 8 July 2018, online.

[14] Melanie Manion, ‘Survey research in the study of contemporary China: learning from local samples’, *The China Quarterly*, 1994, 139, online.

[15] Real-Time Interactive World-Wide Intelligence (RIWI), online.

[16] ‘Privacy policy’, RIWI, 23 January 2023, online.

[17] Raking is a method that assigns a proportional weight value to each survey respondent to align the sample distribution with a control variable (that is, population age or gender).

[18] *ChinaFile*, online.

[19] The researchers analysed Guangdong as a province rather than the city of Guangzhou as there was no intention for the procurement data across the regions to be directly compared. The primary goal was to be transparent about where the information on the platform came from, rather than to conduct a comparison of the procurement of surveillance technology across the locations.

[20] Procurement data provided by ChinaFile and verified by ASPI.

[21] Procurement data provided by ChinaFile and verified by ASPI.

[22] Procurement data provided by ChinaFile and verified by ASPI.

[23] Emile Dirks and James Leibold, ‘Genomic surveillance’, ASPI, 17 June 2020, online.

[24] Emile Dirks and James Leibold, ‘Genomic surveillance’, ASPI, 17 June 2020, online.

[25] Procurement data provided by ChinaFile and verified by ASPI.

[26] Procurement data provided by ChinaFile and verified by ASPI.

[27] Procurement data provided by ChinaFile and verified by ASPI.

[28] ‘Hangzhou Normal University: Smart security, smart-safe campus platform construction’ [杭州师范大学：智慧安防，智安校园平台建设], National University Ideological and Political Work Net [全国高校思想政治工作网], 28 December 2022, online.

[29] Procurement data provided by ChinaFile and verified by ASPI.

30 Participants in the Research Platform weren't told that responses would be used in a research report. They were told that participation is anonymous; that the site was created by a team of experts supporting communities around the world to gain access to reliable information; that participation is intended for audiences 18+; that we record depersonalised information to understand aggregate usage of the site (such as what users click on, responses to questions, and other metrics of site functionality); and that users are encouraged to be cautious when sharing the site or information about the site online.

31 Cary Wu, Zilei Shi, Rima Wilkes et al., 'Chinese citizen satisfaction with government performance during COVID-19', *Journal of Contemporary China*, 2021, 30(132):930–944, online.

32 For examples, see Xin He [何欣], 'High-tech bracelets monitor suspects' [高科技手环监控犯罪嫌疑人], *Xinhua News* [新华网], 8 October 2017, online; Litao Nie [聂立涛], 'German media: China strengthens smart surveillance to reduce crime, cameras and robots in action' [德媒:中国加强智能监控减少犯罪 摄像头机器人齐上阵], *Xinhua News* [新华网], 18 May 2016, online.

33 For an example, see Shixian Chen [陈诗娴], Zhen Li [李贞], 'What is "Skynet"?' ["天网"网什么], *People's Daily* [人民日报], 2017, online.

34 For an example, see 'Fallacies and truths in America's perception of China' [美国对华认知中的谬误和事实真相], Ministry of Foreign Affairs of the PRC [外交部], 19 June 2022, online.

35 For an example, see Xiaonan Ye [叶晓楠], 'Surveillance cameras are a "double-edged sword"' [摄像头是把"双刃剑"], *People's Daily* [人民日报], 15 August 2013, online.

36 For example, see Shunwan Zhan [詹顺婉], 'More than 60% of consumers complain that their personal information has been misused', *www.gog.cn* [多彩贵州网], 29 May 2017, online.

37 Countless histories [千万历史], 'A second thought incurs profound fear, data breach will affect everyone' [细思极恐，滴滴数据泄露将危害我们每一个人], *Zhihu* [知乎], 25 October 2022, online; '20% of internet users encountered personal information leakage, how to rectify the data security "disaster areas"?' [两成网民遭遇个人信息泄露，如何整治数据安全"重灾区"？], *Xinhuanet* [新华网], 29 March 2022, online; 'Student information leakage is not only in Renmin University of China, you can buy 200 pieces for as low as 1 yuan online' [学生信息泄露不只在中国人民大学，网上最低1元就能买到200条], CCTV [央视新闻], 7 July 2023, online.

38 For example, see Ryan McMorrow, Gloria Li, 'China censors news of alleged hacking of Shanghai police database', *Financial Times*, 5 July 2022, online.

39 Zeyi Yang, 'The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect', *MIT Technology Review*, 10 October 2022, online.

40 China's SCSs extend beyond traditional financial creditworthiness and regulatory compliance. They also embrace a broader concept of trust, or 'social creditworthiness', and collect data from more sectors. They comprise three components: public, corporate and personal credit systems. The public systems aim to regulate the government's administrative and economic activities. The market-centred corporate credit systems rely on data from banks and financial institutions. The personal credit systems, established by various national and local authorities, monitor legal violations and generate credit scores for residents based on day-to-day social activities. For more detail, see Zeyi Yang, 'The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect'; 'Law of the People's Republic of China on the Construction of Social Credit System' [中华人民共和国社会信用体系建设法], National Development and Reform Commission [国家发展改革委], 14 November 2022, online; Drew Donnelly, 'China social credit system explained—what is it & how does it work?', *Horizons*, 6 April 2023, online; Jessica Reilly, Muyao Lyu, Megan Robertson, 'China's social credit system: speculation vs. reality', *The Diplomat*, 30 March 2021, online; Frank Tang, 'China pushing ahead with controversial corporate social credit rating system for 33 million firms', *South China Morning Post*, 17 September 2019, online; Alexander Trauth-Goik, Chuncheng Liu, 'Black or fifty shades of grey? The power and limits of the social credit blacklist system in China', *Journal of Contemporary China*, 30 September 2022, 32(144):1017–1033, online.

41 Alexander Trauth-Goik, *'Constructing a culture of honesty and integrity': the evolution of China's Han-centric surveillance system*, University of Wollongong, 5 December 2019, online.

42 Standing Committee of the National People's Congress of the PRC [全国人民代表大会常务委员会], 'The Personal Information Protection Law of the People's Republic of China' [中华人民共和国个人信息保护法], Ministry of National Defense of the PRC [中华人民共和国国防部], 20 August 2021, online.

43 Rita Liao, 'China's draft measures demand "individual consent" for facial recognition use', *TechCrunch*, 8 August 2023, online.

44 Josh Ye, 'China drafts rules for using facial recognition technology', *Reuters*, 8 August 2023, online.

45 Office of the Central Cyberspace Affairs Commission [中央网络安全和信息化委员会办公室], 'Notice of the Cyberspace Administration of China regarding the public consultation on the regulations for security management of the application of facial recognition technology (for trial implementation) (draft for comments)' [国家互联网信息办公室关于《人脸识别技术应用安全管理规定（试行）（征求意见稿）》公开征求意见的通知], Cyberspace Administration of China [中国网信网], 8 August 2023, online.

46 John Liu, Paul Mozur, Kalley Huang, 'In a big potential breach, a hacker offers to sell a Chinese police database', *The New York Times*, 5 July 2022, online.

[47] ‘Decision of the Standing Committee of the National People’s Congress on strengthening the protection of network information’ [全国人大常委会关于加强网络信息保护的决定], Central People’s Government of the PRC [中华人民共和国中央人民政府], 28 December 2012, online; Jyh-An Lee, Ching-Yi Liu, ‘Real-name registration rules and the fading digital anonymity in China’, *Washington International Law Journal*, 21 January 2016, online; Catherine Shu, ‘China doubles down on real-name registration laws, forbidding anonymous online posts’, *TechCrunch*, 28 August 2017, online; Tracy Qu, ‘China updates rules on real-name registration online in crackdown on schemes to revive banned user accounts’, *South China Morning Post*, 27 October 2021, online.

Acronyms and abbreviations

CCP	Chinese Communist Party
CCTV	closed-circuit television
DNA	deoxyribonucleic acid
FRT	facial-recognition technology
LCA	latent class analysis
PRC	People’s Republic of China
RIWI	Real-Time Interactive World-Wide Intelligence
SCS	social credit system
UN	United Nations