Q & A

Josh Chin & Liza Lin on How China Developed its 'All-Seeing' Surveillance State

The journalists and authors talk about what sets China's use of surveillance tech apart from other countries; how the building blocks of that tech came from the West; and how the surveillance state can be both seductive and terrifying.

BY DAVID BARBOZA — SEPTEMBER 25, 2022

Josh Chin and Liza Lin are distinguished foreign correspondents at The Wall Street Journal and the co-authors of a new book that examines China's use of technology to strengthen its authoritarian system. The book, Surveillance State: Inside China's Quest to Launch a New Era of Social Control, has been greeted with wide acclaim. Chin, who is based in Taipei, is the deputy bureau chief of The Wall Street Journal's China bureau. He is a recipient of the Dan Bolles Medal and was part of an investigative team with Lin that won the Gerald Loeb Award for international reporting in 2018. Lin covers Asia technology news for The Wall Street Journal. She was part of a team that was a finalist for the Pulitzer Prize in 2021. What follows is a lightly edited transcript of my interview with them prior to the book's release.

Josh Chin.
Illustration by Ellie Foreman-Peck

Q: Josh, Liza, what a terrific book you've written on China and its surveillance state, a book that brings us to this Orwellian state of tracking, tracing and control. Can you tell us how this book came about?

A: **Josh:** The book is based on an investigative series that Liza and I led for *The Wall Street Journal* in 2017. Liza was covering startups at the time, and she had run across this company called SenseTime,[1] which was raising a lot of money. It had developed this world leading facial recognition software and was selling it to police departments all over China. So we went to their showroom and it was like something out of "Minority Report." It was just totally mind blowing. But this was real, and it was being used in places like Chongqing. So we got back to *The Journal*'s bureau [in Beijing], and we said: "We've got to write this up." That was the first story in the series. Then we spent the rest of the year digging into stories about state surveillance. And what was really surprising was the extent to which the Communist Party had gone all-in on these technologies. It was working with big tech companies and startups to develop and put them into practice.

Liza, how would you describe it?

Liza: It essentially started in a very *Wall Street Journal* style: I was following the money, and there was a ton of money going to AI. And it was going into one particular aspect of AI, which was facial recognition. So when SenseTime invited us to their office it was quite jarring. Employees were using facial recognition to verify their identity before they even got inside [the office]. And this was back in 2017. Inside the SenseTime[2] building, there was a huge screen that took up the entire wall and it showed a street scene just outside of their office. Several cameras were mounted on the intersection of a road, and every pedestrian, car or bicycle that went by, were all [digitally] boxed up [on the screen] with labels like 'red shirt' or 'green Toyota', with the car's make and model. When we talked with them, they said their technologies were being bought by social media companies. But then they said, "The biggest implication of our technology is that it's being bought by public security bureaus. We're helping catch these bad people in Chongqing or in Hangzhou." That's when it hit us that it was a much bigger story than we expected.

So what started with a look at SenseTime, which has since been placed on the U.S. government's Entity List, eventually shifted to Xinjiang and the efforts to use surveillance equipment to monitor ethnic minorities there and in other regions. Is that right?
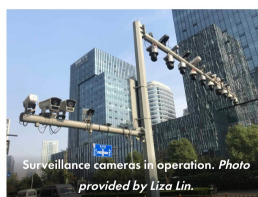
JOSH CHIN: BIO AT A GLANCE

AGE	45
BIRTHPLACE	Salt Lake City, Utah
CURRENT POSITION	Deputy China bureau chief at *The Wall Street Journal*
SPOUSE	Gillian Wong

Josh: So in the latter half of 2017, we'd done the first story [in the WSJ] on facial recognition, and we were looking at other stories. And at that time, there had been a few reports trickling out of Xinjiang about the [re-education] camps. Back then, everyone was just referring to them as schools. No one quite knew what they were, or what was going on. One of our editors in Hong Kong had a buddy who had traveled to Xinjiang and came back talking about all the security checkpoints with iris scanners and other new technology. The editor mentioned this to us and immediately our ears pricked up. We were like, "Well, that sounds kind of familiar" — and so we decided to go there. I went with a videographer from the Journal. We rented a car because we figured we might be picked up at the airport by surveillance. We drove in from Gansu Province. And as soon as we drove across the border, it was like being in a kind of dystopian, high-tech war zone. It was so clear that whatever was happening in Xinjiang was totally new, and kind of terrifying. I think BuzzFeed beat us to the punch actually — we have to give her [journalist Megha Rajagopalan] proper respect there. But BuzzFeed's story came out, and then we came out with our story. And that was the beginning of making that connection between the surveillance and the re-education efforts.

Liza Lin at The Great Hall of the People, Beijing. *Photo provided by Liza Lin.*

Surveillance cameras in operation. *Photo provided by Liza Lin.*

A family walking away from a re-education camp in Turpan, Xinjiang, in 2018. *Photo provided by Josh Chin.*

For those who don't really know, how do you describe this so-called surveillance state?

Liza: The surveillance state in China now is all-seeing in the sense that if you do something wrong, it would be very easy for the Communist Party to retrace your steps, figure out who you are, and figure out what you're buying on Taobao or elsewhere. It's all-seeing in a retrospective sense. In Xinjiang, there's a lot of predictive policing and instantaneous terrorism alerts, but I don't think that's uniformly rolled out across the country.

A monitor of a computer at an inspection point showing a database with photos and other information about residents in Kashgarin, Xinjiang, June 28, 2018. *Credit: Yomiuri Shimbun via [AP Images](#)*

How does the country do it? And who aids in the development of these sophisticated systems?

Liza: I can start with the technology companies. So they [the authorities] have access to the Chinese technology companies' data. Think about the technology titans, such as Alibaba and Tencent. With a very easy-to-get police warrant, the authorities can go up to a tech company and say, "We suspect this person of being involved with terrorism or some crime against national security. Give me this person's data." In some senses, it's not that different from the West because, obviously, for Google or Facebook, law enforcement officers could go to these companies and get the data. The difference in China is the ease with which the public security officers can get that data. In a place like the U.S., you would need a court or a judge to sign off on that before the police can come to the company and say, "We want information about this person because of a crime." In China, however, the sign-off only needs to come from a senior police officer. This is the frictionless nature of getting that warrant. So they have what Alibaba and Tencent have access to: a range of things that you can buy, what you purchase on social, what you purchase on ecommerce, who your contacts are, what you're saying to your contacts, where you are; then they'd have the home address of this person, the office address. That's a lot of data already. And then you go into the CCTV [closed circuit television] cameras, of which China has probably about half a million across the country at this stage. Not all of them are enabled with AI, but all of them are recording video, which can be used to retrace your steps.

LIZA LIN: BIO AT A GLANCE	
AGE	38
BIRTHPLACE	Singapore
CURRENT POSITION	China Correspondent at *The Wall Street Journal*
MARITAL STATUS	Married

" **What the Communist Party ultimately wants to do is use these**

technologies to shape behavior; to sort of engineer society in ways that can ultimately serve the Communist Party's goals.

"

— Josh Chin

Josh: There's the commercial data, what the tech companies have. Also, the telecom companies are state-owned, so they can trace your location by your SIM card. They also have all your data that a government normally has, your ID, your photos.

Urumqi population data collection form. *Provided by Josh Chin.*

And in places like Xinjiang, actually in huge swaths of China, they are collecting DNA: they have one of the world's largest DNA databases. In some cases, they're collecting voice data, so they can identify you through phone calls. If they don't know who you're calling they can pick a sample of your voice and identify a person that way. Obviously, fingerprints, as well. They even have gait recognition, so they can match you by how you walk.

How do China's capabilities compare with the rest of the world? Are they ahead in technology, or just implementation?

Josh: By far, the most sophisticated uses of surveillance technology have been developed by American companies. Silicon Valley invented behavioral data analytics. They invented technologies for collecting massive amounts of data and using it in predictive ways. The difference in China is the surveillance and the use of that data by the state. It's being melded with power in a way that's vastly more comprehensive than anywhere else in the world. Countries like Israel, for example, use quite a bit of fairly sophisticated surveillance technology to track Palestinians. But it doesn't match the scale of use in China, or the ambition. In Israel, the aim is to track Palestinians, who are potentially a threat, and it's very security driven. In China, security is just one piece of it. What the Communist Party ultimately wants to do is use these technologies to shape behavior; to sort of engineer society in ways that can ultimately serve the Communist Party's goals. Nowhere else is even remotely close to that kind of ambition.

Liza: What really stands out as well is the concentration of all that data in the hands of one entity. Because in the U.S., you have a lot of data collection, but it's being collected by different entities, like corporations or the government. But in China, the Communist Party has almost unfettered access to all the data, including corporate data.

How did the Party's thinking about this data evolve over time? It was fascinating to read in your book the roots of some of this surveillance state ideology. Can you talk about that a little?

Josh: This idea of using data and surveillance to control and engineer society has been floating around in China for decades. It was the missile scientists like Qian Xuesen, in the '80s, who brought up this idea. At the time, it was not really technologically possible. But it was always there, the idea of seeing societies as an engineering problem. And what happened is around the time that Xi Jinping was coming to power, we had a series of events that crystallized for the Communist Party how important it was to grasp technology and control technology, and turn it to their own ends.
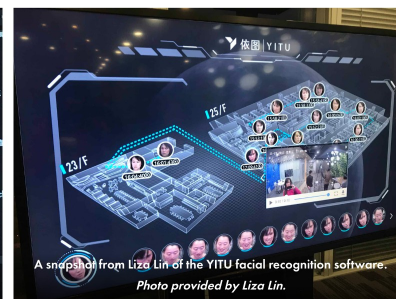
One of the most remarkable of these events was the Wenzhou train crash, a high speed train crash in 2011, where the Communist Party just completely lost control of the narrative. They were overwhelmed online by all this commentary, with people using the train as a metaphor for Chinese society running out of control. We talked to officials and government advisors who were involved in some of these discussions. The Communist Party decided right around that time that they needed to take the initiative with technology, to make technology work for them, rather than against them. And a couple of years later you started to see these huge advances in AI and in machine learning applications like facial recognition started to develop capabilities that made it possible.

Liza: You also saw the evolution of Internet Protocol cameras, which allowed [the authorities] to link up entire CCTV systems. In the past, each camera would only be able to record its footage to a server. With internet protocol cameras, you enable deep learning and machine learning AI, which in turn enables facial recognition and all these other applications, making the surveillance state much more of a reality than a dream for the Chinese Communist Party.

Josh Chin testing a mood analytics system at a Security Expo in Beijing, 2018. *Photo provided by Josh Chin.*

A snapshot from Liza Lin of the YITU facial recognition software. *Photo provided by Liza Lin.*

Is this home-grown technology or did China import these technologies from the U.S. or other countries?

Liza: This was probably one of the most interesting parts of the research because we realized how much of the fundamentals and building blocks of the Chinese surveillance state came from the West. And it's everything from lower-tech stuff, such as databases or hard disk drives, to the high-end stuff like cutting edge chips that allow you to run facial recognition or other sorts of deep learning applications at a very fast speed.

Click here to read Eliot Chen's Big Picture on the key concepts in the semiconductor supply chain.

It wasn't just a supply chain relationship; it was also a financial relationship. In 2018, Josh and I were analyzing a list of 37 Chinese companies that were recognized by the Chinese Security and Protection Industry Association for doing breakthrough work in "Safe Cities." And out of that list, about 50 percent of those companies had some sort of supply chain

relationship to American companies. And these were big names, ranging from Qualcomm to Japan's Softbank to Silver Lake [the U.S. investment firm].

How did you find this information on the role of American or western technology companies?

Liza: We went through hundreds of government contracts to see what was in the makeup of the Chinese surveillance state. And we realized that people were asking for hard disk drives, and they were asking for certain types of hard disk drives. They're asking for those made by Seagate, for example, or Western Digital. And that's because Seagate, Western Digital and Toshiba effectively control most of the low-end hard disk drive market globally. And they would be very specific in what they were looking for, such as a certain Intel chip, or an Nvidia chip. And we found that many American companies were actively marketing their chips to public security.

A large number of Chinese firms have been put on the U.S. Entity List and they have been restricted in purchasing equipment or technology from American firms. Has this been effective?

Liza: It's hard to tell because the supply chain by its very nature is so murky. And that's the defense that the companies tend to always pull out: "It's very hard for us to figure out who our end user is when there are so many uses for our chips." In the case of SenseTime — and I know this because they listed last year and they spoke about it — it says one of its entities was put on the [U.S.] Entity List. So that means that American companies can't sell to that one Beijing entity, but there are others entities that
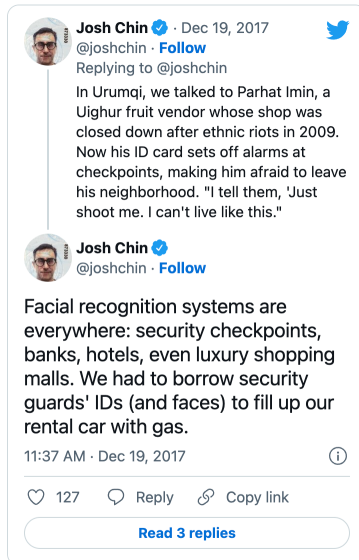

Ceremony marking SenseTime's listing on the Hong Kong Stock Exchange, December 30, 2022. *Credit: SenseTime*

they can sell to. So yes, these companies have been put on the Entity List, but there are workarounds.

So is this ineffective, or is there another reason to target them?

Liza: With sanctions, the U.S. is sending a very clear political message: What's happening in Xinjiang is not right, and we don't support it. The Entity List in particular was used in the Trump era. Prior to that, it wasn't used for human rights purposes. But in the Trump era, it was repurposed to make certain political points or to drive home certain political messages and also to hit out against human rights abuses in China.

You're both reporters for *The Wall Street Journal* in a country that is increasingly uncomfortable with western journalists and scrutiny of what is happening in Xinjiang. How closely were you surveilled while working on this book?

Josh: The most obvious experience came in Xinjiang, when we were still reporting for *The Wall Street Journal*. I was driving with my colleague on a stretch of desert where we had gotten lost. We were trying to find our way back to the highway. We were on this dirt road in the middle of nowhere and all of a sudden we were surrounded by this cloud of dust. And when the dust settled, we realized that we were trapped on either side by police cars, and these guys with guns. And they gestured for us to get out and interrogated us about who we were and where we were going. We asked how they had spotted us since we were in the middle of nowhere, and they said, "Our cameras picked you up, and sent us an alert about where you were." So that was my first introduction to what it's like to be targeted by these technologies.

The difficulty with that is that you never know exactly how the state knows what it knows. Sometimes, a source will get visited by police after you talk to them. It could have been they were tapping the interviewees' phones, someone might have seen us and informed on us. In some ways, that's kind of the point: you never actually know. All you know is that someone is watching somewhere or could be watching somewhere. And the intent is to get you to regulate your own behavior just based on that fear.

> **Your entire life can basically be arranged through an app, and you don't think about it as surveillance, but that's the result of surveillance. It's invisible, and intentionally invisible.**

— *Josh Chin*

China has clearly shown that it's capable of rolling this out in a remarkable and chilling way to police and control its own citizens in an authoritarian state. But does it export these technologies or capabilities to the rest of the world?

Josh: It's absolutely exportable and it is being exported. There's a scholar at the University of Texas named Sheena Greitens, who back in 2020 did a survey and found that there are so-called Safe City systems made by Chinese companies. These are basically state surveillance systems that have been sold to police departments or government agencies in 80 countries around the world, on every continent except for Antarctica and Australia.

So it's definitely being exported, especially to countries along the Belt and Road and in the Global South, countries that China wants to bring into its orbit economically. The Chinese government acts as a sort of auxiliary salesman for companies like Huawei or ZTE. The one example we have in the book to illustrate this is Uganda, where Huawei had been calling the Ugandan president, Yoweri Museveni, for years. And in 2018, Chinese diplomats basically arranged for a bunch of Ugandan police to fly out to China. Part of the purpose was to visit Huawei headquarters. But then they also visited Chinese security services in Beijing and learned directly from Chinese police how they use these surveillance systems. So the government is very much marketing these systems abroad.

Yoweri K Museveni visiting a part of Uganda's National CCTV System, at the Police Headquarters in Naguru, Kampala. November 28, 2019. *Credit: Yoweri K Museveni via [Twitter](https://twitter.com)*
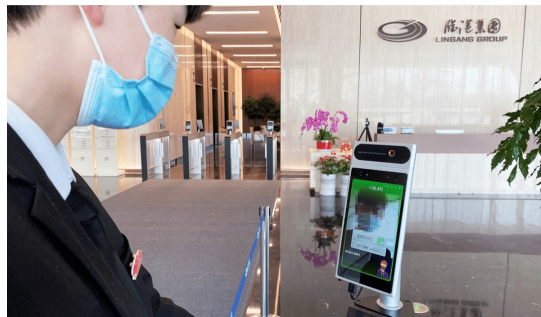
What you describe in the book sounds like a nightmare if you're used to the freedoms we take for granted in the West. But what does it feel like on the ground in China, or for ordinary Chinese?

Josh: When we started off, it was very hard to find anyone in China outside of Xinjiang who really had much of an opinion about surveillance. Most people didn't really notice it, or they didn't think about it. And to the extent that they did think about it, they didn't find it problematic. But as we were writing the book, we started to notice that better educated urban residents were starting to get something of a privacy movement boiling up; but it was very focused on company collection of user data. And the Communist Party was very good at channeling that growing interest in privacy towards companies. So there was never really a question in China about whether the government has a right to use this data, and whether that's a good or a bad thing.

Companies are very much facing backlash over their use of data. But for most people it's sort of working in the background to make life easier and more convenient. You know, anyone who lived in China in the '90s or early 2000s would remember having to stand in the line of a bank to pay your electricity bill and sit there for an hour just to pay this bill. It was just such a pain. And now, everything can be done on WeChat. Your entire life can basically be arranged through an app, and you don't think about it as surveillance, but that's the result of surveillance. It's invisible, and intentionally invisible.

But wasn't this surveillance state enhanced during COVID, and in fact made all the more powerful in what would seem like a good cause — mass surveillance to defeat the spread of a deadly virus?

Liza: For the most part, we felt that COVID was a victory for the Communist Party in terms of its use of surveillance to keep things under control. In this case the enemy is different; a terrorist may be very easy to track but but with a pandemic you have a virus that leaves no tracks; it's much more

infectious and harder to stop. It's like an invisible enemy. But in spite of those challenges, China managed to keep Covid deaths very low. The last time I checked the Johns Hopkins University of Medicine database, looking at the deaths per 100,000 population in China, it's just one death per 100,000. In the U.S., the corresponding number is 315. So even using general estimates and stats, you would still say that COVID was in a sense a victory for the Chinese surveillance state. And I think Chinese citizens also thought so, because a lot of the people we spoke to said that they were willing to give up some sense of privacy or some data in exchange for not getting infected with COVID.

But haven't the COVID lockdowns also exposed the limits of this system, or perhaps the brutality that can come from it? We've seen very harsh lockdowns across China, people even running from buildings to avoid lockdowns. And people are starting to resent the surveillance, right?
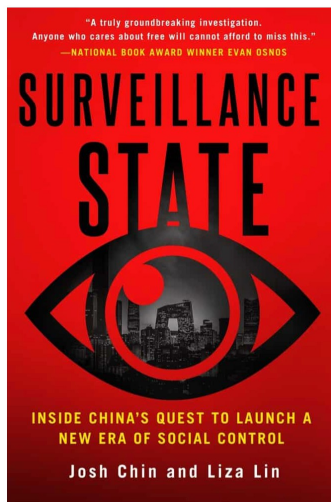
Josh: The lockdowns have really crystallized the difficulty with state surveillance. People in Shanghai were certainly upset, anxious and angry about being locked down. And understandably because a lot of them couldn't get food; it was incredibly scary. Certainly people in Shanghai now have a different opinion about state surveillance. But one of the takeaways from the lockdowns that I've had is that it really does give the Communist Party the tools to exert control. The government can feel confident that in an entire city, even in one the size of Shanghai, they could keep people locked up.

> **" … state surveillance can be very seductive, or it can be very terrifying, depending on who you are and where you are. "**
>
> *— Liza Lin*

Liza: The lockdowns showed the limitations of state surveillance when dealing with a virus. State surveillance is extremely useful in the early stages, when your transmission chains are still stoppable, and when you're doing contact tracing, and you're figuring out who might carry the virus; then you can isolate the person. But in a lot of the lockdowns we saw this year, the transmission chain had gone out of control. And by then state surveillance could do nothing to stop it. You had to resort to a physical lockdown. So it does illustrate this limitation on state surveillance.

Have you come to some conclusions about the development of China's surveillance state? What do you want readers to take away from this marvelous book?

Josh Chin and Liza Lin's *Surveillance State: Inside China's Quest to Launch a New Era of Social Control,* published September 6, 2022. Credit: **Macmillan**

Josh: One of the conclusions we came away with is that these technologies that the Chinese companies are using have the potential to reinforce authoritarianism in really meaningful ways, that will challenge democracy going forward. And one of the tasks for democracies is to figure out exactly what their position is on these technologies and how they want to deal with them because it's inevitable: facial recognition and predictive policing are already being used in the United States. A lot of democracies have not come to terms with that in a serious way. There's a tendency, especially in the United States, to just wave it away as all bad. But that doesn't seriously wrestle with the costs and benefits of this technology. And as long as democracies do that, sort of wave it away, it can give space for the technology to be melded with authoritarianism in ways that could really change the landscape of human governance.

Liza: My takeaway is that state surveillance can be very seductive, or it can be very terrifying, depending on who you are and where you are. And that was really what we tried to aim for in the book. Because in Xinjiang, it is really awful that a million people could be interned or incarcerated because an algorithm said that they might be a danger to the state. And on the flip side, we tried to go down to the very wealthy city of Hangzhou to show that data collection does have its benefits, it can actually help ease up traffic jams, send the friction out of daily life or can help health care workers and ambulances get to an accident scene faster. So there are these trade offs between data privacy, national security and convenience that everyone has to go through and decide.

David Barboza is the co-founder and a staff writer at The Wire. Previously, he was a longtime business reporter and foreign correspondent at The New York Times. @DavidBarboza2

● COVER STORY

Seed Savior?

BY ISABELLA BORSHOFF

Agrichemical giant Syngenta is unique on the world stage: it is a state-owned Chinese firm with an American CEO. After ChemChina's historic purchase of the company in 2017 — the largest ever purchase by a Chinese company overseas — Syngenta is now ready for its big China debut with a planned blockbuster IPO in Shanghai this fall. But while "modernizing" farming

● THE BIG PICTURE

Wingtech Takes Flight

BY ELIOT CHEN

A look at the low-end smartphone maker: its rapid growth, its evolving business and its investors.

● NEWS AND ANALYSIS

China Goes Nuclear

BY ISABELLA BORSHOFF

China is poised to be a leader in next generation nuclear power.

debut with a planned blockbuster IPO in Shanghai this fall. But while "modernizing" farming in China has been good for Syngenta's business, helping Beijing achieve its long-sought after goal of food self sufficiency will be more complicated feat.

News Products

Visit News Products Store

Our best open-source research on Chinese companies, as well as industry guides to 100 of the most influential people in a China-focused industry.

The Wire China Archives   Read More Articles ›

The Wire *China*

Your account

About Us   Archives   Contact Us