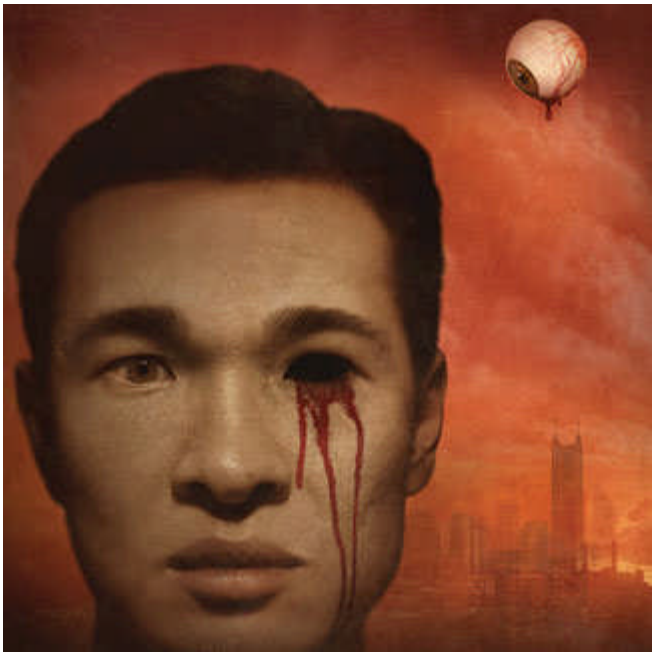
China's All-Seeing Eye

With the help of U.S. defense contractors, China is building the prototype for a high-tech police state. It is ready for export.



NAOMI KLEIN

ROLLING STONE MAGAZINE

May 29, 2008

Thirty years ago, the city of Shenzhen didn't exist. Back in those days, it was a string of small fishing villages and collectively run rice paddies, a place of rutted dirt roads and traditional temples. That was before the Communist Party chose it — thanks to its location close to Hong Kong's port — to be China's first "special economic zone," one of only four areas where capitalism would be permitted on a trial basis. The theory behind the experiment was that the "real" China would keep its socialist soul intact while profiting from the private-sector jobs and industrial development created in Shenzhen. The result was a city of pure commerce, undiluted by history or rooted culture — the crack cocaine of capitalism. It was a force so addictive to investors that the Shenzhen experiment quickly expanded, swallowing not just the surrounding Pearl River Delta, which now houses roughly 100,000 factories, but much of the rest of the country as well. Today, Shenzhen is a city of 12.4 million people, and there is a good chance that at least half of everything you own was made here: iPods, laptops, sneakers, flatscreen TVs, cellphones, jeans, maybe your desk chair, possibly your car and almost certainly your printer. Hundreds of luxury condominiums tower over the city; many are more than 40 stories high, topped with three-story penthouses. Newer neighborhoods like Keji Yuan are packed with ostentatiously modern corporate campuses and decadent shopping malls. Rem Koolhaas, Prada's favorite architect, is building a stock exchange in Shenzhen that looks like it floats — a design intended, he says, to "suggest and

illustrate the process of the market." A still-under-construction superlight subway will soon connect it all at high speed; every car has multiple TV screens broadcasting over a Wi-Fi network. At night, the entire city lights up like a pimped-out Hummer, with each five-star hotel and office tower competing over who can put on the best light show.

Many of the big American players have set up shop in Shenzhen, but they look singularly unimpressive next to their Chinese competitors. The research complex for China's telecom giant Huawei, for instance, is so large that it has its own highway exit, while its workers ride home on their own bus line. Pressed up against Shenzhen's disco shopping centers, Wal-Mart superstores — of which there are nine in the city — look like dreary corner stores. (China almost seems to be mocking us: "You call *that* a superstore?") McDonald's and KFC appear every few blocks, but they seem almost retro next to the Real Kung Fu fast-food chain, whose mascot is a stylized Bruce Lee.

American commentators like CNN's Jack Cafferty dismiss the Chinese as "the same bunch of goons and thugs they've been for the last 50 years." But nobody told the people of Shenzhen, who are busily putting on a 24-hour-a-day show called "America" — a pirated version of the original, only with flashier design, higher profits and less complaining. This has not happened by accident. China today, epitomized by Shenzhen's transition from mud to megacity in 30 years, represents a new way to organize society. Sometimes called "market Stalinism," it is a potent hybrid of the most powerful political tools of authoritarian communism — central planning, merciless repression, constant surveillance — harnessed to advance the goals of global capitalism.

Now, as China prepares to showcase its economic advances during the upcoming Olympics in Beijing, Shenzhen is once again serving as a laboratory, a testing ground for the next phase of this vast social experiment. Over the past two years, some 200,000 surveillance cameras have been installed throughout the city. Many are in public spaces, disguised as lampposts. The closed-circuit TV cameras will soon be connected to a single, nationwide network, an all-seeing system that will be capable of tracking and identifying anyone who comes within its range — a project driven in part by U.S. technology and investment. Over the next three years, Chinese security executives predict they will install as many as 2 million CCTVs in Shenzhen, which would make it the most watched city in the world. (Security-crazy London boasts only half a million surveillance cameras.)

The security cameras are just one part of a much broader high-tech surveillance and censorship program known in China as "Golden Shield." The end goal is to use the latest people-tracking technology — thoughtfully supplied by American giants like IBM, Honeywell and General Electric — to create an airtight consumer cocoon: a place where Visa cards, Adidas sneakers, China Mobile cellphones, McDonald's Happy Meals, Tsingtao beer and UPS delivery (to name just a few of the official sponsors of the Beijing Olympics) can be enjoyed under the unblinking eye of the state, without the threat of democracy breaking out. With political unrest on the rise across China, the government hopes to use the surveillance shield to identify and counteract dissent before it explodes into a mass movement like the one that grabbed the world's attention at Tiananmen Square.

Remember how we've always been told that free markets and free people go hand in hand? That was a lie. It turns out that the most efficient delivery system for capitalism is actually a communist-style police state, fortressed with American "homeland security" technologies, pumped up with "war on terror" rhetoric. And the global corporations currently earning superprofits from this social experiment are unlikely to be content if the lucrative new market remains confined to cities such as Shenzhen. Like everything else assembled in China with American parts, Police State 2.0 is ready for export to a neighborhood near you.

Zhang Yi points to an empty bracket on the dashboard of his black Honda. "It used to hold my GPS, but I leave it at home now," he says. "It's the crime — they are too easy to steal." He quickly adds, "Since the surveillance cameras came in, we have seen a very dramatic decrease in crime in Shenzhen."

After driving for an hour past hundreds of factory gates and industrial parks, we pull up to a salmon-color building that Zhang partly owns. This is the headquarters of FSAN: CCTV System. Zhang, a prototypical Shenzhen yuppie in a royal-blue button-down shirt and black-rimmed glasses, apologizes for the mess. Inside, every inch of space is lined with cardboard boxes filled with electronics parts and finished products.

Zhang opened the factory two and a half years ago, and his investment has already paid off tenfold. That kind of growth isn't unusual in the field he has chosen: Zhang's factory makes digital surveillance cameras, turning out 400,000 a year. Half of the cameras are shipped overseas, destined to peer from building ledges in London, Manhattan and Dubai as part of the global boom in "homeland security." The other half stays in China, many right here in Shenzhen and in

neighboring Guangzhou, another megacity of 12 million people. China's market for surveillance cameras enjoyed revenues of $4.1 billion last year, a jump of 24 percent from 2006.

Zhang escorts me to the assembly line, where rows of young workers, most of them women, are bent over semiconductors, circuit boards, tiny cables and bulbs. At the end of each line is "quality control," which consists of plugging the camera into a monitor and making sure that it records. We enter a showroom where Zhang and his colleagues meet with clients. The walls are lined with dozens of camera models: domes of all sizes, specializing in day and night, wet and dry, camouflaged to look like lights, camouflaged to look like smoke detectors, explosion-proof, the size of a soccer ball, the size of a ring box.

The workers at FSAN don't just make surveillance cameras; they are constantly watched by them. While they work, the silent eyes of rotating lenses capture their every move. When they leave work and board buses, they are filmed again. When they walk to their dormitories, the streets are lined with what look like newly installed streetlamps, their white poles curving toward the sidewalk with black domes at the ends. Inside the domes are high-resolution cameras, the same kind the workers produce at FSAN. Some blocks have three or four, one every few yards. One Shenzhen-based company, China Security & Surveillance Technology, has developed software to enable the cameras to alert police when an unusual number of people begin to gather at any given location.

In 2006, the Chinese government mandated that all Internet cafes (as well as restaurants and other "entertainment" venues) install video cameras with direct feeds to their local police stations. Part of a wider surveillance project known as "Safe Cities," the effort now encompasses 660 municipalities in China. It is the most ambitious new government program in the Pearl River Delta, and supplying it is one of the fastest-growing new markets in Shenzhen.

But the cameras that Zhang manufactures are only part of the massive experiment in population control that is under way here. "The big picture," Zhang tells me in his office at the factory, "is integration." That means linking cameras with other forms of surveillance: the Internet, phones, facial-recognition software and GPS monitoring.

This is how this Golden Shield will work: Chinese citizens will be watched around the clock through networked CCTV cameras and remote monitoring of computers.

They will be listened to on their phone calls, monitored by digital voice-recognition technologies. Their Internet access will be aggressively limited through the country's notorious system of online controls known as the "Great Firewall." Their movements will be tracked through national ID cards with scannable computer chips and photos that are instantly uploaded to police databases and linked to their holder's personal data. This is the most important element of all: linking all these tools together in a massive, searchable database of names, photos, residency information, work history and biometric data. When Golden Shield is finished, there will be a photo in those databases for every person in China: 1.3 billion faces.

Shenzhen is the place where the shield has received its most extensive fortifications — the place where all the spy toys are being hooked together and tested to see what they can do. "The central government eventually wants to have city-by-city surveillance, so they could just sit and monitor one city and its surveillance system as a whole," Zhang says. "It's all part of that bigger project. Once the tests are done and it's proven, they will be spreading from the big province to the cities, even to the rural farmland."

In fact, the rollout of the high-tech shield is already well under way.

When the Tibetan capital of Lhasa was set alight in March, the world caught a glimpse of the rage that lies just under the surface in many parts of China. And though the Lhasa riots stood out for their ethnic focus and their intensity, protests across China are often shockingly militant. In July 2006, workers at a factory near Shenzhen expressed their displeasure over paltry pay by overturning cars, smashing computers and opening fire hydrants. In March of last year, when bus fares went up in the rural town of Zhushan, 20,000 people took to the streets and five police vehicles were torched. Indeed, China has seen levels of political unrest in recent years unknown since 1989, the year student protests were crushed with tanks in Tiananmen Square. In 2005, by the government's own measure, there were at least 87,000 "mass incidents" — governmentspeak for large-scale protests or riots.

This increased unrest — a process aided by access to cellphones and the Internet — represents more than a security problem for the leaders in Beijing. It threatens their whole model of command-and-control capitalism. China's rapid economic growth has relied on the ability of its rulers to raze villages and move mountains to make way for the latest factory towns and shopping malls. If the

people living on those mountains use blogs and text messaging to launch a mountain-people's-rights uprising with each new project, and if they link up with similar uprisings in other parts of the country, China's dizzying expansion could grind to a halt.

At the same time, the success of China's ravenous development creates its own challenges. Every rural village that is successfully razed to make way for a new project creates more displaced people who join the ranks of the roughly 130 million migrants roaming the country looking for work. By 2025, it is projected that this "floating" population will swell to more than 350 million. Many will end up in cities like Shenzhen, which is already home to 7 million migrant laborers.

But while China's cities need these displaced laborers to work in factories and on construction sites, they are unwilling to offer them the same benefits as permanent residents: highly subsidized education and health care, as well as other public services. While migrants can live for decades in big cities like Shenzhen and Guangzhou, their residency remains fixed to the rural community where they were born, a fact encoded on their national ID cards. As one young migrant in Guangzhou put it to me, "The local people want to make money from migrant workers, but they don't want to give them rights. But why are the local people so rich? Because of the migrant workers!"

With its militant protests and mobile population, China confronts a fundamental challenge. How can it maintain a system based on two dramatically unequal categories of people: the winners, who get the condos and cars, and the losers, who do the heavy labor and are denied those benefits? More urgently, how can it do this when information technology threatens to link the losers together into a movement so large it could easily overwhelm the country's elites?

The answer is Golden Shield. When Tibet erupted in protests recently, the surveillance system was thrown into its first live test, with every supposedly liberating tool of the Information Age — cellphones, satellite television, the Internet — transformed into a method of repression and control. As soon as the protests gathered steam, China reinforced its Great Firewall, blocking its citizens from accessing dozens of foreign news outlets. In some parts of Tibet, Internet access was shut down altogether. Many people trying to phone friends and family found that their calls were blocked, and cellphones in Lhasa were blitzed with text messages from the police: "Severely battle any creation or any spreading of

rumors that would upset or frighten people or cause social disorder or illegal criminal behavior that could damage social stability."

During the first week of protests, foreign journalists who tried to get into Tibet were systematically turned back. But that didn't mean that there were no cameras inside the besieged areas. Since early last year, activists in Lhasa have been reporting on the proliferation of black-domed cameras that look like streetlights — just like the ones I saw coming off the assembly line in Shenzhen. Tibetan monks complain that cameras — activated by motion sensors — have invaded their monasteries and prayer rooms.

During the Lhasa riots, police on the scene augmented the footage from the CCTVs with their own video cameras, choosing to film — rather than stop — the violence, which left 19 dead. The police then quickly cut together the surveillance shots that made the Tibetans look most vicious — beating Chinese bystanders, torching shops, ripping metal sheeting off banks — and created a kind of copumentary: *Tibetans Gone Wild*. These weren't the celestial beings in flowing robes the Beastie Boys and Richard Gere had told us about. They were angry young men, wielding sticks and long knives. They looked ugly, brutal, tribal. On Chinese state TV, this footage played around the clock.

The police also used the surveillance footage to extract mug shots of the demonstrators and rioters. Photos of the 21 "most wanted" Tibetans, many taken from that distinctive "streetlamp" view of the domed cameras, were immediately circulated to all of China's major news portals, which obediently posted them to help out with the manhunt. The Internet became the most powerful police tool. Within days, several of the men on the posters were in custody, along with hundreds of others.

The flare-up in Tibet, weeks before the Olympic torch began its global journey, has been described repeatedly in the international press as a "nightmare" for Beijing. Several foreign leaders have pledged to boycott the opening ceremonies of the games, the press has hosted an orgy of China-bashing, and the torch became a magnet for protesters, with anti-China banners dropped from the Eiffel Tower and the Golden Gate Bridge. But inside China, the Tibet debacle may actually have been a boon to the party, strengthening its grip on power. Despite its citizens having unprecedented access to information technology (there are as many Internet users in China as there are in the U.S.), the party demonstrated that it could still control what they hear and see. And what they saw on their TVs

and computer screens were violent Tibetans, out to kill their Chinese neighbors, while police showed admirable restraint. Tibetan solidarity groups say 140 people were killed in the crackdown that followed the protests, but without pictures taken by journalists, it is as if those subsequent deaths didn't happen.

Chinese viewers also saw a world unsympathetic to the Chinese victims of Tibetan violence, so hostile to their country that it used a national tragedy to try to rob them of their hard-won Olympic glory. These nationalist sentiments freed up Beijing to go on a full-fledged witch hunt. In the name of fighting a war on terror, security forces rounded up thousands of Tibetan activists and supporters. The end result is that when the games begin, much of the Tibetan movement will be safely behind bars — along with scores of Chinese journalists, bloggers and human-rights defenders who have also been trapped in the government's high-tech web.

Police State 2.0 might not look good from the outside, but on the inside, it appears to have passed its first major test.

In Guangzhou, an hour and a half by train from Shenzhen, Yao Ruoguang is preparing for a major test of his own. "It's called the 10-million-faces test," he tells me.

Yao is managing director of Pixel Solutions, a Chinese company that specializes in producing the new high-tech national ID cards, as well as selling facial-recognition software to businesses and government agencies. The test, the first phase of which is only weeks away, is being staged by the Ministry of Public Security in Beijing. The idea is to measure the effectiveness of face-recognition software in identifying police suspects. Participants will be given a series of photos, taken in a variety of situations. Their task will be to match the images to other photos of the same people in the government's massive database. Several biometrics companies, including Yao's, have been invited to compete. "We have to be able to match a face in a 10 million database in one second," Yao tells me. "We are preparing for that now."

The companies that score well will be first in line for lucrative government contracts to integrate face-recognition software into Golden Shield, using it to check for ID fraud and to discover the identities of suspects caught on surveillance cameras. Yao says the technology is almost there: "It will happen next year."

When I meet Yao at his corporate headquarters, he is feeling confident about how his company will perform in the test. His secret weapon is that he will be using facial-recognition software purchased from L-1 Identity Solutions, a major U.S. defense contractor that produces passports and biometric security systems for the U.S. government.

To show how well it works, Yao demonstrates on himself. Using a camera attached to his laptop, he snaps a picture of his own face, round and boyish for its 54 years. Then he uploads it onto the company's proprietary Website, built with L-1 software. With the cursor, he marks his own eyes with two green plus signs, helping the system to measure the distance between his features, a distinctive aspect of our faces that does not change with disguises or even surgery. The first step is to "capture the image," Yao explains. Next is "finding the face."

He presses APPLY, telling the program to match the new face with photos of the same person in the company's database of 600,000 faces. Instantly, multiple photos of Yao appear, including one taken 19 years earlier — proof that the technology can "find a face" even when the face has changed significantly with time. "

It took 1.1 milliseconds!" Yao exclaims. "Yeah, that's me!"

In nearby cubicles, teams of Yao's programmers and engineers take each other's pictures, mark their eyes with green plus signs and test the speed of their search engines. "Everyone is preparing for the test," Yao explains. "If we pass, if we come out number one, we are guaranteed a market in China."

Every couple of minutes Yao's phone beeps. Sometimes it's a work message, but most of the time it's a text from his credit-card company, informing him that his daughter, who lives in Australia, has just made another charge. "Every time the text message comes, I know my daughter is spending money!" He shrugs: "She likes designers."

Like many other security executives I interviewed in China, Yao denies that a primary use of the technology he is selling is to hunt down political activists. "Ninety-five percent," he insists, "is just for regular safety." He has, he admits, been visited by government spies, whom he describes as "the internal-security people." They came with grainy pictures, shot from far away or through keyhole

cameras, of "some protesters, some dissidents." They wanted to know if Yao's facial-recognition software could help identify the people in the photos. Yao was sorry to disappoint them. "Honestly, the technology so far still can't meet their needs," he says. "The photos that they show us were just too blurry." That is rapidly changing, of course, thanks to the spread of high-resolution CCTVs. Yet Yao insists that the government's goal is not repression: "If you're a [political] organizer, they want to know your motive," he says. "So they take the picture, give the photo, so at least they can find out who that person is."

Until recently, Yao's photography empire was focused on consumers — taking class photos at schools, launching a Chinese knockoff of Flickr (the original is often blocked by the Great Firewall), turning photos of chubby two-year-olds into fridge magnets and lampshades. He still maintains those businesses, which means that half of the offices at Pixel Solutions look like they have just hosted a kid's birthday party. The other half looks like an ominous customs office, the walls lined with posters of terrorists in the cross hairs: FACE MATCH, FACE PASS, FACE WATCH. When Beijing started sinking more and more of the national budget into surveillance technologies, Yao saw an opportunity that would make all his previous ventures look small. Between more powerful computers, higher-resolution cameras and a global obsession with crime and terrorism, he figured that face recognition "should be the next dot-com."

Not a computer scientist himself — he studied English literature in school — Yao began researching corporate leaders in the field. He learned that face recognition is highly controversial, with a track record of making wrong IDs. A few companies, however, were scoring much higher in controlled tests in the U.S. One of them was a company soon to be renamed L-1 Identity Solutions. Based in Connecticut, L-1 was created two years ago out of the mergers and buyouts of half a dozen major players in the biometrics field, all of which specialized in the science of identifying people through distinct physical traits: fingerprints, irises, face geometry. The mergers made L-1 a one-stop shop for biometrics. Thanks to board members like former CIA director George Tenet, the company rapidly became a homeland-security heavy hitter. L-1 projects its annual revenues will hit $1 billion by 2011, much of it from U.S. government contracts.

In 2006, Yao tells me, "I made the first phone call and sent the first e-mail." For a flat fee of $20,000, he gained access to the company's proprietary software, allowing him to "build a lot of development software based on L-1's technology." Since then, L-1's partnership with Yao has gone far beyond that token

investment. Yao says it isn't really his own company that is competing in the upcoming 10-million-faces test being staged by the Chinese government: "We'll be involved on behalf of L-1 in China." Yao adds that he communicates regularly with L1 and has visited the company's research headquarters in New Jersey. ("Out the window you can see the Statue of Liberty. It's such a historic place.") L1 is watching his test preparations with great interest, Yao says. "It seemed that they were more excited than us when we tell them the results."

L-1's enthusiasm is hardly surprising: If Yao impresses the Ministry of Public Security with the company's ability to identify criminals, L-1 will have cracked the largest potential market for biometrics in the world. But here's the catch: As proud as Yao is to be L-1's Chinese licensee, L-1 appears to be distinctly less proud of its association with Yao. On its Website and in its reports to investors, L-1 boasts of contracts and negotiations with governments from Panama and Saudi Arabia to Mexico and Turkey. China, however, is conspicuously absent. And though CEO Bob LaPenta makes reference to "some large international opportunities," not once does he mention Pixel Solutions in Guangzhou.

After leaving a message with the company inquiring about L-1's involvement in China's homeland-security market, I get a call back from Doni Fordyce, vice president of corporate communications. She has consulted Joseph Atick, the company's head of research. "We have nothing in China," she tells me. "Nothing, absolutely nothing. We are uninvolved. We really don't have any relationships at all."

I tell Fordyce about Yao, the 10-million test, the money he paid for the software license. She'll call me right back. When she does, 20 minutes later, it is with this news: "Absolutely, we've sold testing SDKs [software development kits] to Pixel Solutions and to others [in China] that may be entering a test." Yao's use of the technology, she said, is "within his license" purchased from L-1.

The company's reticence to publicize its activities in China could have something to do with the fact that the relationship between Yao and L-1 may well be illegal under U.S. law. After the Chinese government sent tanks into Tiananmen Square in 1989, Congress passed legislation barring U.S. companies from selling any products in China that have to do with "crime control or detection instruments or equipment." That means not only guns but everything from police batons and handcuffs to ink and powder for taking fingerprints, and software for storing them. Interestingly, one of the "detection instruments" that prompted the

legislation was the surveillance camera. Beijing had installed several clunky cameras around Tiananmen Square, originally meant to monitor traffic flows. Those lenses were ultimately used to identify and arrest key pro-democracy dissidents.

"The intent of that act," a congressional staff member with considerable China experience tells me, "was to keep U.S. companies out of the business of helping the Chinese police conduct their business, which might ultimately end up as it did in 1989 in the suppression of human rights and democracy in China."

Pixel's application of L-1 facial-recognition software seems to fly in the face of the ban's intent. By his own admission, Yao is already getting visits from Chinese state spies anxious to use facial recognition to identify dissidents. And as part of the 10-million-faces test, Yao has been working intimately with Chinese national-security forces, syncing L-1's software to their vast database, a process that took a week of intensive work in Beijing. During that time, Yao says, he was on the phone "every day" with L-1, getting its help adapting the technology. "Because we are representing them," he says. "We took the test on their behalf."

In other words, this controversial U.S. "crime control" technology has already found its way into the hands of the Chinese police. Moreover, Yao's goal, stated to me several times, is to use the software to land lucrative contracts with police agencies to integrate facial recognition into the newly built system of omnipresent surveillance cameras and high-tech national ID cards. As part of any contract he gets, Yao says, he will "pay L-1 a certain percentage of our sales."

When I put the L-1 scenario to the Commerce Department's Bureau of Industry and Security — the division charged with enforcing the post-Tiananmen export controls — a representative says that software kits are subject to the sanctions if "they are exported from the U.S. or are the foreign direct product of a U.S.-origin item." Based on both criteria, the software kit sold to Yao seems to fall within the ban.

When I ask Doni Fordyce at L-1 about the embargo, she tells me, "I don't know anything about that." Asked whether she would like to find out about it and call me back, she replies, "I really don't want to comment, so there is no comment." Then she hangs up.

You have probably never heard of L-1, but there is every chance that it has heard of you. Few companies have collected as much sensitive information about U.S. citizens and visitors to America as L-1: It boasts a database of 60 million records, and it "captures" more than a million new fingerprints every year. Here is a small sample of what the company does: produces passports and passport cards for American citizens; takes finger scans of visitors to the U.S. under the Department of Homeland Security's massive U.S.-Visit program; equips U.S. soldiers in Iraq and Afghanistan with "mobile iris and multimodal devices" so they can collect biometric data in the field; maintains the State Department's "largest facial-recognition database system"; and produces driver's licenses in Illinois, Montana and North Carolina. In addition, L-1 has an even more secretive intelligence unit called SpecTal. Asked by a Wall Street analyst to discuss, in "extremely general" terms, what the division was doing with contracts worth roughly $100 million, the company's CEO would only say, "Stay tuned."

It is L-1's deep integration with multiple U.S. government agencies that makes its dealings in China so interesting: It isn't just L-1 that is potentially helping the Chinese police to nab political dissidents, it's U.S. taxpayers. The technology that Yao purchased for just a few thousand dollars is the result of Defense Department research grants and contracts going as far back as 1994, when a young academic named Joseph Atick (the research director Fordyce consulted on L-1's China dealings) taught a computer at Rockefeller University to recognize his face.

Yao, for his part, knows all about the U.S. export controls on police equipment to China. He tells me that L-1's electronic fingerprinting tools are "banned from entering China" due to U.S. concerns that they will be used to "catch the political criminals, you know, the dissidents, more easily." He thinks he and L-1 have found a legal loophole, however. While fingerprinting technology appears on the Commerce Department's list of banned products, there is no explicit mention of "face prints" — likely because the idea was still in the realm of science fiction when the Tiananmen Square massacre took place. As far as Yao is concerned, that omission means that L-1 can legally supply its facial-recognition software for use by the Chinese government.

Whatever the legality of L-1's participation in Chinese surveillance, it is clear that U.S. companies are determined to break into the homeland-security market in China, which represents their biggest growth potential since 9/11. According to

the congressional staff member, American companies and their lobbyists are applying "enormous pressure to open the floodgates."

The crackdown in Tibet has set off a wave of righteous rallies and boycott calls. But it sidesteps the uncomfortable fact that much of China's powerful surveillance state is already being built with U.S. and European technology. In February 2006, a congressional subcommittee held a hearing on "The Internet in China: A Tool for Freedom or Suppression?" Called on the carpet were Google (for building a special Chinese search engine that blocked sensitive material), Cisco (for supplying hardware for China's Great Firewall), Microsoft (for taking down political blogs at the behest of Beijing) and Yahoo (for complying with requests to hand over e-mail-account information that led to the arrest and imprisonment of a high-profile Chinese journalist, as well as a dissident who had criticized corrupt officials in online discussion groups). The issue came up again during the recent Tibet uproar when it was discovered that both MSN and Yahoo had briefly put up the mug shots of the "most wanted" Tibetan protesters on their Chinese news portals.

In all of these cases, U.S. multinationals have offered the same defense: Cooperating with draconian demands to turn in customers and censor material is, unfortunately, the price of doing business in China. Some, like Google, have argued that despite having to limit access to the Internet, they are contributing to an overall increase of freedom in China. It's a story that glosses over the much larger scandal of what is actually taking place: Western investors stampeding into the country, possibly in violation of the law, with the sole purpose of helping the Communist Party spend billions of dollars building Police State 2.0. This isn't an unfortunate cost of doing business in China: It's the goal of doing business in China. "Come help us spy!" the Chinese government has said to the world. And the world's leading technology companies are eagerly answering the call.

As *The New York Times* recently reported, aiding and abetting Beijing has become an investment boom for U.S. companies. Honeywell is working with Chinese police to "set up an elaborate computer monitoring system to analyze feeds from indoor and outdoor cameras in one of Beijing's most populated districts." General Electric is providing Beijing police with a security system that controls "thousands of video cameras simultaneously, and automatically alerts them to suspicious or fast-moving objects, like people running." IBM, meanwhile, is installing its "Smart Surveillance System" in the capital, another system for linking video cameras and scanning for trouble, while United Technologies is in

Guangzhou, helping to customize a "2,000-camera network in a single large neighborhood, the first step toward a citywide network of 250,000 cameras to be installed before the Asian Games in 2010." By next year, the Chinese internal-security market will be worth an estimated $33 billion — around the same amount Congress has allocated for reconstructing Iraq.

"We're at the start of a massive boom in Chinese security spending," according to Graham Summers, a market analyst who publishes an investor newsletter in Baltimore. "And just as we need to be aware of how to profit from the growth in China's commodity consumption, we need to be aware of companies that will profit from 'security consumption.' . . . There's big money to be made."

While U.S. companies are eager to break into China's rapidly expanding market, every Chinese security firm I come across in the Pearl River Delta is hatching some kind of plan to break into the U.S. market. No one, however, is quite as eager as Aebell Electrical Technology, one of China's top 10 security companies. Aebell has a contract to help secure the Olympic swimming stadium in Beijing and has installed more than 10,000 cameras in and around Guangzhou. Business has been growing by 100 percent a year. When I meet the company's fidgety general manager, Zheng Sun Man, the first thing he tells me is "We are going public at the end of this year. On the Nasdaq." It also becomes clear why he has chosen to speak with a foreign reporter: "Help, help, help!" he begs me. "Help us promote our products!"

Zheng, an MBA from one of China's top schools, proudly shows me the business card of the New York investment bank that is handling Aebell's IPO, as well as a newly printed English-language brochure showing off the company's security cameras. Its pages are filled with American iconography, including businessmen exchanging wads of dollar bills and several photos of the New York skyline that prominently feature the World Trade Center. In the hall at company headquarters is a poster of two interlocking hearts: one depicting the American flag, the other the Aebell logo.

I ask Zheng whether China's surveillance boom has anything to do with the rise in strikes and demonstrations in recent years. Zheng's deputy, a 23-year veteran of the Chinese military wearing a black Mao suit, responds as if I had launched a direct attack on the Communist Party itself. "If you walk out of this building, you will be under surveillance in five to six different ways," he says, staring at me hard. He lets the implication of his words linger in the air like an unspoken threat.

"If you are a law-abiding citizen, you shouldn't be afraid," he finally adds. "The criminals are the only ones who should be afraid."

One of the first people to sound the alarm on China's upgraded police state was a British researcher named Greg Walton. In 2000, Walton was commissioned by the respected human-rights organization Rights & Democracy to investigate the ways in which Chinese security forces were harnessing the tools of the Information Age to curtail free speech and monitor political activists. The paper he produced was called "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China." It exposed how big-name tech companies like Nortel and Cisco were helping the Chinese government to construct "a gigantic online database with an all-encompassing surveillance network — incorporating speech and face recognition, closed-circuit television, smart cards, credit records and Internet surveillance technologies."

When the paper was complete, Walton met with the institute's staff to strategize about how to release his explosive findings. "We thought this information was going to shock the world," he recalls. In the midst of their discussions, a colleague barged in and announced that a plane had hit the Twin Towers. The meeting continued, but they knew the context of their work had changed forever.

Walton's paper did have an impact, but not the one he had hoped. The revelation that China was constructing a gigantic digital database capable of watching its citizens on the streets and online, listening to their phone calls and tracking their consumer purchases sparked neither shock nor outrage. Instead, Walton says, the paper was "mined for ideas" by the U.S. government, as well as by private companies hoping to grab a piece of the suddenly booming market in spy tools. For Walton, the most chilling moment came when the Defense Department tried to launch a system called Total Information Awareness to build what it called a "virtual, centralized grand database" that would create constantly updated electronic dossiers on every citizen, drawing on banking, credit-card, library and phone records, as well as footage from surveillance cameras. "It was clearly similar to what we were condemning China for," Walton says. Among those aggressively vying to be part of this new security boom was Joseph Atick, now an executive at L-1. The name he chose for his plan to integrate facial-recognition software into a vast security network was uncomfortably close to the surveillance system being constructed in China: "Operation Noble Shield."

Empowered by the Patriot Act, many of the big dreams hatched by men like Atick have already been put into practice at home. New York, Chicago and Washington, D.C., are all experimenting with linking surveillance cameras into a single citywide network. Police use of surveillance cameras at peaceful demonstrations is now routine, and the images collected can be mined for "face prints," then cross-checked with ever-expanding photo databases. Although Total Information Awareness was scrapped after the plans became public, large pieces of the project continue, with private data-mining companies collecting unprecedented amounts of information about everything from Web browsing to car rentals, and selling it to the government.

Such efforts have provided China's rulers with something even more valuable than surveillance technology from Western democracies: the ability to claim that they are just like us. Liu Zhengrong, a senior official dealing with China's Internet policy, has defended Golden Shield and other repressive measures by invoking the Patriot Act and the FBI's massive e-mail-mining operations. "It is clear that any country's legal authorities closely monitor the spread of illegal information," he said. "We have noted that the U.S. is doing a good job on this front." Lin Jiang Huai, the head of China Information Security Technology, credits America for giving him the idea to sell biometric IDs and other surveillance tools to the Chinese police. "Bush helped me get my vision," he has said. Similarly, when challenged on the fact that dome cameras are appearing three to a block in Shenzhen and Guangzhou, Chinese companies respond that their model is not the East German Stasi but modern-day London.

Human-rights activists are quick to point out that while the tools are the same, the political contexts are radically different. China has a government that uses its high-tech web to imprison and torture peaceful protesters, Tibetan monks and independent-minded journalists. Yet even here, the lines are getting awfully blurry. The U.S. currently has more people behind bars than China, despite a population less than a quarter of its size. And Sharon Hom, executive director of the advocacy group Human Rights in China, says that when she talks about China's horrific human-rights record at international gatherings, "There are two words that I hear in response again and again: Guantánamo Bay."

The Fourth Amendment prohibition against illegal search and seizure made it into the U.S. Constitution precisely because its drafters understood that the power to snoop is addictive. Even if we happen to trust in the good intentions of the snoopers, the nature of any government can change rapidly — which is why the

Constitution places limits on the tools available to any regime. But the drafters could never have imagined the commercial pressures at play today. The global homeland-security business is now worth an estimated $200 billion — more than Hollywood and the music industry combined. Any sector of that size inevitably takes on its own momentum. New markets must be found — which, in the Big Brother business, means an endless procession of new enemies and new emergencies: crime, immigration, terrorism.

In Shenzhen one night, I have dinner with a U.S. business consultant named Stephen Herrington. Before he started lecturing at Chinese business schools, teaching students concepts like brand management, Herrington was a military-intelligence officer, ascending to the rank of lieutenant colonel. What he is seeing in the Pearl River Delta, he tells me, is scaring the hell out of him — and not for what it means to China.

"I can guarantee you that there are people in the Bush administration who are studying the use of surveillance technologies being developed here and have at least skeletal plans to implement them at home," he says. "We can already see it in New York with CCTV cameras. Once you have the cameras in place, you have the infrastructure for a powerful tracking system. I'm worried about what this will mean if the U.S. government goes totalitarian and starts employing these technologies more than they are already. I'm worried about the threat this poses to American democracy."

Herrington pauses. "George W. Bush," he adds, "would do what they are doing here in a heartbeat if he could."

China-bashing never fails to soothe the Western conscience — here is a large and powerful country that, when it comes to human rights and democracy, is so much worse than Bush's America. But during my time in Shenzhen, China's youngest and most modern city, I often have the feeling that I am witnessing not some rogue police state but a global middle ground, the place where more and more countries are converging. China is becoming more like us in very visible ways (Starbucks, Hooters, cellphones that are cooler than ours), and we are becoming more like China in less visible ones (torture, warrantless wiretapping, indefinite detention, though not nearly on the Chinese scale).

What is most disconcerting about China's surveillance state is how familiar it all feels. When I check into the Sheraton in Shenzhen, for instance, it looks like any

other high-end hotel chain — only the lobby is a little more modern and the cheerful clerk doesn't just check my passport but takes a scan of it.

"Are you making a copy?" I ask.

"No, no," he responds helpfully. "We're just sending a copy to the police."

Up in my room, the Website that pops up on my laptop looks like every other Net portal at a hotel — only it won't let me access human-rights and labor Websites that I know are working fine. The TV gets CNN International — only with strange edits and obviously censored blackouts. My cellphone picks up a strong signal for the China Mobile network. A few months earlier, in Davos, Switzerland, the CEO of China Mobile bragged to a crowd of communications executives that "we not only know who you are, we also know where you are." Asked about customer privacy, he replied that his company only gives "this kind of data to government authorities" — pretty much the same answer I got from the clerk at the front desk.

When I leave China, I feel a powerful relief: I have escaped. I am home safe. But the feeling starts to fade as soon as I get to the customs line at JFK, watching hundreds of visitors line up to have their pictures taken and fingers scanned. In the terminal, someone hands me a brochure for "Fly Clear." All I need to do is have my fingerprints and irises scanned, and I can get a Clear card with a biometric chip that will let me sail through security. Later, I look it up: The company providing the technology is L-1.

[From Issue 1053 — May 29, 2008] URL:
http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye