America invented the three-digit credit score. Now companies in China are taking the idea to the extreme, using big data to track and rank what you do—your purchases, your pastimes, your mistakes.

PHOTOGRAPHS BY DAN WINTERS; ILLUSTRATIONS BY JAMES GRAHAM

- MARA HVISTENDAHL
  AUTHOR
- BUSINESS
- 12.14.17
- 06:00 AM

INSIDE CHINA'S VAST NEW EXPERIMENT IN SOCIAL RANKING

IN 2015, WHEN Lazarus Liu moved home to China after studying logistics in the United Kingdom for three years, he quickly noticed that something had changed: Everyone paid for everything with their phones. At McDonald's, the convenience store, even at mom-and-pop restaurants, his friends in Shanghai used mobile payments. Cash, Liu could see, had been largely replaced by two smartphone apps: Alipay and WeChat Pay. One day, at a vegetable market, he watched a woman his mother's age pull out her phone to pay for her groceries. He decided to sign up.

To get an Alipay ID, Liu had to enter his cell phone number and scan his national ID card. He did so reflexively. Alipay had built a reputation for reliability, and compared to going to a bank managed with slothlike indifference and zero attention to customer service, signing up for Alipay was almost fun. With just a few clicks he was in. Alipay's slogan summed up the experience: "Trust makes it simple."

Alipay turned out to be so convenient that Liu began using it multiple times a day, starting first thing in the morning, when he ordered breakfast through a food delivery app. He realized that he could pay for parking through Alipay's My Car feature, so he added his driver's license and license plate numbers, as well as the engine number of his Audi. He started making his car insurance payments with the app. He booked doctors' appointments there, skipping the chaotic lines for which Chinese hospitals are famous. He added friends in Alipay's built-in social network. When Liu went on vacation with his fiancée (now his wife) to Thailand, they paid at restaurants and bought trinkets with Alipay. He stored whatever money was left over, which wasn't much once the vacation and car were paid for, in an Alipay money market account. He could have paid his electricity, gas, and internet bills in Alipay's City Service section. Like many young Chinese who had become enamored of the mobile payment services offered by Alipay and WeChat, Liu stopped bringing his wallet when he left the house.

If you live in the United States, you are by now accustomed to relinquishing your data to corporations. Credit card companies know when you run up bar tabs or buy sex toys. Facebook knows if you like Tasty cooking videos or Breitbart News. Uber knows where you go and how you behave en route. But Alipay knows all of these things about its users and more. Owned by Ant Financial, an affiliate of the massive Alibaba corporation, Alipay is sometimes called a super app. Its main competitor, WeChat, belongs to the social and gaming giant Tencent. Alipay and WeChat are less like individual apps than entire ecosystems. Whenever Liu opened Alipay on his phone, he saw a neat grid of icons that vaguely resembled the home screen on his Samsung. Some of the icons were themselves full-blown third-party apps. If he wanted to, he could access Airbnb, Uber, or Uber's Chinese rival Didi, entirely from inside Alipay. It was as if Amazon had swallowed eBay, Apple News, Groupon, American Express, Citibank, and YouTube—and could siphon up data from all of them.

One day a new icon appeared on Liu's Alipay home screen. It was labeled Zhima Credit (or Sesame Credit). The name, like that of Alipay's parent company, evoked the story of Ali Baba and the 40 thieves, in which the words open sesame magically unseal a cave full of treasure. When Liu touched the icon, he was greeted by an image of the Earth. "Zhima Credit is the embodiment of personal credit," the text underneath read. "It uses big data to conduct an objective assessment. The higher the score, the better your credit." Further down was a button that read, in clean white characters, "Start my credit journey." He tapped.

IN 1956 AN electrical engineer named Bill Fair and a mathematician named Earl Isaac started a small tech company out of a San Francisco apartment. They named it Fair, Isaac and Co., but the business eventually came to be known, for short, as FICO. Their chief innovation was using computer-driven statistical analysis to translate people's personal details and financial history into a simple score, predicting how likely they were to pay back loans. Before FICO, credit bureaus relied in part on gossip culled from people's landlords, neighbors, and local grocers. Applicants' race could be counted against them, as could messiness, poor morals, and "effeminate gestures." Algorithmic scoring, Fair and Isaac argued, was a more equitable, scientific alternative to this unfair reality. FICO's approach eventually caught on among the credit bureaus—TransUnion, Experian, and Equifax—and in 1989 FICO introduced the credit score we know today, enabling millions of Americans to take out mortgages and rack up credit card bills.

During the past 30 years, by contrast, China has grown to become the world's second largest economy without much of a functioning credit system at all. The People's Bank of China, the country's central banking regulator, maintains records on millions of consumers, but they often contain little or no information. Until recently, it was difficult to get a credit card with any bank other than your own. Consumers mainly used cash. As housing prices spiked, this became increasingly untenable. "Now you need two suitcases to buy a house, not just one," says Zennon Kapron, who heads the financial tech consultancy Kapronasia. Still, efforts to establish a reliable credit system foundered because China lacked a third-party credit scoring entity. What it did have by the end of 2011 were 356 million smartphone users.

That year, Ant Financial launched a version of Alipay with a built-in scanner for reading QR codes—square, machine-readable labels that can hold over 100 times more information than a standard bar code. (WeChat Pay, which launched in 2013, has a similar built-in scanner.) Scanning a QR code can bring you to a website, or pull up an app, or connect you to a person's social media profile. Codes started showing up on graves (scan to learn more about the deceased) and the shirts of waiters (scan to tip).

Beggars printed out QR codes and set them out on the street. The codes linked the online and offline realms on a scale not seen anywhere else in the world. That first year with the QR scanner, Alipay mobile payments reached nearly $70 billion.

In 2013, Ant Financial executives retreated to the mountains outside Hangzhou to discuss creating a slew of new products; one of them was Zhima Credit. The executives realized that they could use the data-collecting powers of Alipay to calculate a credit score based on an individual's activities. "It was a very natural process," says You Xi, a Chinese business reporter who detailed this pivotal meeting in a recent book, Ant Financial. "If you have payment data, you can assess the credit of a person." And so the tech company began the process of creating a score that would be "credit for everything in your life," as You explains it.

Ant Financial wasn't the only entity keen on using data to measure people's worth. Coincidentally or not, in 2014 the Chinese government announced it was developing what it called a system of "social credit." In 2014, the State Council, China's governing cabinet, publicly called for the establishment of a nationwide tracking system to rate the reputations of individuals, businesses, and even government officials. The aim is for every Chinese citizen to be trailed by a file compiling data from public and private sources by 2020, and for those files to be searchable by fingerprints and other biometric characteristics. The State Council calls it a "credit system that covers the whole society."

For the Chinese Communist Party, social credit is an attempt at a softer, more invisible authoritarianism. The goal is to nudge people toward behaviors ranging from energy conservation to obedience to the Party. Samantha Hoffman, a consultant with the International Institute for Strategic Studies in London who is researching social credit, says that the government wants to preempt instability that might threaten the Party. "That's why social credit ideally requires both coercive aspects and nicer aspects, like providing social services and solving real problems. It's all under the same Orwellian umbrella."

In 2015 Ant Financial was one of eight tech companies granted approval from the People's Bank of China to develop their own private credit scoring platforms. Zhima Credit appeared in the Alipay app shortly after that. The service tracks your behavior on the app to arrive at a score between 350 and 950, and offers perks and rewards to those with good scores. Zhima Credit's algorithm considers not only whether you repay your bills but also what you buy, what degrees you hold, and the scores of your friends. Like Fair and Isaac decades earlier, Ant Financial executives talked publicly about how a data-driven approach would open up the financial system to people who had been locked out, like students and rural Chinese. For the more than 200 million Alipay users who have opted in to Zhima Credit, the sell is clear: Your data will magically open doors for you.

Participating in Zhima Credit is voluntary, and it's unclear whether or how signing up for it could affect an individual's rating in the government system. Ant Financial declined to let me interview anyone from the company, but did provide a statement from Hu Tao, the general manager of Zhima Credit. "Zhima Credit is dedicated to creating trust in a commercial setting and independent of any government-initiated social credit system," the statement reads. "Zhima Credit does not share user scores or underlying data with any third party including the government without the user's prior consent."

Ant Financial did state, however, in a 2015 press release that the company plans "to help build a social integrity system." And the company has already cooperated with the Chinese government in one important way: It has integrated a blacklist of more than 6 million people who have defaulted on court fines into Zhima Credit's database. According to Xinhua, the state news agency, this union of big tech and big government has helped courts punish more than 1.21 million defaulters, who opened their Zhima Credit one day to find their scores plunging.

The State Council has signaled that under the national social credit system people will be penalized for the crime of spreading online rumors, among other offenses, and that those deemed "seriously untrustworthy" can expect to receive substandard services. Ant Financial appears to be aiming for a society divided along moral lines as well. As Lucy Peng, the company's chief executive, was quoted as saying in Ant Financial, Zhima Credit "will ensure that the bad people in society don't have a place to go, while good people can move freely and without obstruction."

I LIVED IN China for the better part of a decade but left in 2014, before mobile payments had fully taken hold. Today $5.5 trillion in mobile payments are made every year in China. (In contrast, the US mobile payments market in 2016 was worth roughly $112 billion.) When I returned for a visit in August, I was determined to be a part of the new cashless China. So I signed up for Alipay and Zhima Credit a few hours after emerging bleary-eyed from the plane. Because I lacked a transaction history, I immediately faced what felt like an embarrassing judgment: a score of 550.

On my first day in Shanghai, I opened Zhima Credit to scan a yellow bike that I found parked at an angle on the sidewalk. China's bike-sharing culture had, like mobile payments, emerged out of nowhere, and Shanghai's streets were littered with brightly colored bikes, deposited wherever the riders pleased. A scan of a bike's QR code revealed a four-digit number that unlocked the back wheel, and a ride across town cost roughly 15 cents. Because of my middling score, however, I had to pay a $30 deposit before I could scan my first bike. Nor could I get deposit-free hotel stays or GoPro rentals, or free umbrella rentals. I belonged to the digital underclass.

In China, anxiety about pianzi, or swindlers, runs deep. How do I know you're not a pianzi? is a question people often ask when salespeople call on the phone or repairmen show up at the door. While my score likely didn't put me in the ranks of pianzi, one promise of Zhima Credit was identifying those who were. Companies can buy risk assessments for users that detail whether they have paid their rent or utilities or appear on the court blacklist. For businesses, such products are billed as time-savers. On the site Tencent Video, I stumbled across an ad for Zhima Credit in which a businessman scrutinizes strangers as he rides the subway. "Everybody looks like a pianzi," he despairs. His employees, trying to guard against shady customers, cover the office conference room walls with photos of lowlifes and criminals. But then—tada!—the boss discovers Zhima Credit, and all of their problems are solved. The staff celebrate by tearing the photos off the wall.

For those with good behavior, Zhima Credit offers perks through cooperation agreements that Ant Financial has signed with hundreds of companies and institutions. Shenzhou Zuche, a car rental company, allows people with credit scores over 650 to rent a car without a deposit. In exchange for this vetting, Shenzhou Zuche shares data, so that if a Zhima Credit user crashes one of the rental company's cars and refuses to pay up, that detail is fed back into his or her credit score. For a while people with scores over 750 could even skip the security check line at Beijing Capital Airport.

Two years after signing up for Zhima Credit, Lazarus Liu was trending up to that number. I met Liu, who is 27 and works at a large corporation, one Saturday afternoon at a mall in central Shanghai, outside a Forever 21. He wore a black shirt, black sneakers, and black Air Jordan shorts, and his face was framed by a fresh fade, with a jolt of black hair that flopped to one side. We walked to a Starbucks filled with young people hunched over their phones, sipping peach iced teas and green tea Frappuccinos. Liu claimed the last open table.

Liu told me that he chose his English name, Lazarus, after converting to Catholicism three years ago, but that his religion was mostly a private affair. He saw his Zhima Credit score the same way; it revealed something about him, but he kept those insights mostly to himself. He rarely checked his score—it just lurked in the background of the Alipay app on his Samsung—and because it was good, he didn't have to. After starting at 600 out of a possible 950 points, he had reached 722, a score that entitled him to favorable terms on loans and apartment rentals, as well as showcasing on several dating apps should he and his wife ever split up. With a few dozen more points, he could get a streamlined visa to Luxembourg, not that he was planning such a trip.

As Liu amassed a favorable transaction and payment history on Alipay, his score naturally improved. But it could go down if he neglected to pay a traffic fine, for example. And the privileges that come with a high score might someday be revoked for behaviors that have nothing to do with consumer etiquette. In June 2015, as 9.4 million Chinese teenagers took the grueling national college entrance examination, Hu Tao, the Zhima Credit general manager, told reporters that Ant Financial hoped to obtain a list of students who cheated, so that the fraud could become a blight on their Zhima Credit records. "There should be consequences for dishonest behavior," she avowed. The good were moving without obstruction. A threat hung over the rest.

ALIPAY KNOWS THAT at 1 pm on the afternoon of August 26, I rented an Ofo brand bike outside Shanghai's former French Concession and rode north, parking it across from Jing'an Temple. It knows that at 1:24 pm I bought a snack in the mall next to the temple. It knows that afterward I got in a Didi car bound for a neighborhood to the northwest. It knows that at 3:11 pm I disembarked and entered a supermarket, and it knows (because Alibaba owns the supermarket, which accepts only Alipay at checkout) that at 3:36 pm I bought bananas, cheese, and crackers. It knows that I then got in a taxi, and that I arrived at my destination at 4:01 pm. It knows the identification number of the taxi that drove me there. It knows that at 4:19 pm I paid $8 for an Amazon delivery. For three sweet hours—one of which I spent in the swimming pool—it does not know my whereabouts. Then it knows that I rented another Ofo bike outside a hotel in central Shanghai, cycled 10 minutes, and at 7:11 pm parked it outside a popular restaurant. Because Ant Financial is a strategic investor in Ofo, Alipay might know the route I took.

The algorithm behind my Zhima Credit score is a corporate secret. Ant Financial officially lists five broad categories of information that feed into the score, but the company provides only the barest of details about how these ingredients are cooked together. Like any conventional credit scoring system, Zhima Credit monitors my spending history and whether I have repaid my loans. But elsewhere the algorithm veers into voodoo, or worse. A category called Connections considers the credit of my contacts in Alipay's social network. Characteristics takes into consideration what kind of car I drive, where I work, and where I went to school. A category called Behavior, meanwhile, scrutinizes the nuances of my consumer life, zeroing in on actions that purportedly correlate with good credit. Shortly after Zhima Credit's launch, the company's technology director, Li Yingyun, told the Chinese magazine Caixin that spending behavior like buying diapers, say, could boost one's score, while playing videogames for hours on end could lower it. Online speculation held that donating to charity, presumably through Alipay's built-in donation service, was good. But I'm not sure whether the $3 I gave for feeding brown bear cubs qualifies me as a philanthropist or a cheapskate.

I began to check my score obsessively, but because scores are only reevaluated monthly, the number didn't budge. Each time I opened the app, I encountered an alarming orange screen. In the foreground was a gauge in the shape of a half-circle, with a dial showing that I had reached only a quarter of my potential. An article on the portal Sohu.com explained that my score put me in the category of "common folk." The page read: "Cultural level is not high. Retired or nearly retired." In China, where many elderly lost out on years of education during the Cultural Revolution, this was not a compliment. According to Sohu, only 5 percent of the population had scores worse than mine.

To see if I could do anything to pull my score up, I took a taxi one morning to a chic open-air shopping center outside Shanghai's city center to meet with Chen Chen, a 30-year-old illustrator. Chen told a mutual friend on WeChat that she had an "excellent" rating on Zhima Credit, and I wanted to ask her counsel. We bought coffee and walked to an outdoor seating area. Chen wore a button-down shirt open over a white T-shirt and skinny jeans. Her hair was bleached to a straw yellow, and a line of sparkly eye shadow was swept under each eye. On Zhima Credit she clocked in at 710, and her background color was a calming sky blue.

She explained how to boost my score. "They will check what kind of friends you have," she said. "If your friends are all high-score people, it's good for you. If you have some bad-credit people as friends, it's not nice." After signing up for Alipay, I sent friend requests to all of my phone contacts. Only six people accepted. One of my new Alipay friends was a man I used to tutor in English and probably my wealthiest friend in Shanghai. He owned several businesses, a fleet of cars, and a spacious villa in a posh neighborhood. But another was my old tailor, who lived with her family in a single room in a dilapidated house, with piles of cloth obscuring the thin windows. Did the tailor's impact on my score cancel out the businessman's? And was I dragging both of them down?

Chen said she knew the scores of her close friends but not those of acquaintances or work colleagues. There are chat rooms where people with decent scores seek out other high scorers, presumably to boost their ratings. But in general, people simply make assumptions about which contacts have good credit and which are better left unfriended. Users like Chen hadn't yet taken the step of shutting low scorers like me out of their network, she assured me. Zhima Credit was still fairly new, and an acquaintance's low score might still be charitably explained, she said: "Maybe they just haven't used it long enough."

TO UNDERSTAND THE allure that social engineering holds for Chinese leaders, you have to go back decades, to long before apps and big data. In the years after the 1949 Communist Revolution, the government assigned everyone to local work units, which became the locus of surveillance and control. Individuals spied on their neighbors while also doing everything they could to avoid black marks on their own dang'an, or government files. But maintaining the system required massive state effort and oversight. As economic reforms in the 1980s led millions of people to leave their villages and migrate to cities, the work unit system fell apart. Migration also had a secondary effect: Cities filled up with strangers and pianzi.

It didn't take long for the central government to start thinking about gamifying good behavior. Leaders realized that "if we are going to have a market system that is supposed to be self-guiding, we also need to have self-guiding credit systems," says Rogier Creemers, a scholar of Chinese law at the Leiden Institute for Area Studies in the Netherlands. In the late 1990s, a working group at a Chinese Academy of Sciences institute developed the basic concepts behind the social credit system. But the technology wasn't advanced enough to support the Communist Party's broader political designs.

Nearly a decade ago, I spent a few weeks in Suining, a mostly rural county in Jiangsu province, near Shanghai. Back then, local governance was not subtle. When officials decided to clamp down on people running red lights, they urged citizens to take pictures of offenders, whose images would later be featured on the local television channel.

Then, in 2010, Suining became one of the first areas in China to pilot a social credit system. Officials there began assessing residents on a range of criteria, including education level, online behavior, and how well they followed traffic laws. Each of Suining's 1.1 million citizens older than 14 started out with 1,000 points, and points were added or deducted based on behavior. Taking care of elderly family members earned you 50 points. Helping the poor merited 10 points. Helping the poor in a way that was reported by the media: 15. A drunk driving conviction meant the loss of 50 points, as did bribing an official. After the points were tallied up, citizens were assigned grades of A, B, C, or D. Grade A citizens would be given priority for school admissions and employment, while D citizens would be denied licenses, permits, and access to some social services.

The Suining system was rudimentary, and it briefly sparked a national debate over what criteria should be included in a social credit score. But it provided a testing ground for what could work nationally. And however crude the letter grades were, they were less crude than what they replaced. Social credit in Suining was accompanied by a shift to subtler government messaging.

Since the Suining pilot, dozens of cities have developed their own systems. The power of technology had caught up. Eventually, these systems will be integrated into the nationwide government social credit system, which entails a significant logistical headache. To aid in the task, the government has enlisted Baidu, a big tech company, to help develop the social credit database by the 2020 deadline.

The Chinese tech companies have, in their way, helped to shift the Party's attitude toward digital technologies. When the internet first came to China, bursting into people's lives in the form of blogs and chat rooms, the Party saw it as a threat. Here was a place where people might speak their minds, join together, dissent. Leaders responded to these impulses through censorship and other aggressive tactics. But companies like Ant Financial have shown just how useful digital technologies can be in gathering and deploying information. Instead of merely reacting to content by banning search terms or shutting down websites, the government now collaborates with the private sector on facial and voice recognition technologies, along with artificial intelligence research.

In 2015, a few months after Zhima Credit debuted, Alibaba founder Jack Ma and 14 other executives traveled to the US with President Xi Jinping for his first state visit. Ma, along with leaders at Tencent and Baidu, also sits on the board of the Internet Society of China, a quasi-governmental organization under the direction of the Party.

This strategic nexus is a delicate one, though. In recent months Chinese regulators have taken steps to exert more control over tech companies. Last August, the People's Bank of China ordered mobile and online payment companies to connect to a central government clearinghouse, giving regulators access to transaction data. Two months later, The Wall Street Journal reported that Chinese internet regulators were considering taking a 1 percent stake in the major tech companies.

One possible scenario for a social credit partnership is that the central bank will oversee the development of a broader metric, like a FICO score, while letting companies like Ant Financial collect data to feed into that score. Whatever its eventual structure, the larger social credit system "will definitely be under the government's control," says You Xi, the reporter who wrote the book about Ant Financial. "The government doesn't want this very important infrastructure of the people's credit in one big company's hands."

Chinese people who have been branded untrustworthy are getting the first glimpse of what a unified system might mean. One day last May, Liu Hu, a 42-year-old journalist, opened a travel app to book a flight. But when he entered his name and national ID number, the app informed him that the transaction wouldn't go through because he was on the Supreme People's Court blacklist. This list—literally, the List of Dishonest People—is the same one that is integrated into Zhima Credit. In 2015 Liu had been sued for defamation by the subject of a story he'd written, and a court had ordered him to pay $1,350. He paid the fine, and even photographed the bank transfer slip and messaged the photo to the judge in the case. Perplexed as to why he was still on the

list, he contacted the judge and learned that, while transferring his fine, he had entered the wrong account number. He hurried to transfer the money again, following up to make sure the court had received it. This time the judge did not reply.

Although Liu hadn't signed up for Zhima Credit, the blacklist caught up with him in other ways. He became, effectively, a second-class citizen. He was banned from most forms of travel; he could only book the lowest classes of seat on the slowest trains. He could not buy certain consumer goods or stay at luxury hotels, and he was ineligible for large bank loans. Worse still, the blacklist was public. Liu had already spent a year in jail once before on charges of "fabricating and spreading rumors" after reporting on the shady dealings of a vice-mayor of Chongqing. The memory of imprisonment left him stoic about this new, more invisible punishment. At least he was still with his wife and daughter.

Still, Liu took to his blog to stir up sympathy and convince the judge to take him off the list. As of October he was still on it. "There is almost no oversight of the court executors" who maintain the blacklist, he told me. "There are many mistakes in implementation that go uncorrected." If Liu had a Zhima Credit score, his troubles would have been compounded by other worries. The way Zhima Credit is designed, being blacklisted sends you on a rapid downward spiral. First your score drops. Then your friends hear you are on the blacklist and, fearful that their scores might be affected, quietly drop you as a contact. The algorithm notices, and your score plummets further.

SOON AFTER I returned to the US from my visit to China, Equifax, the US credit-reporting agency, announced that it had been hacked. The breach exposed the credit records of some 145 million people. Like many Americans, I got a quick and hard lesson. My credit card number had been stolen a few weeks earlier, but because I had been traveling overseas I hadn't bothered to freeze my credit. When I tried to do so after the hack, I found that an already difficult process had become nearly impossible. Equifax's site was only partly operational, and its phone lines were jammed. Desperate, I signed up for a credit-monitoring service called Credit Karma, which, in exchange for the very same information that I was trying to protect, showed me my score with two of the three major bureaus.

These numbers were communicated to me through a credit gauge similar to Zhima Credit's, down to the color coding of scores. I learned that my credit score had dipped by a few dozen points. There were four or five attempts to take out credit in my name that I didn't recognize.

Now I had two tracking systems scoring me, on opposite sides of the globe. But these were only the scores that I knew about. Most Americans have dozens of scores, many of them drawn from behavioral and demographic metrics similar to those used by Zhima Credit, and most of them held by companies that give us no chance to opt out. Others we enter into voluntarily. The US government can't legally compel me to participate in some massive data-driven social experiment, but I give up my data to private companies every day. I trust these corporations enough to participate in their vast scoring experiments. I post my thoughts and feelings on Facebook and leave long trails of purchases on Amazon and eBay. I rate others in Airbnb and Uber and care a little too much about how others rate me. There is not yet a great American super app, and the scores compiled by data brokers are mainly used to better target ads, not to exert social control. But through a process called identity resolution, data aggregators can use the clues I leave behind to merge my data from various sources.

Do you take antidepressants? Frequently return clothes to retailers? Write your name in all caps when filling out online forms? Data brokers collect all of this information and more. As in China, you may even be penalized for who your friends are. In 2012, Facebook patented a method of credit assessment that could consider the credit scores of people in your network. The patent describes a tool that arrives at an average credit score for your friends and rejects a loan application if that average is below a certain minimum. The company has since revised its platform policies to prohibit outside lenders from using Facebook data to determine credit eligibility. The company could still decide to get into the credit business itself, though. ("We often seek patents for technology we never implement, and patents should not be taken as an indication of future plans," a Facebook spokesperson said in response to questions about the credit patent.) "You could imagine a future where people are watching to see if their friends' credit is dropping and then dropping their friends if that affects them," says Frank Pasquale, a big-data expert at University of Maryland Carey School of Law. "That's terrifying."

Often, data brokers are flat-out wrong. The data broker Acxiom, which provides some information about what it collects on a site called AboutTheData.com, has me pegged as a single woman with a high school education and a "likely Las Vegas gambler," when in fact I'm married, have a master's degree, and have never even bought a lottery ticket. But it is impossible to challenge these assessments, since we're never told that they exist. I know more about Zhima Credit's algorithm than I do about how US data brokers rate me. This is, as Pasquale points out in his book The Black Box Society, essentially a "one-way mirror."

After I left China, I checked back in with Lazarus Liu on WeChat. He sent me a screenshot of his Zhima Credit score, which had increased by eight points since we met. His screen read "Fantastic," and the font had shifted to soft italics.

We talked about a new facial recognition feature called Smile to Pay that Ant Financial had introduced at a concept restaurant in Hangzhou owned by KFC. The walls of the restaurant were adorned with gigantic white phones. To order, you simply tapped a picture of what you wanted and then showed the phone your face, typing in your cell phone number to confirm payment. First smartphones had eliminated the need for a wallet; now Smile to Pay eliminated the need for a phone. All you needed was your face.

Liu wasn't eager to try Smile to Pay. The "government affairs" page on Zhima Credit's website suggests that Ant Financial partners with local governments throughout China to use its facial recognition capabilities, but that wasn't what made Liu uneasy. While studying abroad, he had played around with Android's Face Unlock feature. His roommate, who shared his square jaw, had been able to unlock his phone a few times. "I feel that it could be unsafe," he messaged me. "I would want to see that it's the real thing." He wrote real thing in English, for emphasis.

While chatting with Liu, I, too, had opened up Zhima Credit. My score had increased by four points. "You still have room to improve," the app informed me delicately. But next to my new score, 554, was a small green arrow. I was on my way up.

Mara Hvistendahl (@marahvistendahl) is a national fellow at New America and a contributing correspondent at Science.

This article appears in the January issue

STYLING BY NICOLE SCHNEIDER; ON-SET STYLING BY CRISTINA FACUND

Life in the fishbowl

In the future, most people will live in a total surveillance state – and some of us might even like it

Suppose you're walking home one night, alone, and you decide to take a shortcut through a dark alley. You make it halfway through, when suddenly you hear some drunks stumbling behind you. Some of them are shouting curses. They look large and powerful, and there are several of them. Nonetheless, you feel safe, because you know someone is watching.

You know this because you live in the future where surveillance is universal, ubiquitous and unavoidable. Governments and large corporations have spread cameras, microphones and other tracking devices all across the globe, and they also have the capacity to store and process oceans of surveillance data in real time. Big Brother not only watches your sex life, he analyses it. It sounds nightmarish —but it might be inevitable. So far, attempts to control surveillance have generally failed. We could be headed straight for the panopticon, and if recent news developments are any indication, it might not take that long to get there.

Maybe we should start preparing. And not just by wringing our hands or mounting attempts to defeat surveillance. For if there's a chance that the panopticon is inevitable, we ought to do some hard thinking about its positive aspects. Cataloguing the downsides of mass surveillance is important, essential even. But we have a whole literature devoted to that. Instead, let's explore its potential benefits.

The first, and most obvious, advantage of mass surveillance is a drastic reduction in crime. Indeed, this is the advantage most often put forward by surveillance proponents today. The evidence as to whether current surveillance achieves this is ambiguous; cameras, for instance, seem to have an effect on property crime, but not on incidences of violence. But today's world is very different from a panopticon full of automatically analysed surveillance devices that leave few zones of darkness.

If calibrated properly, total surveillance might eradicate certain types of crime almost entirely. People respond well to inevitable consequences, especially those that follow swiftly on the heels of their conduct. Few would commit easily monitored crimes such as assault or breaking and entering, if it meant being handcuffed within minutes. This kind of ultra-efficient police capability would require not only sensors capable of recording crimes, but also advanced computer vision and recognition algorithms capable of detecting crimes quickly. There has been some recent progress on such algorithms, with further improvements expected. In theory, they would be able to alert the police in real time, while the crime was still ongoing. Prompt police responses would create near-perfect deterrence, and violent crime would be reduced to a few remaining incidents of overwhelming passion or extreme irrationality.

If surveillance recordings were stored for later analysis, other types of crimes could be eradicated as well, because perpetrators would fear later discovery and punishment. We could expect crimes such as low-level corruption to vanish, because bribes would become perilous (to demand or receive) for those who are constantly under watch. We would likely see a similar reduction in police brutality. There might be an initial spike in detected cases of police brutality under a total surveillance regime, as incidents that would previously have gone unnoticed came to light, but then, after a short while, the numbers would tumble. Ubiquitous video recording, mobile and otherwise, has already begun to expose such incidents.

On a smaller scale, mass surveillance would combat all kinds of abuses that currently go unreported because the abuser has power over the abused. You see this dynamic in a variety of scenarios, from the dramatic (child abuse) to the more mundane (line managers insisting on illegal, unpaid overtime). Even if the victim is too scared to report the crime, the simple fact that the recordings existed would go a long way towards equalising existing power differentials. There would be the constant risk of some auditor or analyst stumbling on the recording, and once the abused was out of the abuser's control (grown up, in another job) they could retaliate and complain, proof in hand. The possibility of deferred vengeance would make abuse much less likely to occur in the first place.

With reduced crime, we could also expect a significant reduction in police work and, by extension, police numbers. Beyond a rapid-reaction force tasked with responding to rare crimes of passion, there would be no need to keep a large police force on hand. And there would also be no need for them to enjoy the special rights they do today. Police officers can, on mere suspicion, detain you, search your person, interrogate you, and sometimes enter your home. They can also arrest you on suspicion of vague 'crimes' such as 'loitering with intent'. Our present police force is given these powers because it needs to be able to investigate. Police officers can't be expected to know who committed what crime, and when, so they need extra powers to be able to figure this out, and still more special powers to protect themselves while they do so. But in a total-surveillance world, there would be no need for humans to have such extensive powers of investigation. For most crimes, guilt or innocence would be obvious and easy

to establish from the recordings. The police's role could be reduced to arresting specific individuals, who have violated specific laws.

If all goes well, there might be fewer laws for the police to enforce. Most countries currently have an excess of laws, criminalising all sorts of behaviour. This is only tolerated because of selective enforcement; the laws are enforced very rarely, or only against marginalised groups. But if everyone was suddenly subject to enforcement, there would have to be a mass legal repeal. When spliffs on private yachts are punished as severely as spliffs in the ghetto, you can expect the marijuana legalisation movement to gather steam. When it becomes glaringly obvious that most people simply can't follow all the rules they're supposed to, these rules will have to be reformed. In the end, there is a chance that mass surveillance could result in more personal freedom, not less.

The military is another arm of state power that is ripe for a surveillance-inspired shrinking. If cross-border surveillance becomes ubiquitous and effective, we could see a reduction in the $1.7 trillion that the world spends on the military each year. Previous attempts to reduce armaments have ultimately been stymied by a lack of reliable verification. Countries can never trust that their enemies aren't cheating, and that encourages them to cheat themselves. Arms races are also made worse by a psychological phenomenon, whereby each side interprets the actions of the other as a dangerous provocation, while interpreting its own as purely defensive or reactive. With cross-border mass surveillance, countries could check that others are abiding by the rules, and that they weren't covertly preparing for an attack. If intelligence agencies were to use all the new data to become more sophisticated observers, countries might develop a better understanding of each other. Not in the hand-holding, peace-and-love sense, but in knowing what is a genuine threat and what is bluster or posturing. Freed from fear of surprising new weapons, and surprise attacks, countries could safely shrink their militaries. And with reduced armies, we should be able to expect reduced warfare, continuing the historical trend in conflict reduction since the end of the Second World War.

Of course, these considerations pale when compared with the potential for mass surveillance to help prevent global catastrophic risks, and other huge disasters. Pandemics, to name just one example, are among the deadliest dangers facing the human race. The Black Death killed a third of Europe's population in the 14th century and, in the early 20th century, the Spanish Flu killed off between 50 and 100 million people. In addition, smallpox buried more people than the two world wars combined. There is no reason to think that great pandemics are a thing of the past, and in fact there are reasons to think that another plague could be due soon. There is also the possibility that a pandemic could arise from synthetic biology, the human manipulation of microbes to perform specific tasks. Experts are divided as to the risks involved in this new technology, but they could be tremendous, especially if someone were to release, accidentally or malevolently, infectious agents deliberately engineered for high transmissibility and deadliness.

Mass surveillance could help greatly here, by catching lethal pandemics in their earliest stages, or beforehand, if we were to see one being created artificially. It could also expose lax safety standards or dangerous practices in legitimate organisations. Surveillance could allow for quicker quarantines, and more effective treatment of pandemics. Medicines and doctors could be rushed to exactly the right places, and micro-quarantines could be instituted. More dramatic measures, such as airport closures, are hard to implement on a large scale, but these quick-response tactics could be implemented narrowly and selectively. Most importantly, those infected could be rapidly informed of their condition, allowing them to seek prompt treatment.

With proper procedures and perfect surveillance, we could avoid pandemics altogether. Infections would be quickly isolated and eliminated, and eradication campaigns would be shockingly efficient. Tracking the movements and actions of those who fell ill would make it much easier to research the causes and pathology of diseases. You can imagine how many lives would have been saved had AIDS been sniffed out by epidemiologists more swiftly.

Likewise, mass surveillance could prevent the terrorist use of nukes, dirty bombs, or other futuristic weapons. Instead of blanket bans in dangerous research areas, we could allow research to proceed and use surveillance to catch bad actors and bad practices. We might even see an increase in academic freedom.

Surveillance could also be useful in smaller, more conventional disasters. Knowing where everyone in a city was at the moment an earthquake struck would make rescue services much more effective, and the more cameras around when hurricanes hit, the better. Over time, all of this footage would increase our understanding of disasters, and help us to mitigate their effects.

Indeed, there are whole new bodies of research that could emerge from the data provided by mass surveillance. Instead of formulating theories and laboriously recruiting a biased and sometimes unwilling group for testing, social scientists, economists and epidemiologists could use surveillance data to test their ideas. And they could do it from home, immediately, and have access to the world's entire population. Many theories could be rapidly confirmed or discarded, with great benefit to society. The panopticon would be a research nirvana.

Mass surveillance could also make our lives more convenient, by eliminating the need for passwords. The surveillance system itself could be used for identification, provided the algorithms were sufficiently effective. Instead of Mr John Smith typing in 'passw0rd!!!' to access his computer or '2345' to access his money, the system could simply track where he was at all times, and grant him access to any computers and money he had the right to. Long security lines at airports could also be eliminated. If surveillance can detect prohibited items, then searches are a waste of time. Effective crime detection and deterrence would mean that people would have little reason to lock their cars or their doors.

Doing business in a mass surveillance society would be smoother, too. Outdoor festivals and concerts would no longer need high fences, security patrols, and intimidating warnings. They could simply replace them with clear signs along the boundary of the event, as anyone attending would be identified and billed directly. People could dash into a shop, grab what they needed, and run out, without having to wait in line or check out. The camera system would have already billed them. Drivers who crashed into

parked cars would no longer need to leave a note. They'd be tracked anyway, and insurance companies would have already settled the matter by the time they returned home. Everyday human interactions would be changed in far-reaching ways. Lying and hypocrisy would become practically impossible, and one could no longer project a false image of oneself. In the realm of personal identity, there would be less place for imagination or reinvention, and more place for honesty.

Today's intricate copyright laws could be simplified, and there would be no need for the infantilising mess of reduced functionality that is 'Digital Rights Management'. Surveillance would render DRM completely unnecessary, meaning that anyone who purchased a song could play it anytime, on any machine, while copying it and reusing it to their heart's content. There would be no point in restricting these uses, because the behaviour that copyrights holders object to —passing the music on to others — would be detected and tagged separately. Every time you bought a song, a book, or even a movie, you'd do so knowing that it would be with you wherever you went for the rest of your life.

The virtues and vices of surveillance are the imagined virtues and vices of small villages, which tend to be safe and neighbourly, but prejudiced and judgemental. With the whole world as the village, we can hope that the multiplicity of cultures and lifestyles would reduce a global surveillance culture's built-in potential for prejudice and judgment. With people more trusting, and less fearful, of each other, we could become more willing to help out, more willing to take part in common projects, more pro-social and more considerate. Yes, these potential benefits aren't the whole story on mass surveillance, and I would never argue that they outweigh the potential downsides. But if we're headed into a future panopticon, we'd better brush up on the possible upsides. Because governments might not bestow these benefits willingly —we will have to make sure to demand them.

[Stuart Armstrong](#) is a research fellow at the Future of Humanity Institute in Oxford, where he works on decision theory and the risks of AI.