MENDING CHINA'S DATA FENCES

Online data theft is rife. Will new data protection rules fix the problem?

By Mark Andrews

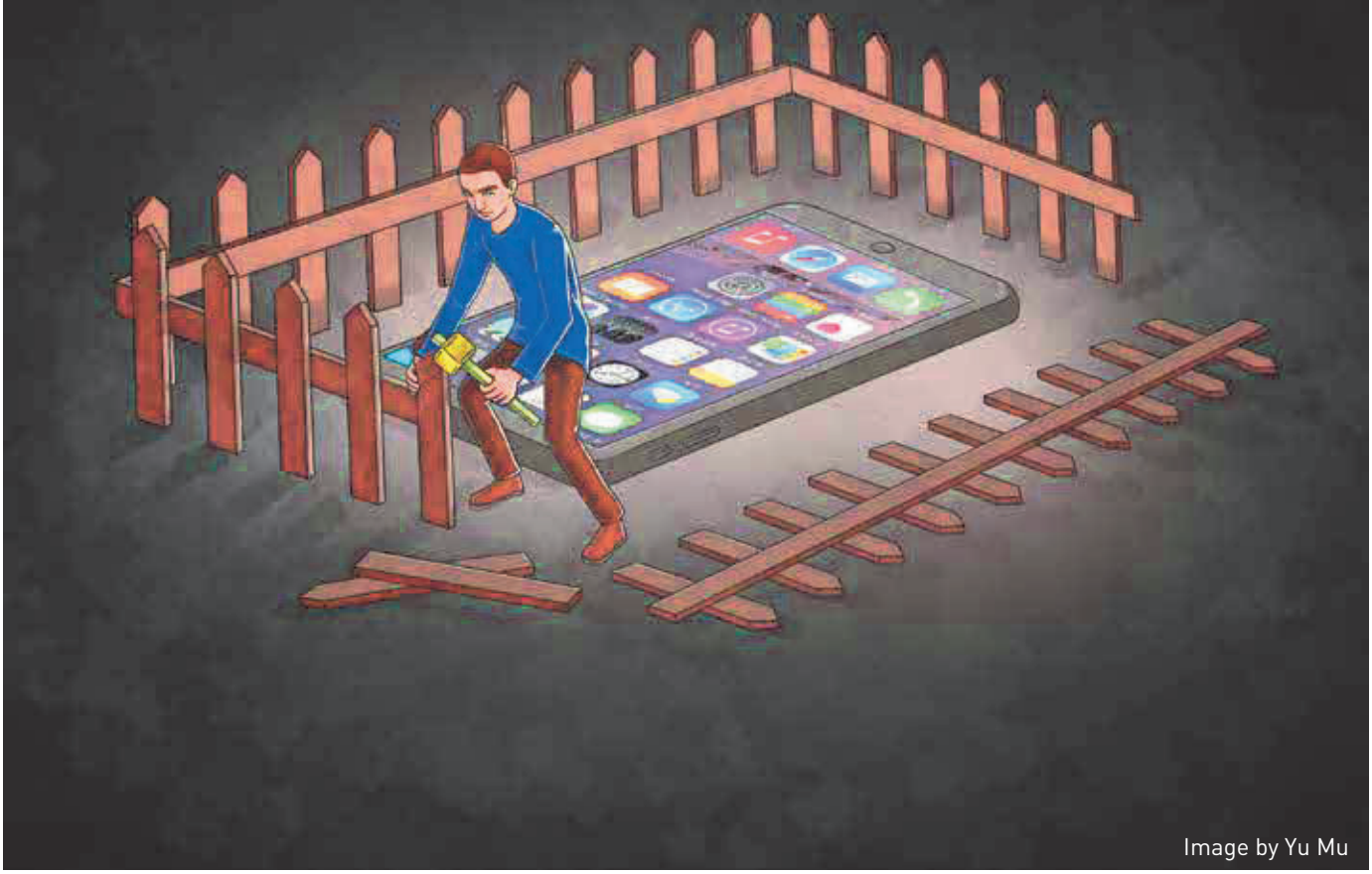


Image by Yu Mu

Online data theft is rife in China, affecting more than 80% of internet users, and tech companies often display a cavalier attitude to using people's personal information. But there are signs that things could be about to change

Film director Jean-Luc Godard once said that art has the power to reveal our most secret selves. For visitors to artist Deng Yufeng's exhibition *Secrets* in Wuhan in April, this proved truer than they could ever have imagined.

Those entering the gallery found a wall of blue screens displaying the personal information of thousands of people: names, ages, heights, telephone numbers, bank details and even train ticket purchases. Deng had purchased the data online for just a few yuan each.

Police quickly shut down the exhibition and placed Deng under investigation, but the artist had successfully highlighted the ease of purchasing citizens' details on the black market. Data theft is rife, affecting more than 80% of the country's internet users, according to the Internet Security Society of China. Whereas the average data breach in the United States involves 1,458 records, in China it is 11 million.

Many tech companies, both big and small, have a cavalier attitude to the use and sharing of netizens' data. In its 2018 survey of 22 major global internet and telecommunications companies, Ranking Digital Rights scored Baidu bottom among global internet firms and Tencent third worst.

"Baidu and Tencent disclosed hardly any information in the Governance category, which means they are lacking disclosure of commitments to freedom of expression and privacy principles and measures taken to implement those commitments across the company's global operations," Laura Reed, a senior research analyst at Ranking Digital Rights, commented.

But things may be about to change for China's leak-prone tech giants. In May, the government implemented new data protection rules called the Personal Information Security Specification.

Some analysts have hailed the Specification as a watershed for data privacy, with a few even comparing it to the European Union's game-changing General Data Protection Regulation (GDPR) law. While there are important differences between the two, Beijing's new rules appear to reflect a wider shift in the way the Chinese government, companies and consumers perceive online privacy.

Private I

Until recently, there was a widely held belief that consumers simply did not care as much about their privacy as people in the West. China has historically approached the idea of individual privacy differently.

The Chinese word for privacy, *yinsi*, is a homonym of the word for "personal secrets," and word developed a negative connotation after the Chinese Communist Party came to power in 1949. The right to privacy was only added to the constitution in the 1980s, and even then this offered little real protection.

Past studies have also seemed to indicate a lack of concern for data security in China. A 2013 survey of consumers in 12 countries by the Boston Consulting

> Chinese consumers dislike spam calls and emails just as much as everyone else, but until recently that wasn't perceived as a privacy issue
>
> Sara Xia
> Attorney
> Harris Bricken

Volunteers redact sensitive information at Deng Yufeng's exhibition *Secrets*, which displays the data of 300,000 people

Group found that 75% of respondents outside China considered it important to be cautious when sharing personal information online, but only 50% of Chinese respondents agreed.

Baidu CEO Robin Li, then, probably felt like he was swimming with the tide when he told an audience in March this year: "I think Chinese people are more open or less sensitive about the privacy issue. If they are able to trade privacy for convenience, for safety, for efficiency, in a lot of cases they're willing to do that."

But the furious reaction, with a string of negative headlines and social media commenters accusing the tech billionaire of being "shameless," showed he had badly misjudged the public mood.

There is growing evidence that consumers are starting to take the security of their personal information seriously. In a survey by Tencent's research arm Penguin, published in August, only 4% of people reported having no worries about data privacy, while 35% said they were constantly anxious about it.

Pushback against the tech companies is also growing. In January, online payment giant Ant Financial was forced to apologize for enrolling customers in its Sesame Credit scheme, which tracks users' behavior and personal networks, without permission. The same month, a consumer group sued Baidu for monitoring users' phone calls without their consent.

"It's not that consumers didn't care about privacy before," says Sara Xia, an attorney at law firm Harris Bricken. "Chinese consumers dislike spam calls and emails just as much as everyone else in the world, but until recently that wasn't perceived as a privacy issue."

What has changed is that the costs of data theft have become much higher as consumers have moved their finances online. Today, it is common for consumers to manage their money entirely through smartphones, from making day-to-day purchases using mobile payment apps Alipay and WeChat Pay to investing in wealth management products.

"As daily transactions shift to the online space it becomes clear that there are major upsides but also risks," says Samm Sacks, a senior fellow at US think tank Center for Strategic and International Studies (CSIS). Her research focuses on data protection law in China.

These risks became clear in 2016, when Xu Yuyu, an 18-year-old student from a poor family in Shandong Province, died of a heart attack after being conned out of her tuition fees. The scammer had reportedly paid a hacker to steal her financial details.

The trend among online services, such as WeChat, to require users to register using their real names and phone numbers is also worrying consumers. "That awareness creates more concerns about privacy," says Jared Nelson, a partner at MWE China Law Offices.

Online lenders have a record of accessing debtors' contact lists and then harassing their friends and family members with threatening phone calls. In one extreme case, a company even paid local pensioners to follow around customers with a megaphone in an effort to shame them into repaying their loans.

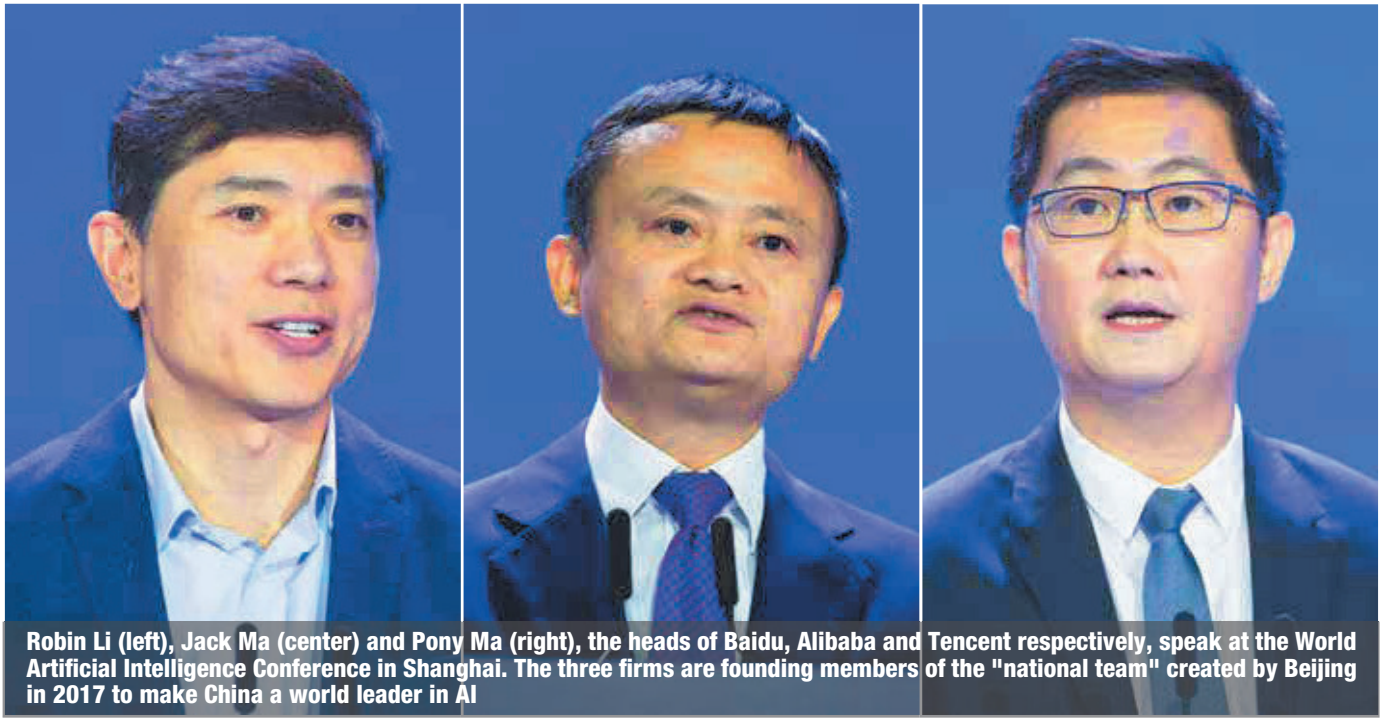
A New Order?

The big question is to what extent the Personal Information Security Specification rules force companies to change their behavior. Analysts remain sharply divided over this issue.

On paper, the Specification appears similar to the EU's GDPR law. "There are places where it seems the rules were very much inspired by the GDPR," says Nelson. "They use the same language, the same types of ideas, the same types of restrictions."

This suggests that China may be inclined to follow the European approach to online regulation, which imposes strict

> It seems the Chinese rules were very much inspired by the EU's GDPR. They use the same types of ideas
>
> Jared Nelson
> Partner
> MWE China Law Offices



Robin Li (left), Jack Ma (center) and Pony Ma (right), the heads of Baidu, Alibaba and Tencent respectively, speak at the World Artificial Intelligence Conference in Shanghai. The three firms are founding members of the "national team" created by Beijing in 2017 to make China a world leader in AI

rules on tech companies, rather than the more laissez-faire American model.

As with the GDPR, the Specification not only states that companies must obtain the explicit consent of users to collect data, but it also says that companies should only obtain data that is necessary to the functioning of their services.

This means that, in theory at least, tech companies will no longer be able to force users to grant access to a huge range of data when they download an app, as has been the case in the past. A recent investigation of 200 Chinese finance apps found that 95 asked to read users' text messages and 97 wanted access to customers' contact lists, according to the *Financial Times*.

However, there is one crucial difference between the Chinese and European rules that is causing confusion. GDPR is a law with clear penalties, but the Specification, despite laying out detailed requirements, is merely a set of guidelines. Designed to add flesh to the bones of China's Cybersecurity Law, which came into effect in June 2017, the Specification only advises companies on how they should comply with the law.

"If a company's data practice is inconsistent with the Specification, it is not automatically in violation of any law," says Xia, of Harris Bricken.

Nevertheless, Sacks insists that the Specification will be far from toothless. "If regulators wanted to crack down on a company they could use this as a tool to do an audit," she says. "While it's not necessary for everyone to comply, companies that don't are vulnerable if there is some sort of *ad hoc* enforcement."

Many companies have rushed to hire compliance officers and data protection lawyers to help them comply with the new regulations. According to Nelson, most internet companies are not even close to full compliance, but in general firms see the rules as something they should follow.

"The government has already been enforcing the rules in place," says Nelson, adding that his clients in a variety of industries have received questions about their websites and WeChat accounts.

Data Wars

China is still in the early stages of deciding how strictly it wants to clamp down on data-hungry tech companies. While it is under pressure from data protection advocates, it is also wary of harming emerging industries like artificial intelligence (AI).

Beijing has identified AI as one of ten strategic industries that it wants to lead in the future. In the global AI race, the ability of Chinese companies to hoover up vast volumes of data on the country's 900 million internet users is widely seen as giving them a head-start. As a result, the government may be hesitant to restrict access to the world's largest data reserves.

"Companies right now are moving aggressively to be innovators in the AI space, and to do that they need to train algorithms using datasets with lots of information," says Sacks. "If you overly restrict the companies with these rules, you undermine Beijing's goal to be a global AI leader."

Other experts are more optimistic that Beijing can reconcile data protection with the needs of the country's tech industry. As an executive at e-CarX, a connected-car system developer owned by auto group Geely, points out, personal information is of little value for many big-data products.

"We are unable to identify a user and see where they went on any given day," says the executive, who is speaking on

condition of anonymity. "In fact, the data of individual users is not useful to us; it is only useful when data from all our users is pooled."

This is not the case in other industries, such as e-commerce, digital advertising and facial recognition. But even in these industries, some argue that the value of truly enormous datasets is overrated.

"Data is a key input into AI research and drives forward commercialization, but at a certain point having more data brings diminishing marginal returns," says Jeffrey Ding, a researcher at the University of Oxford's Future of Humanity Institute.

According to Ding, global companies like Facebook have an advantage in terms of the breadth of data they hold, while Chinese companies have the edge in terms of the depth of their datasets. But because this data relates mostly to China, it may be of limited use when developing products for overseas markets.

When it comes to innovation in AI, other reforms could have a far greater long-term impact than the data protection rules. One example is the government's mooted plan to force AI companies to pool their data in public shared databases.

If implemented, the public databases would be a game-changer for AI researchers across the world, but the move would be highly disruptive for leading tech giants, which guard their data jealously.

> **If you overly restrict companies, you undermine Beijing's goal to be a global AI leader**
>
> Samm Sacks
> Senior Fellow
> Center for Strategic and International Studies

According to Ding, the policy would also be tough to implement as companies use different data protocols.

And there is another reason why the government may disregard the lobbying of the tech industry and prioritize data protection. Beijing has called for the creation of a national social credit scheme by 2020. The project functions like a credit scoring system and is designed to make up for the fact that a large percentage of people in China have no credit history at all—the country has only 300 million credit card users.

But the social credit system goes much further, drawing on a huge range of user data from online platforms such as Alipay to assess a person's overall trustworthiness. Existing trial systems use a carrot-and-stick approach to reward users with high scores and punish misbehavior—for example, by banning users from buying train or plane tickets.

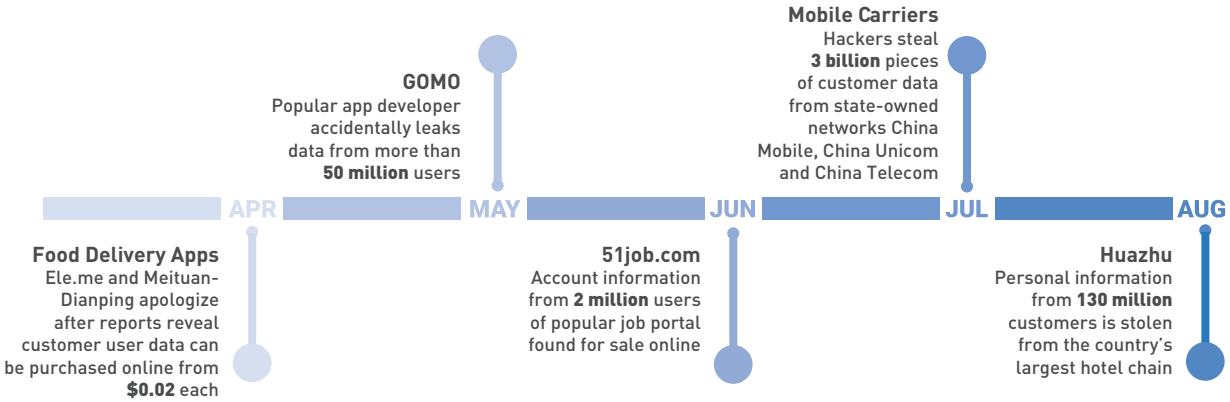
At the moment, there are no signs of a widespread pushback against the social credit system, but this could change if public trust in companies involved in the project, such as Ant Financial, deteriorate.

"Growing awareness toward misuse of user data could ensure that any social credit system must have limits on the extent to which it collects personal information on citizens," says Ding.

"[The government] runs the risk of a public backlash, like the one suffered by Ant over Sesame Credit, if the public fails to see the use of the social credit system as legitimate," agrees Sacks.

A YEAR OF LEAKS

A series of huge data breaches have rocked the Chinese internet in 2018



Source: IDC Worldwide