Social control 4.0? China’s Social Credit Systems

Katika Kühnreich
10 August 2018

China’s digital Social Credit Systems operate a form of gamified control, rewarding users while rating them according to online and offline behaviour. By 2020, the Chinese government plans to introduce a nationwide system. Western observers are appalled, but are our own social media essentially all that different?

With China’s geopolitical ambitions currently at the centre of attention, the domestic policies of the Communist Party of China (CPC) are going largely unnoticed. [1] Yet it is becoming clear that internally, China is also undergoing wholesale transformation: by the year 2020, the CPC aims to introduce digital systems for social control nationwide. Through the Social Credit Systems (SCSs), some of which have already been in operation for four years, the ambition is to produce a score for every Chinese citizen based on their behaviour. [2]

An enormous amount of data is being captured to calculate this: payment practices, criminal records, shopping habits, online browsing and messaging behaviours as well as social behaviour in general. Conformity leads to rewards such as cheap credit, job progression or a speedier journey through security checks. By contrast, undesirable behaviour carries the risk of punishment.

The SCSs have access to many private and state databases. In 2014, the CPC permitted eight private providers to develop their own digital rating systems. All the systems use algorithms and artificial intelligence (AI) to calculate points or scores in an automated process. At the same time, the CPC began installing state scoring systems in selected ‘Special Zones’. [3] When the SCSs are made mandatory across the country in around two years’ time, the intention is that all Chinese citizens as well as companies will have access to their own centrally recorded points account.

The CPC is promoting the SCSs as a milestone on the path towards the ‘Socialist Harmonious Society’. Officially, the scoring systems are intended to modernise governing capacity and promote trust within society as well as between the government, population and economy. However, the capabilities afforded by the systems also mean that they can be viewed as an instrument of social control. With China’s economic rise over the past decades, there has been a growth in socio-economic inequality, resulting in social
tensions. In 2014 alone – the first year of the SCSs – there were a total of around 90,000 disturbances in China, officially described as ‘mass incidents’ – an average of around 250 per day. This figure has since risen. [4]

Photo source: Flickr

**Instruments of social control**

In order to deal with these disturbances, China is drawing on its millennia-old tradition of state centralisation and bureaucracy. Systems of control justified through Confucianism partly persisted in the Leninist organisation of the People’s Republic. These included the household registration system *Hukou* and the assignment to a social unit known as *Danwei* – where each unit supervised its members and kept political records on them (*Dang’an*).

These structures formed the basis for decisions on promotions, party membership and even marriages. After the death of Mao Zedong, some systems of control lost significance as a consequence of the political transformations of the reform era. However, state propaganda became more significant after 1989. [5]

With the SCSs, China is entering a new phase of surveillance and control in which the CPC is combining the potential of analogue and digital surveillance, of propaganda and subtle forms of discipline. The development of the Internet as well as mobile devices like smartphones (‘smarps’) and wearables – smart watches or glasses – has offered security services and propaganda departments new means of surveillance and influence.

At the same time, the CPC is profiting from the idiosyncrasies of the Chinese Internet. [6] Not only is the Chinese web subject to strict regulations, access is also restricted by the ‘Great Firewall’. Internally, the ‘Golden Shield Project’ is the principle means of monitoring online events. This includes the ‘Bureau of Public Information and Network Security Supervision’, or the ‘Network Supervision Bureau’ for short. There are also several other government departments, ministries and authorities responsible for internet surveillance. [7]

Alongside a growing number of specially trained police officers and inspectors employed from the private sector, AI systems are increasingly being used to trawl the Internet for any statements critical of the regime. [8] Additionally, an army of regime-friendly commentators are active in online forums, known colloquially as the ‘Fifty Cent Party’ (五毛). They are accused of attempting to influence public debate in support of the CPC. [9]

**China’s web giants: Baidu, Alibaba and Tencent**

The CPC itself viewed the Internet from its very inception as a form of communication to be controlled. State censorship measures are not, however, aimed at suppressing critical comment about the regime completely. Rather, the CPC seeks to pre-empt the emergence of large-scale collective action. [10] Furthermore, as with censorship measures in general, many of the Chinese attempts at control can be at least partly circumvented.
China therefore has a relatively heterogeneous online landscape.

This landscape is nonetheless different from that in the West. Since the Chinese web is largely screened off from the rest of the World Wide Web, it is also not dominated by the US tech giants. Instead, distinct commercial structures have formed. The three largest companies – Baidu (百度), Alibaba (阿里巴巴) and Tencent (腾讯) – are known as BAT. They not only supply the infrastructure for the SCSs but are also at the forefront in the development of AI worldwide.

All three companies have access to enormous reserves of data. [11] The search engine giant Baidu also operates China’s largest online encyclopaedia and the payment app Baidu Pay. Alibaba, the company known to most western customers as ‘AliExpress’, is in turn the biggest player in Chinese online retail. It also provides a popular consumer-to-consumer platform, Taobao Wang, used by approximately 470 million people a month. In addition, Alibaba holds about a third of the shares in China’s most popular microblogging platform, Sina Weibo, used by around 380 million Chinese people monthly. The company’s financial services group includes the social credit system ‘Sesame Credit’ and the popular payment app Alipay. In the past year, the Alibaba Group announced turnover of around 8.3 billion US dollars. Since 2016, it has also been the owner of the Hong Kong-based daily, South China Morning Post.

The third company in the group, Téngxùn, is known in the West as Tencent. Amongst gamers, it has been a household name outside China for many years due to its involvements in video game companies. However, Tencent also has shares in the globally popular social media (SocMe) service Snapchat – a fact that is much less well known. Further key services are QQ and WeChat: with almost 900 million active users, QQ is China’s most popular messaging service; WeChat is a messaging app for smarps that reaches around a billion people worldwide. With the WeChat Pay option it also constitutes a payment app used across China. [12]

(Meta) data and other digital traces

For Chinese Internet users, these services are part of everyday life. Around 95 per cent of users access the web either via a mobile device, either in addition to a PC or exclusively. [13] Like any web user, they leave behind huge digital footprints – personal details and data about their online behaviour – which is collected and evaluated by both commercial and state entities, which can then identify, categorise and classify users. [14] This data forms the basis for the SCSs and score calculation. The scoring is carried out with the assistance of algorithms and AI systems – a process which is not made transparent to users.

Digital systems have two further traits that are particularly relevant for the SCSs: on the one hand, stored data can be duplicated and traded any number of times; on the other hand, digital systems do not forget. What is more, the Chinese SCSs constitute hybrid systems: they incorporate both digital and analogue data in their evaluations, in other words not only online but also offline patterns of behaviour. This has been enabled partly through the increased use of ‘smart’ cameras with facial recognition in public spaces. [15] The integration of analogue and digital surveillance is particularly advanced in the predominantly Muslim province of Xinjiang – where the number of ‘mass incidents’ is also
comparatively high.

**Alibaba’s Sesame Credit**

Alibaba’s Sesame Credit System provides a good illustration of how scoring is carried out. Like western companies, Alibaba skims off massive amounts of data from its users, as SocMe services supply information on their moods, preferences and ‘friendships’. Data on product orders and interactions with web banners is also captured in detail. At least as important are payment processes and internet searches, which are augmented with metadata on pages accessed and dynamic data. Scoring is then made within five areas: the user’s credit history, their liquidity, their personal details, their habits and behavioural patterns, and their SocMe contacts. [16] The lowest Sesame Credit System score is 350 and the maximum 950. The current evaluation process rates the use of Alibaba products particularly highly.

Alibaba’s Sesame Credit System in some ways resembles bonus programmes like the Payback loyalty card in Germany. By registering for this service and thereby permitting the release, use and sale of personal data, users receive concessions which increase with their score. In the Sesame Credit System, users can – after a specified score level – apply for immediate loans or loan products, without also having to pay a deposit.

Even in areas related to security, there are advantages to be gained. After a certain score level, security checks at airports can be passed through more quickly. Benefits are available outside China too: as of 2015, the embassies of Singapore and Luxembourg offer simplified Visa conditions for Chinese citizens who have reached a certain number of points. [17] In order to calculate this, the Sesame Credit System collaborates with numerous other commercial and public databases – including, also since 2015, China’s largest dating service Baihe, which holds intimate data on around 90 million people. The Sesame Credit System also incorporates databases from Chinese courts – with consequences for those with convictions, who have to accept additional restrictions. [18]

The implications of this are demonstrated by one of the latest clampdowns: as of 1 May 2018, citizens on a government blacklist can be prevented from traveling by rail or by air for up to a year. [19] Sanctions were already possible – albeit in a milder form: last March the National Development and Reform Commission disclosed that so far over 9 million people had been banned from flying, while more than three million had been unable to buy top-class train tickets because of negative data entries. [20] Those affected include people who had supposedly published false information on terrorism – an offence open to flexible interpretation worldwide.

**Playful surveillance: The gamification principle**

It remains to be seen how extensive the SCSs will be in 2020, when the CPC aims to introduce them nationwide. In the West, they are already being compared with two classic conceptions of the penal and disciplinary system: Bentham’s panopticon – in particular in its interpretation by Michel Foucault – and George Orwell’s dystopia, *1984*. [21] However, such comparisons do not capture the full dimensions of the SCSs. The Chinese scoring systems are a form of technological surveillance involving commercial and state actors in equal measure. At the same time, and unlike Orwell’s ‘Big Brother’,
they are characterised by elements of participatory play, and therefore by a far greater degree of free will and involvement from those observed.

The technique known as ‘gamification’, which plays an important part in the development of computer games, plays a key role. [22] Its aim is to hold the attention of players for as long as possible, simultaneously generating positive emotions towards the game. Today, gamification is deployed in practically all areas of society – including in the military, management and advertising.

The SCSs motivate users not only through scores, but also through variations in level and ‘mini games’. Scoring allows people to compare themselves with each other, thus encouraging them to increase their own score. Even the prospect of receiving small awards when on a low score motivates people to participate – an effect also evidenced in the popularity of loyalty programmes in the West. Recruitment is a snowball effect: having been enlisted, users in turn advertise the product to those in their own social circles, luring more people into the system. The services are thus able not only to gain a large market share, but also to become monopolies.

In East as in West: The net under surveillance

Although forms of playful surveillance are by no means used only in China, the typical reaction in the West to reports on Chinese SCSs is one of perturbation. This shows not only that western prejudices about China still exist, but also how uncritically processes of digitalisation are perceived in this part of the world.

Western discourse all too often ignores the fact that the great majority of the Internet is already commercialised through and through. It is a space where companies collect and evaluate massive amounts of data in order to produce and sell detailed user profiles. [23] This spying ranges from credit data evaluation to the investigation of consumer behaviour through loyalty systems, and from bike and car hire services to petition platforms such as Change.org. [24]

In the West too, this continual process of comparison and evaluation is leading to the steady dissolution of the private sphere, alongside a culture of conformity in private life and an increasing avoidance of risk in professional life. [25] As a result, there is a threat of greater ‘social rigidity’, which makes action against injustice and inequity more difficult. [26] This development has been made easier by the widespread assumption that data and especially algorithms are largely neutral – despite the fact that computer code is written by people with their own personal convictions, who of course also make mistakes. [27]

In addition to this comes the fact that it is above all companies and states that are driving digitalisation, meaning they are the ones who determine its direction. Even if governments, in contrast to private companies, must at least theoretically justify themselves to their citizens, we have known at the latest since the Snowden leaks that western states crave data just as much as authoritarian regimes. Even a good five years after the NSA affair, nothing has changed in this regard. On the contrary, online surveillance has since become even more profuse – not least thanks to collaboration between governments and the private sector. [28]
For individuals, protecting oneself against mass surveillance is becoming ever more difficult – especially since we understand less and less about the ‘smart’ devices that we use every day and the techniques of manipulation that are employed. Hardly anyone knows what data traces are left behind when surfing the internet unprotected, let alone what detailed conclusions can be drawn from this data about our personal thoughts and desires. We are thus not fully aware of how far our private sphere is already being dissolved. Encryption and anonymisation services do offer some protection, but they cannot answer the questions of how technology and digitalisation are changing our society for better or worse.

Alongside illegal access, databases conceal another underestimated danger. Governments and companies can pass away, but the data remains. We cannot foresee the conclusions that future governments or companies and their CEOs will draw from our data or the categories and algorithms by which we will be evaluated.

The Chinese SCSs therefore pose to all of us the question of why massive amounts of data about us are collected, moved, evaluated and sold. What kind of society will digital mass surveillance lead to? And what can we do to counter it? One thing is clear: data is power. It is a power that we cannot physically sense and hence, much like nuclear radiation, one whose dangers we can only dimly perceive. It is therefore time to deal globally with the question of the shift of power and manipulation in the age of digitalisation. Its implications force us to pose anew questions of power and legitimacy, privacy, autonomy and the good life – and to decide whether we want to remain passive users or become actively involved in shaping systems that influence our lives.

**Footnotes**


7. This coexistence and interdependence of jurisdictions is typical of the Chinese Internet. It makes it more difficult for citizens to intervene, which also affects issues of data protection, since there is no central point of contact.


11. Tencent’s SCS caused controversy as it was one of the first to also factor in its customer’s friendship circles when calculating creditworthiness. See Meng Jing, ‘Tencent to use social networks for credit-rating services’, www.chinadaily.com.cn, 8.8.2015.


14. This practice was originally used in criminology and psychiatry to identify deviant behaviour. For more on this see: Andreas Bernard, *Komplizen des Erkennungsdienstes: Das Selbst in der digitalen Kultur*, Frankfurt a. M. 2017 [The Triumph of Profiling: forthcoming, Polity Press].


