Big Brother is Lurking

With increasing technology and data acquisition, their misuse and discrimination should be dealt with through legislation and enforcement to protect the privacy of individuals

By Shaan Katari Libby

MONITORING LIVES
Facial recognition, a booming, yet controversial, technology, is being harnessed by several countries, including India

"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time."

—George Orwell's *1984*, a dystopian fiction of the future, complete with Two Minutes of Hate each day and condemnation of any counter-revolutionary activities. This final book of Orwell is fast becoming frighteningly real today in some jurisdictions.

LET'S start with China. Private information is required for routine transactions there. Tragedies have ensued with telecom fraud increasing by 36.4 percent between 2015 and 2016 alone; a teenager died in 2016 after a heart attack when her university tuition was stolen and a college professor lost CNY17 million. The government responded to all this by publishing several laws to protect private information, giving users the ability to agree to the purpose, method and scope. Supervision and security requirements are now in place for the telecom, healthcare and education industries.

However, the government has also efficiently used technology to its own advantage, leaping ahead of the game in the areas of artificial intelligence and facial recognition. China has been in the lead when it comes to the rollout of facial recognition technology from transport hubs to schools, shopping centres and residential complexes. Studies done by the Nandu Personal Information Protection Centre, Beijing, have revealed that 74 percent of the responders were concerned about this and prefer traditional forms of ID over facial recognition. The chief worry is that the operators will be lax with the data. There is also a worry that their movements are being tracked by unknown watchers.

UNI

Due to the Aadhaar card exercise, India now has the biometric data of 1.2 billion people, ie, one-sixth of humanity. The Aadhaar Act was found to be an exception to the right to privacy by the SC.

The thing with facial recognition is that unlike fingerprints, one need not be near the camera—it just picks up some nodal points and having scanned you, "recognises" you instantly. This is also being used for payments instead of using cash or a QR code. Bank accounts are linked to the faces of customers and automatically debited. The Chinese ministry of public security has been building the world's most extensive facial recognition database.

Over 120 million Chinese citizens today pay using Alipay, a mobile payment app that uses only one's face as credentials. Some smartphones work this way. While there is no question about the efficiency of this mode, the concern is privacy. Extensive knowledge is being amassed about where citizens go, what they do, for how long and who is or is not financially secure.

Further, China has a "social credit" system in place, reminiscent of the Orewellian notion of Big Brother watching you. All aspects of the life of a citizen are judged—behaviour and trustworthiness. Jaywalking or failing to pay a court bill, playing music loudly in a public space, and such other "transgressions" can make one lose one's rights to, say, booking a train ticket. This is already in place piecemeal in local government. When the final version is completed, it plans to hoover up all the data collected by private companies like Alibaba, some of which are already being used for trials.

Ultimately, every individual will have a social credit score and some will simply be blacklisted if they refuse to pay a fine, for instance. Liu Hu, a journalist in China, wrote about censorship and government corruption and has been arrested, fined, and blacklisted. This means, he is on the List of Dishonest Persons Subject to Enforcement by the Supreme People's Court. He can no longer buy a plane ticket or property or take a loan. All this has been done without any official advance notification. The Communist Party of China is the ultimate arbiter, although in theory, there is a court one can appeal to.

The reasons the government has given for implementing this is to build trust and ensure that Chinese society functions without scandal and pollution. However, the flip side is clear— vague notions like national security and unity of the nation can be worthy of blacklisting. Essentially, any hint of dissent can blot out a person's future. Mindboggling, to say the least.

Repercussions have already been felt during the Hong Kong democracy protests where critical posts were apparently removed and video platforms turned off comments saying there were system upgrades. And virtual private networks which protect privacy online were compromised. The Muslim minority of Uighurs has been subjected to increased surveillance, according to reports, with over 5,00,000 scans of faces conducted. This entire protocol of a social credit system is part of an authoritarian regime, and there is nothing here that a liberal democratic country should aspire to.

Moving now to India. We have been experimenting with many things with regard to criminals. We have a National Crime Records Bureau (NCRB) set up in 1986 to assist investigators. This links 15,000 plus police stations but we have a long way to go to cover the whole country. This would seem to most a welcome step so long as it is for convicted criminals and kept secure. Right now, this is still in the works. This has led to people being hired in our homes without anyone having any idea if they might be rapists or murderers. We go by a whim and a prayer. Within the NCRB's purview is the Central Finger Print Bureau, a national repository of ▶

UNI

CONCERN FOR PRIVACY
The use of drones for surveillance regarding law and order breakdown is debatable

fingerprints with over a million 10-digit fingerprints of convicted criminals as well as those who have been arrested. One hopes the latter are deleted if found not guilty. The Bureau is now linking up with Advanced Facial Recognition Systems and integrating with other central databases of the government. They have also been entrusted with maintaining the National Database of Sexual Offenders which is shared with states/UTs.

The Aadhaar card, which has essentially replaced the ration card for the common man, takes biometric data, both an iris scan and a fingerprint, to identify residents of India and give them access to government welfare schemes. One also needs an Aadhaar to pay income tax.

How do we square this with the right to privacy enshrined in Article 21 of the Constitution? In the case of *Justice Puttuswamy and Anr v Union of India and Ors*, the Supreme Court held that Aadhaar does not violate the fundamental right to privacy when a person agrees to share biometric data. It further held that Aadhaar would be needed for government welfare schemes and PAN card applications, as well as for income tax filing. Overall, the Aadhaar Act was found to be a reasonable exception to the right to privacy as it was backed by a statute (existence of law), passed the test of proportionality and served a legitimate state aim.

The Court did make it harder for private companies to seek Aadhaar data. Justice Chandrachud of the Supreme Court in his dissenting judgment said that constitutional guarantees cannot be compromised by the vicissitudes of technology. He was against the passing of the Aadhaar Act as a money bill, the lack of robust mechanism for protection of personal information and the profiling of citizens. Due to the Aadhaar exercise, India now has the biometric data of 1.2 billion people, ie, one-sixth of humanity. That is a massive responsibility.

When it comes to the right to privacy, the latest use of drones with video enhancement software and forensic tools to help cover processions or marches to watch for any breakdown of law and order could also be a double-edged sword.

Moving to the UK, in 2018, the General Data Protection Regulation (GDPR) came into force to make personal data safer. Individuals will now have the power to demand that companies delete personal data they hold, regulators will be able to work together across the EU and enforcement includes a maximum fine of 20m euros. They now require a data protection officer to be appointed for any police/authority that monitors or tracks behaviour. There are compliance requirements, training and internal audits in place. The watchdog responsible is the Information Commissioner.

Inspired by the GDPR, India has, via the Data Protection Bill 2019, sought to protect an individual's privacy rights but has accorded sweeping powers to itself. This includes obtaining personal information on grounds of sovereignty or public order. Justice BN Srikrishna, chairman of the committee set up by the government to examine the data protection law, has said this is dangerous. Perhaps the government could ensure that the overseeing agency is a politically independent body.

In short, technology, data acquisition, its misuse and discrimination are issues to be grappled with and dealt with responsibly via legislation and enforcement. No country should ever have to witness (or worse, believe) the elegant lettering saying War is Peace; Freedom is Slavery; Ignorance is Strength. ■

—The writer is Barrister-at-Law, Honourable Society of Lincoln's Inn, UK, and a leading advocate in Chennai. With inputs from RK Padmanaban and Tarun M