Perfected in China, a threat in the West

The state can gather more information, more easily, than ever before. Do not underestimate the risks

THEY'RE watching you. When you walk to work, CCTV cameras film you and, increasingly, recognise your face. Drive out of town, and number-plate-reading cameras capture your journey. The smartphone in your pocket leaves a constant digital trail. Browse the web in the privacy of your home, and your actions are logged and analysed. The resulting data can be crunched to create a minute-by-minute record of your life.

Under an authoritarian government such as China's, digital monitoring is turning a nasty police state into a terrifying, all-knowing one. Especially in the western region of Xinjiang, China is applying artificial intelligence (AI) and mass surveillance to create a 21st-century panopticon and impose total control over millions of Uighurs, a Turkic-language Muslim minority (see Briefing). In Western democracies, police and intelligence agencies are using the same surveillance tools to solve and deter crimes and prevent terrorism (see Technology Quarterly). The results are effective, yet deeply worrying.

Between freedom and oppression stands a system to seek the consent of citizens, maintain checks and balances on governments and, when it comes to surveillance, set rules to restrain those who collect and process information. But with data so plentiful and easy to gather, these protections are being eroded. Privacy rules designed for the landline phone, post-box and filing cabinet urgently need to be strengthened for the age of the smartphone, e-mail and cloud computing.

I spy with my many eyes

When East Germany collapsed in 1989, people marvelled at the store of information the Stasi security service had garnered on them, and the vast network of informants it took to compile it. Since then the digital revolution has transformed surveillance, as it has so much else, by making it possible to collect and analyse data on an unprecedented scale. Smartphones, web browsers and sensors provide huge quantities of information that governments can hack or collect; data centres allow them to store it indefinitely; AI helps them find needles in the digital haystacks thus assembled. Technologies that once seemed a friend of freedom, allowing dissidents in dictatorships to communicate and organise more easily, now look more Orwellian, letting autocrats watch people even more closely than the Stasi did.

Xinjiang is the nightmarish extreme that the new technology makes possible: a racist police state. Fearing insurrection and separatism, China's rulers have reinforced techniques of totalitarian control—including the mass detention of Uighurs for re-education—with digital technology. In parts of the province streets have poles bristling with CCTV cameras every 100-200 metres. They record each passing driver's face and the car's numberplate. Uighurs' mobile phones must run government-issued spyware. The data associated with their ID cards include not just name, sex and occupation, but can contain relatives' details, fingerprints, blood type, DNA information, detention record and "reliability status". All this and more is fed into the Integrated Joint Operations Platform (IJOP), an AI-powered system, to generate lists of suspects for detention.

Totalitarianism on Xinjiang's scale may be hard to replicate, even across most of China. Repressing an easily identified minority is easier than ensuring absolute control over entire populations. But elements of China's model of surveillance will surely inspire other autocracies—from Russia to Rwanda to Turkey—to which the necessary hardware will happily be sold. Liberal states have an obligation to expose and chastise this export of oppression, however limited their tools of suasion.

The West must look at itself, too. These days its police forces can also have access to a Stasi's worth of data. Officers can set up bogus phone towers to track people's movements and contacts. Data from numberplate-readers can track a person's movements for years. Some American cities have predictive-policing programs akin to IJOP that analyse past crimes to predict future ones. All this allows the monitoring of possible attackers, but the potential for abuse is great. Hundreds of American police officers are known to have used confidential databases to dig dirt on journalists, ex-girlfriends and others.

Watching the detectives

How to balance freedom and safety? Start by ensuring that the digital world, like the real one, has places where law-abiding people can enjoy privacy. Citizens of liberal democracies do not expect to be frisked without good cause, or have their homes searched without a warrant. Similarly, a mobile phone in a person's pocket should be treated like a filing cabinet at home. Just as filing cabinets can be locked, encryption should not be curtailed. A second priority is to limit how long information on citizens is kept, constrain who has access to it and penalise its misuse fittingly. In 2006 the European Union issued a directive requiring mobile-phone firms to keep customers' metadata for up to two years. That law was struck down by the European Court of Justice in 2014. Misuse of police data should be a criminal offence for which people are punished, not a "mistake" absolved by a collective apology.

A third priority is to monitor the use of AI. Predictive-policing systems are imperfect, better at finding patterns of burglary than of, say, murder. Face-recognition may produce lots of "false positive" results. AI trained with biased data—eg, patterns of arrest that feature a disproportionate number of black people—may reproduce those biases. Some sentencing algorithms are more likely to label black defendants than white ones as being at high risk of reoffending. Such algorithms must be open to scrutiny, not protected as trade secrets.

Vigilance and transparency must be the watchwords. They may enhance the technology's effectiveness: the routine wearing of bodycams by police, for instance, appears to reduce public complaints. Consultation matters, too. A bill recently proposed in California would compel police agencies to disclose what surveillance gear they have, publish data on its use and seek public input before buying any more. If that makes progress slower so be it. Police rightly watch citizens to keep them safe. Citizens must watch the police to remain free. ■