1984 in 2019

The New Privacy Threat from China's Social Credit Surveillance Systems

BY JOHN GLYNN

In George Orwell's classic novel, *1984* the story's protagonist, Winston Smith, is a low-ranking member of the ruling Party in London, in the nation of Oceania. Wherever Winston goes, even within the supposed comfort of his own home, the Party's eyes monitor him through telescreens; everywhere he looks he sees the face of Big Brother, the Party's seemingly omniscient leader. Although Western democracies are nowhere near the extremes of social control envisioned in this cautionary tale, written as it was when the technology was unavailable to even the most industrialized countries, that is no longer the case, as evidenced in recent stories abut China's move to place hundreds of millions of cameras around its country to monitor every move of its citizens.

In *1984*, language is controlled, something that we can see today with mandatory pronouns and the steady stream of misinformation. The Party created by Orwell strives to implement an invented language called Newspeak (alternative facts), which attempts to prevent political rebellion by eliminating all words related to it (fake news); or doublethink, holding two contradictory thoughts at the same time (America first/Putin first). In Orwell's dystopia, even thinking rebellious thoughts is illegal. Such thoughtcrimes are, in fact, the worst of all crimes, even worse than kneeling during the national anthem.

All of this space that we thought was open to us and free for us to express ourselves in suddenly seems somewhat limited, constrained, even controlled, and most certainly monitored. For half a century after the publication of *1984*, it has felt as if society had dodged a bullet, that western democracies were safe, that privacy was guaranteed, and that freedom was a given. When the Snowden revelations came out, however, one thing started to become more apparent: many of Orwell's warnings were, in fact, prophetic. Depending on who you ask, Edward Snowden, a former contractor for the CIA, is either a hero or a traitor. In 2014, after leaking details of extensive Internet and phone surveillance by American intelligence, he fled, seeking refuge in Russia. We now know that the National Security Agency (NSA) and its associated organizations colluded in massive wide scale surveillance of U.S. citizens and foreigners. Prior to Snowden's explosive revelations, most of us had faith in intelligence agencies, believing that specific targeted surveillance was reserved for criminal masterminds and world leaders, but Snowden's revelations blew such notions to smithereens. More troubling still, it emerged that other governments cooperated with, and almost certainly still do, with the United States in the execution of extensive global surveillance. These countries include Australia, Canada and the United Kingdom—three nations with a reputation for egalitarian, anti-totalitarian philosophies.

In modern history, arguably no regime apparatus was more despotic than the East German Stasi. With its monitoring of the population, creating mistrust and a state of widespread fear, the official state security service cracked down on dissenters in a ferocious manner. Although far more covert and far less violent, the NSA operated in a comparable manner, albeit in a more technologically savvy way. What we have today has less to do with physical violence and more to do with structural violence. What complicates the matter further is one obvious, all too sobering truth: Most of our economic and social interactions rely on digital platforms, the very platforms that monitor our every move. It may seem slightly hyperbolic, but our very existence is now inextricably linked to some form of surveillance. Take a social media platform like Facebook; after all, it only works so efficiently because its users—you and I and billions more—allow Zuckerberg's employees to rummage through our personal data in return for recommendation-based services. As we've all come to recently realize, *we* are Facebook's product, which they sell to advertisers and data miners, which we give them in exchange for its (mostly) free service. In Orwell's tale, television screens monitor you, and neighbors spy on neighbors. Fast forward seven decades and the worldwide web acts as an omniscient supervisor, monitoring

every social media comment, online procurement, and virtual footprint.

Perhaps the furtive nature of the surveillance casts the unethical behavior in a nonthreatening light. However, this behavior is not benign; we should see this form of surveillance for what it is—dangerous and dishonorable. After all, there is clearly a difference between ethical data tracking and unethical surveillance. Millions of people, especially Gen Z and Millennials, share freely. Why? Because this is the culture they have have grown up in; they have never known any other way. Being educated in the importance of *critical distance* never entered the dialogue, and the knowledge of where to draw the line in the proverbial sand is lacking.

Imagine an Orwellianized future where the NSA receives data feed from Google. It's a scary thought, no? Actually, the NSA already has tapped into Google's data feed, and such nefarious activity was going on for years, long before Snowden's revelations. If you happen to be a non-American reader, you may find yourself saying, "Well, thankfully, this activity isn't taking place in my country." But then again, maybe you should ask yourself, "How do I know what's really going on?"

In 2018, *The Intercept*, an online news publication dedicated to "adversarial journalism," published an intriguing story. A military facility about 60 kilometers northwest of Oslo built a surveillance base with assistance from—wait for it—the NSA. Interestingly, collaborative efforts between the NIS (Norwegian Intelligence Service) and the NSA began more than 60 years ago, when Norway and the United States entered into an agreement called NORUSA. Despite costing more than $30 million to construct and largely funded by Norwegian taxpayers, operations at the facility were carried out in a surreptitious, Shakespearean-like manner. Remember that this is Norway, routinely listed as one of the best places in the world to live.

Ostensibly, the facility was built to combat terrorism. However, according to *The Intercept* report, its dragnet also managed to capture records of phone calls and messages (text and email) of everyday communication between law-abiding citizens. To this day, somewhat perplexingly, the surveillance appears to continue unabated. *The Intercept* report provided a rare insight into how Norway's relationship with the NSA evolved throughout the decades, culminating in unprecedented levels of unethical surveillance.

And then there's the UAE, a country with a booming economy and thriving expat community. In the fall of 2018, a British researcher studying the effects of the Arab Spring on security policies was sentenced to life in prison for "espionage." After three months in prison—much of this time spent in solitary confinement—he was released, but only after the British Office intervened. In the UAE, the list of foreign academics and intellectuals expelled from the country is massive. The so-called "Jewel of Arabia" is a master of online surveillance, with authorities closely monitoring the academic work at local branches of prestigious Western universities, like the Sorbonne of Paris and New York University. Not only is censorship regularly applied to academics and scholarly events, some scholars have found themselves imprisoned for human rights activism. Friends of mine working at institutions in the UAE speak of unannounced restrictions on internet and Skype use, as well as calls to "refrain" from discussing Middle Eastern politics, *even if the class happens to be called world politics.*

What motivated these limits on academic freedom? Well, it appears to be the authorities' desire to eliminate any activity considered sinister, which could be anything that appears to threaten national security and authority. Moreover, the chaos unleashed by the protests and demonstrations of the Arab Spring appears to weigh heavily on the collective conscious of UAE officials. They will do anything to stop such revolutionary ideologies crossing their borders; the slightest hint of criticism directed at the Emirati elites, or even a request for greater liberties, can have severe consequences for those brave enough to ask questions. WhatsApp and Facebook facilitate radical discussions, platforms where revolutionary action can be organized in a matter of minutes. That is why in 2012 the UAE passed a rather suspicious looking law in which any speech seen as damaging the state, including messages sent via WhatsApp and other messaging services, could be punished with lengthy prison sentences. UAE officials are all too aware of Thomas Dewar's observation that "Minds are like parachutes—they only function when open," so they do everything in their power to deter intellectual deployment.

Surveillance and power share an intimate link. The word *power* is synonymous with China. According to a recent report by PricewaterhouseCoopers (PWC), a multinational professional services network that monitors such matters, within the next 20 years China will become the most powerful economy in the world. With great power comes great responsibility, an expression widely attributed to two very different sources: Voltaire and Spider-Man. Some

argue that power corrupts, but I would argue that it's not power itself that corrupts; it's the *fear of losing power*. One of the ways to maintain power is to control the masses, by introducing strict laws and severe punishments for transgressors.

This brings us to China's authoritarian tech dystopia. At the time of this writing, the Chinese state was rolling out a vast ranking system designed to monitor the behavior of its enormous population, categorizing each individual by a "social credit" score. First announced in 2014, the "social credit system" aims to fortify the idea that maintaining trust is "glorious," while the breach of trust is dishonorable, an idea befitting a country known for zero tolerance. According to Chinese media reports, by 2020 the "social credit system" is due to be fully operational. However, it is already being piloted in major cities around the country, and as if this needed saying, participation in this sinister scheme is mandatory for all citizens.

Just like private credit scores, an individual's social score can rise and fall; the direction of the movement depends on the behavior of the individual. Examples of transgressions include dangerous driving, posting "fake" news online, smoking in nonsmoking zones, and purchasing too many video games—yes, you read the last point correctly. Chinese authorities have already implemented steps to restrict the number of video games an individual can purchase, as well as curbing playing time for avid gamers. In case anyone has doubts about the seriousness of such a system, China has already prevented more than nine million poorly rated citizens from traveling, blocking them from buying tickets for domestic flights. Furthermore, Chinese authorities have also clamped down on more luxurious options, with close to three million people already barred from purchasing business class train tickets. Offenses include boarding a train without a ticket and loitering in the vicinity of boarding gates. The system appears to be as boundless as it is punitive.

Mencius, a sort of poor man's Confucius, once said that the punishment for a crime should not extend to the perpetrator's wife and children, but try telling this to Chinese authorities. Last year, in the eastern province of Zhejiang, a young man was barred from entering an elite university because his father

had failed to pay off a loan. Although the teenager aced China's grueling college entrance exam and was subsequently accepted to the university, he was refused because his father had engaged in "untrustworthy behavior." This is a frightening vision of the future, one that will almost certainly, over the next couple of decades, cast a more global shadow. Unlike in the United States, where the use of facial recognition technology has been met with widespread condemnation,[1] Chinese officials have fully embraced A.I.-based surveillance software, controlling its 1.4 billion people like pawns on a perverse chessboard.

According to a 2018 *New York Times* report,[2] by 2020 the country will have more than 300 million cameras in operation—one for every five citizens. The Chinese aren't just redefining the idea of authority; they are redefining the very definition of personhood. This is Orwell's answer to *Moneyball*, the crudest of *algorithmic governance*. Although China clearly has a penchant for capitalist ventures, it's very much a semi-authoritarian state. Under the guidance of Xi Jinping, now the "leader for life," China is in a unique position to employ intrusive technology. Not only are restrictions on Internet use prevalent, thus limiting the information available to the masses, few privacy protection laws exist. As highlighted in a 2018 *Vanity Fair* report, numerous tech start-ups have already handed over collected data to government authorities.[3] Such compliance has resulted in an immoral union between surveillance and personalized policing.

When it comes to controlling the masses, Chinese authorities pull no punches. The first week of 2019, government officials passed a law that seeks to "Sinicize" Islam. Basically, Beijing is looking to control the religion in the same way it controls the people, through intimidation and coercion. More than one million Uighur Muslims are estimated to be held in "re-education" camps, otherwise known as internment camps. Here, people are forced to denounce Islam and pledge allegiance to the Communist Party. Mass surveillance technology tracks members of the Uighur Muslim minority, gathering data on interactions between friends and family.[4]

No one appears to be out of sight. Military and government agencies now use birdlike drones to spy on people in provinces across the land. By replicating the movements of real birds, these devices maneuver through the sky, capturing high-resolution images along the way. Furthermore, the drones are fitted with a GPS and a data link antenna for instant communication. Cities like Beijing and Shanghai have used facial recognition systems to control traffic and punish violators of traffic laws for quite some time. In Shenzhen, a city in the southeast, AI is being used to display photos of jaywalkers on large LED screens. This method of public shaming has been in place since April of 2017. A year later, police in Shenzhen started posting personal information of jaywalkers online, including photos, names and even ID numbers.

Perhaps the most worrying of all stories involves workers in Hangzhou, the capital of China's Zhejiang province. To the untrained eye, the workers' uniforms look very ordinary. In a dystopian turn, however, the uniforms were fitted with wireless sensors, while the workers' helmets monitored brainwave activity.

The Chinese government recently launched "Made in China 2025," a state-led industrial policy that seeks to make China the dominant force in global affairs. Domination involves power and control, and China's demonstration of domestic power and control should worry us all.

We all like to believe we are in control. After all, we live in a "free" society, an age where we can think and believe what we want. Sadly, for millions of us, true freedom is nothing but an illusion. Jeremy Bentham, the English philosopher, jurist, and social reformer, spoke extensively about the panopticon, in which the power of an authority's "gaze" ensures compliance. The power of the structure, as seen in China and the UAE, has so much to do with the nebulous design, allowing those in power to monitor the masses without their knowledge or consent. When it came to maintaining order through surveillance, or the perception of surveillance, Bentham saw the panopticon as the ultimate device, "a new mode of obtaining power of mind over mind."

As for *1984*, Orwell's magnum opus has always had a strange way of mirroring events in broader society, at different moments throughout history. But let's stop and ask ourselves one question: If *1984* is a reflection of society, is 2019 a reflection of *1984*? S

REFERENCES

1. Schwartz, J. 2018. Facial Recognition Backlash: Technology Giants Scramble. July 18. https://www.bankinfosecurity.com
2. Mozur, Paul. 2018. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. July 8. https://www.nytimes.com
3. Kosoff, Maya. 2018. China's terrifying surveillance state looks a lot like America's future. July 8. https://www.vanityfair.com
4. Samuel, Sigal. 2018. China Is Going to Outrageous Lengths to Surveil Its Own Citizens. August 16. https://www.theatlantic.com