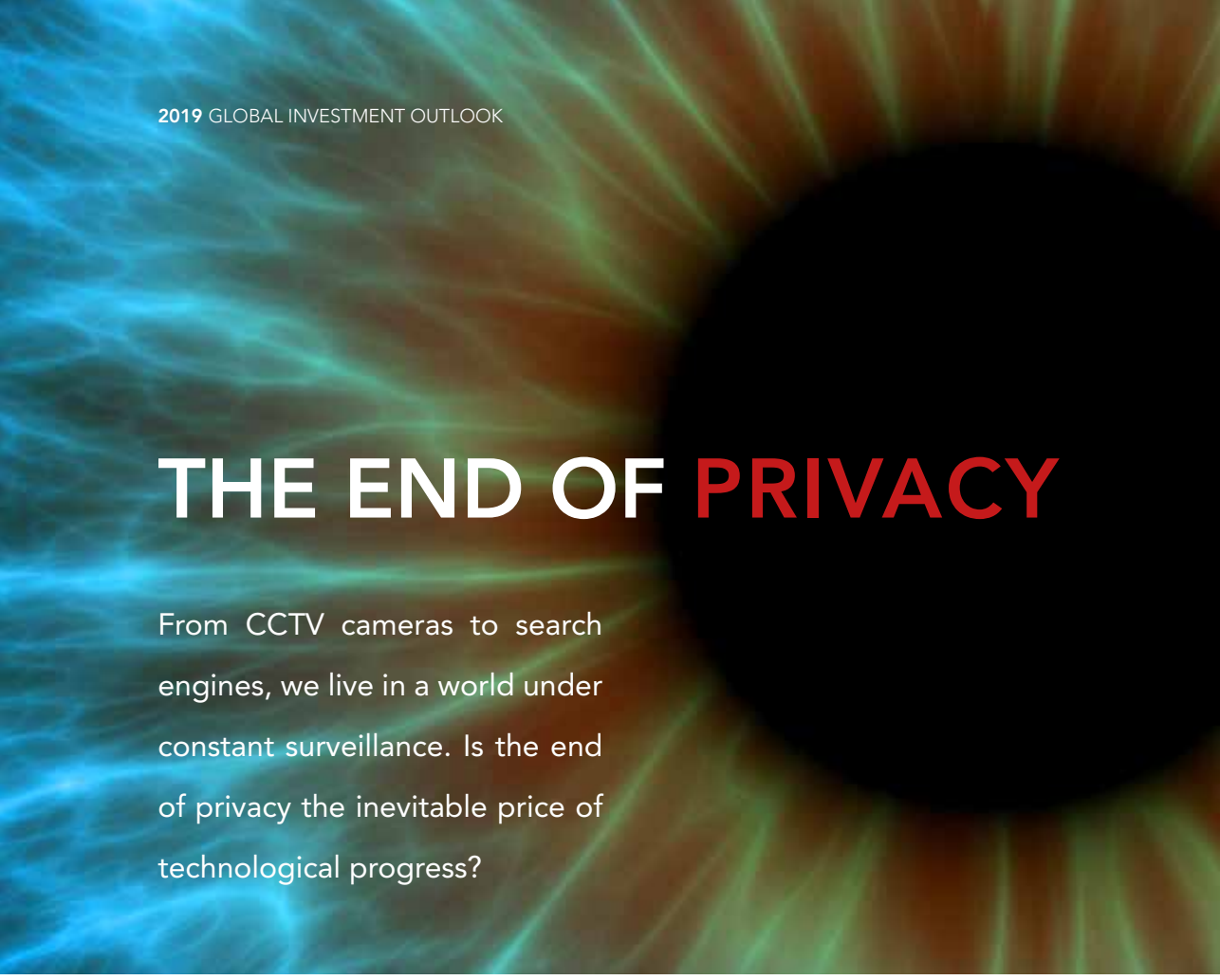


THE END OF PRIVACY

From CCTV cameras to search engines, we live in a world under constant surveillance. Is the end of privacy the inevitable price of technological progress?

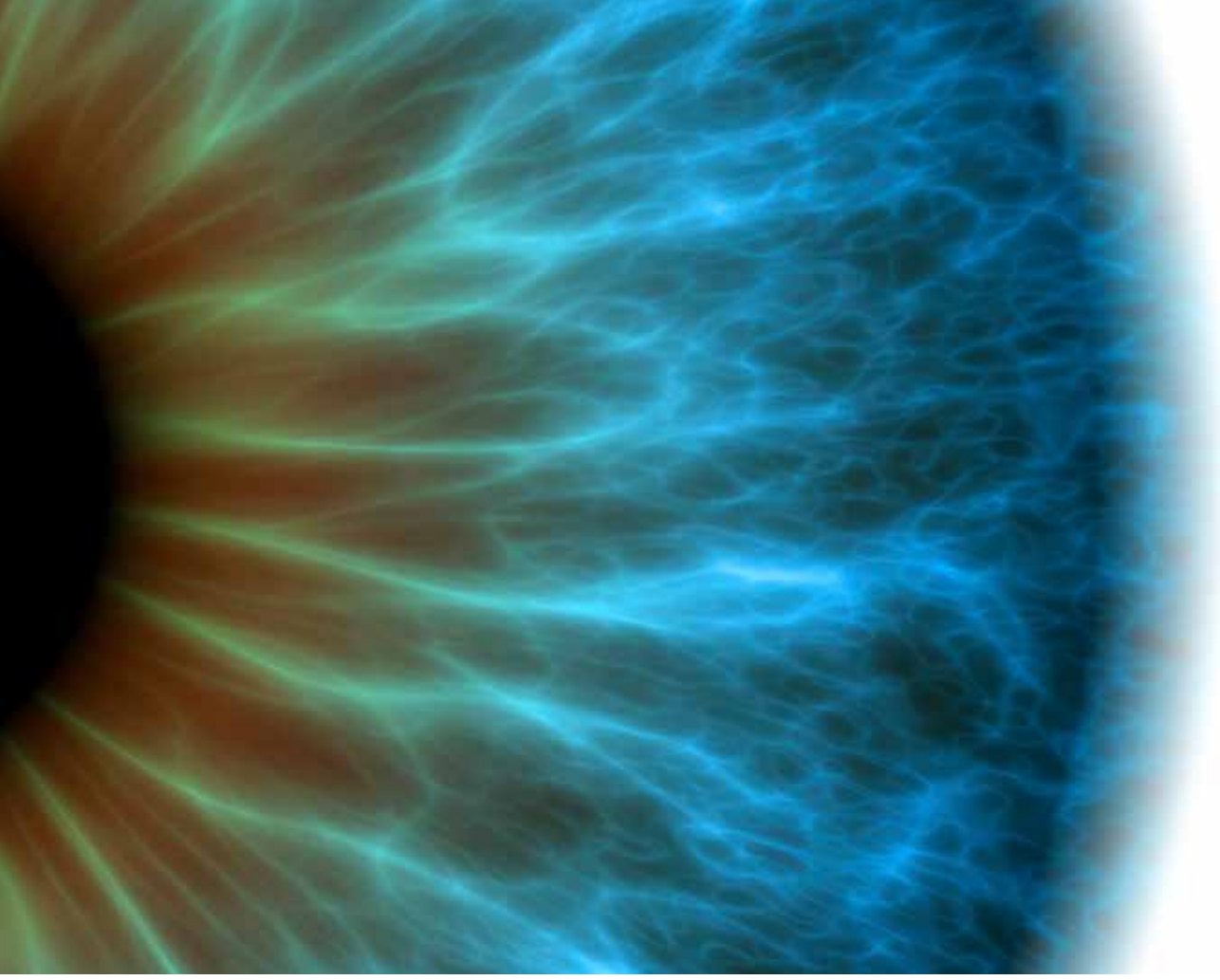
Pity George Orwell. Seven decades ago, when the British writer published his great dystopian novel, the public was stunned by his chilling vision of a future global totalitarian state, where the "Thought Police" kept constant watch on every individual through two-way "Telescreens."

Once hailed as prophetic, *1984* has been outpaced by reality.

Today, we mostly shrug at mass surveillance, winking at the hundreds of millions of CCTV cameras now in operation worldwide, including more than 170 million in China alone. By 2020, according to that country's government, another 400 million will be installed, supporting a national video surveillance network that, says Beijing, will be "omnipresent, fully networked, always working and fully controllable."

Meanwhile, despite some legislation to the contrary, we also seem unbothered by ever-more-granular individual data collection.

We merrily "like" every other Facebook post, pay no heed to eerily well-targeted Google ads and install voice-activated Amazon assistants in our homes. We accept countless cookies every day, never bothering to read the fine print.



We've got nothing to hide, we figure, so why resist the march of technological progress? The end of privacy seems like a small price to pay for a greater sense of personal security – not to mention anywhere, anytime online shopping via apps that remember our shoe size and know we prefer blue to black.

The world's most-populous nation is at the forefront of these trends.

In China, CCTV cameras on every corner are powered by advanced facial recognition software, including some that do not even need to register a face to identify an individual. In Beijing and Shanghai, authorities have recently begun deploying a new surveillance tool that can identify people by how they walk or the shape of their body. Watrix, the company that designed this system, claims to be able to identify people from up to 50 meters away, even when their back is turned or their face covered.

The Chinese are also leaders in voice recognition: iFlyTek, a Chinese artificial intelligence company with ties to state security, claims to be able to monitor a car or a room full of people, identify a targeted individual's voice and record everything that person says.

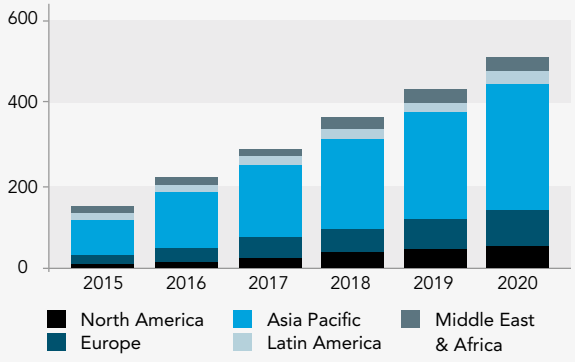
> CHINA HOPES TO BUILD A $150 BILLION ARTIFICIAL INTELLIGENCE INDUSTRY BY 2030, SUPPORTING ITS 'SOCIAL CREDIT SYSTEM'

Why is China so far ahead of the pack? Privacy laws are far less stringent than in the West, giving companies access to reams of personal data. Close ties between the private sector and the government also help, including state support for research and development, alongside extremely robust fundraising.

Today, China has more unicorns – privately held companies valued at over $1 billion – than the US. And while Silicon Valley startups may raise fresh capital once every two years, it is not unusual for hot Chinese startups, including AI firms, to fundraise three to four times per year.

China hopes to build a $150 billion domestic artificial intelligence industry by 2030 as part of an effort to merge surveillance with what the Washington *Post* describes as a "database of information on every citizen, a 'Police Cloud' that aims to scoop up such data as criminal and medical records, travel bookings, online purchase and even social media comments – and link it to everyone's identity card and face."

FACING THE FUTURE
Biometric facial recognition industry revenues, by region (USD MN)



Source: Tractica

It's all part a vast "Social Credit System," expected to be up and running by 2020, whereby every individual will be ranked by a "social score."

Big Data will meet Big Brother, and citizens will be ranked based on whether they have been naughty or nice. Penalties for bad behavior, as judged by the state, may include exclusion from overseas travel, private schools,

domestic hotels and certain employment opportunities – as well as, somewhat ironically, access to high-speed internet. Offenders will also be named and shamed on a public blacklist.

If that sounds unimaginably Orwellian to those of us in the West, think again. Or at least think different.

Landmark legislation such as Europe's General Data Protection Regulation, introduced in May 2018, may govern how companies store and use individual data, but it leaves state surveillance untouched. And even the most well-intentioned legislators will struggle to keep pace with technological progress.

Consider Facebook, which faced its first wave of consumer backlash in 2006 when it introduced its "News Feed," although the service later became a major driver of the company's success. That was just the first in a long line of skirmishes with users and regulators – touching upon issues such as the sale of private information to third parties, massive unreported data theft, foreign election meddling and even mood-manipulation experiments.

While Facebook continues to fight both state and customer-led efforts at greater regulation and data protection, initiatives such as #DeleteFacebook don't seem to be gaining enormous traction. A third of the world is already active on the social network, even if the pace of user growth has now slowed.

▲ By 2020, China plans to have installed a total of nearly 600 million domestic CCTV cameras

Sure, the company has a copy of every message you've ever sent or been sent, every file you've ever sent or been sent, all the contacts in your phone, and all the audio messages you've ever sent or been sent.

But Facebook's data harvesting pales in comparison to Google, which stores your search history across all your devices and creates individual profiles (sold to advertisers) based on your location, gender, age, political leanings, hobbies, career, interests, relationship status and income.

It remains to be seen to what extent web surfers and smartphone users in the West will accept the total loss of privacy. We are seeing the rise of niche search engines like DuckDuckGo, which do not collect any personal information and block hidden web trackers.

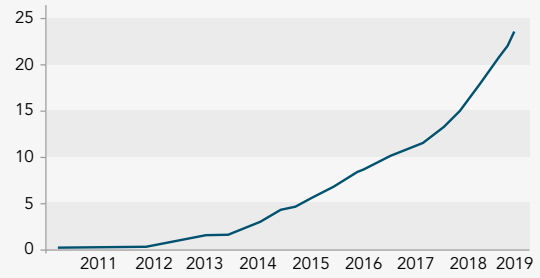
Introduced a decade ago, the privacy-respecting alternative to Google was used for fewer than 5 million searches a day until 2015. Daily DuckDuckGo searches then reached 10 million in 2016 and now stand at nearly 25 million. Compared to Google's 3.5 billion daily searches, that's just a drop in the ocean – but DuckDuckGo's strong growth could nevertheless indicate that the fight for privacy has just begun.

> THE MARKET FOR ALTERNATIVE TECHNOLOGY THAT RESPECTS INDIVIDUAL PRIVACY CLEARLY HAS POTENTIAL

With a $725 billion market capitalization and $110 billion in annual revenues, Google parent Alphabet may represent a far more appealing investment opportunity than tiny firms like DuckDuckGo. Likewise, the global video surveillance industry, valued at about $20 billion in 2015, is expected to grow to $63.2 billion by 2022.

If the end of privacy sounds

ALL THAT IT'S QUACKED UP TO BE?
Daily DuckDuckGo searches (in millions)



Source: DuckDuckGo

▲ Will socially responsible investors decline to invest in firms that erode individual liberty?

like an inevitability, there's one factor that's worth considering: the rise of sustainable, responsible and impact (SRI) investing. As of the end of 2017, one out of every four dollars invested in the United States – or a whopping $12 trillion – was invested according to SRI strategies.

At the same time, some 2,000 firms worldwide have signed the Principles for Responsible Investment, collectively representing an even more staggering $82 trillion in assets owned or under management.

In an age when socially responsible investing is more important than ever, the long-term growth of industries that erode individual liberty could, eventually, be jeopardized. While that's not the case today, especially in markets such as China, societal trends are ultimately unpredictable – and they have a major influence on investor sentiment.

For now, however, there appears to be little reason to believe that the tide will turn. In our homes and workplaces, in our cars and on the streets, data about us is constantly collected and analyzed. We are all tracked and traced, observed and identified, 24/7, in a way that even George Orwell would have found unimaginable.

Does the end of privacy matter? Future generations will decide. ■