VLADIMIR ZIVOJINOVIC FOR *NATURE*

Cameras watch over Belgrade's Republic Square.

RESISTING THE RISE OF FACIAL RECOGNITION

Growing use of surveillance technology has prompted calls for bans and stricter regulation. **By Antoaneta Roussi**

In Belgrade's Republic Square, dome-shaped cameras hang prominently on wall fixtures, silently scanning people walking across the central plaza. It's one of 800 locations in the city that Serbia's government said last year it would monitor using cameras equipped with facial-recognition software, purchased from electronics firm Huawei in Shenzhen, China.

The government didn't ask Belgrade's residents whether they wanted the cameras, says Danilo Krivokapić, who directs a human-rights organization called the SHARE Foundation, based in the city's old town. This year, it launched a campaign called *Hiljade Kamera* – 'thousands of cameras' – questioning the project's legality and effectiveness, and arguing against automated remote surveillance.

Belgrade is experiencing a shift that has already taken place elsewhere. Facial-recognition technology (FRT) has long been in use at airport borders and on smartphones, and as a tool to help police identify criminals. But it is now creeping further into private and public spaces. From Quito to Nairobi, Moscow to Detroit, hundreds of municipalities have installed cameras equipped with FRT, sometimes promising to feed data to central command centres as part of 'safe city' or 'smart city' solutions to crime. The COVID-19

© 2020 Springer Nature Limited. All rights reserved.

pandemic might accelerate their spread.

The trend is most advanced in China, where more than 100 cities bought face-recognition surveillance systems last year, according to Jessica Batke, who has analysed thousands of government procurement notices for *ChinaFile*, a magazine published by the Center on U.S.-China Relations in New York City.

But resistance is growing in many countries. Researchers, as well as civil-liberties advocates and legal scholars, are among those disturbed by facial recognition's rise. They are tracking its use, exposing its harms and campaigning for safeguards or outright bans. Part of the work involves exposing the technology's immaturity: it still has inaccuracies and racial biases (see page 347). Opponents are also concerned that police and law-enforcement agencies are using FRT in discriminatory ways, and that governments could employ it to repress opposition, target protesters or otherwise limit freedoms — as with the surveillance in China's Xinjiang province (see page 354).

Legal challenges have emerged in Europe and parts of the United States, where critics of the technology have filed lawsuits to prevent its use in policing. Many US cities have banned public agencies from using facial recognition — at least temporarily — or passed legislation to demand more transparency on how police use surveillance tools. Europe and the United States are now considering proposals to regulate the technology, so the next few years could define how FRT's use is constrained or entrenched. "What unites the current wave of pushback is the insistence that these technologies are not inevitable," wrote Amba Kak, a legal scholar at New York University's AI Now Institute, in a September report[1] on regulating biometrics.

Surveillance concerns

By 2019, 64 countries used FRT in surveillance, says Steven Feldstein, a policy researcher at the Carnegie Endowment for International Peace in Washington DC, who has analysed the technology's global spread[2]. Feldstein found that cities in 56 countries had adopted smart-city platforms. Many of them purchased their cameras from Chinese firms, often apparently encouraged by subsidized loans from Chinese banks. (US, European, Japanese and Russian firms also sell cameras and software, Feldstein noted.)

Belgrade's project illustrates concerns that many have over the rise of smart-city systems: there is no evidence that they reduce crime more than ordinary video cameras do, and the public knows little about systems that are ostensibly for their benefit. Krivokapić says he is worried that the technology seems more suited to offering an increasingly authoritarian government a tool to curb political dissent.

"Having cameras around in a young democracy such as Serbia can be problematic because of the potential for political misuse," says Ljubiša Bojić, coordinator of the Digital Sociometrics Lab at the University of Belgrade, which studies the effects of artificial intelligence (AI) on society. "Although the situation has changed since the turmoil of the nineties, the dogma of police state and fear of intelligence agencies makes Serbia an inappropriate place for implementation of AI cameras."

"WHAT UNITES THE CURRENT WAVE OF PUSHBACK IS THE INSISTENCE THAT THESE TECHNOLOGIES ARE NOT INEVITABLE."

When the government announced the project, it gave few details. But SHARE found a 2018 press release on Huawei's website (which the firm deleted) that announced tests of high-definition cameras in Belgrade. The document said that the cameras had helped Serbian police to solve several major criminal cases and improve security at major sporting events. This year, the government disclosed that the scheme involves purchasing 8,000 cameras for use in police cars, as body-worn cameras and on buildings.

"There are many questions that remain unanswered," Krivokapić says. "For example, where will the data be stored? In Serbia or in China? Will Huawei have access to the data?" After SHARE and others pressed for more details, the Serbian government said that data wouldn't be collected or kept by Huawei. But Lee Tien, a senior staff attorney at the Electronic Frontier Foundation in San Francisco, California, says that one of the main reasons large technology firms — whether in China or elsewhere — get involved in supplying AI surveillance technology to governments is that they expect to collect a mass of data that could improve their algorithms.

Serbia models its data-protection laws on the European Union's General Data Protection Regulation (GDPR), but it is unclear whether the interior ministry's plans satisfy the country's laws, Serbia's data-protection commissioner said in May. (The interior ministry declined to comment for this article, and Huawei did not respond to questions.)

Overall, there haven't been studies proving that 'safe' or 'smart' cities reduce crime, says Pete Fussey, a sociologist at the University of Essex in Colchester, UK, who researches human rights, surveillance and policing. He says anecdotal claims are being leveraged into a proof of principle for a surveillance technology that is still very new. "The history of technology and law enforcement is littered with examples of hubris and outlandish claims," he says. "It's reasonably uncontroversial to say that surveillance cameras in general are more effective for tackling crimes against things, rather than people. Once you start getting into automated surveillance, it becomes more difficult, partly because it is not used as much."

Pandemic push

In March, Vladimir Bykovsky, a Moscow resident who'd recently returned from South Korea, left his apartment for a few moments to throw out his rubbish. Half an hour later, police were at his door. The officers said he had violated COVID-19 quarantine rules and would receive a fine and court date. Bykovsky asked how they'd known he'd left. The officers told him it was because of a camera outside his apartment block, which they said was connected to a facial-recognition surveillance system working across the whole of Moscow.

"They said they'd received an alert that quarantine had been broken by a Vladimir Bykovsky," he says. "I was just shocked."

The Russian capital rolled out a city-wide video surveillance system in January, using software supplied by Moscow-based technology firm NtechLab. The firm's former head, Alexey Minin, said at the time that it was the world's largest system of live facial recognition. NtechLab co-founder Artem Kukharenko says it supplies its software to other cities, but wouldn't name locations because of non-disclosure agreements. Asked whether it cut down on crime, he pointed to Moscow media reports of hooligans being detained during the 2018 World Cup tournament, when the system was in test mode. Other reports say the system spotted 200 quarantine breakers during the first few weeks of Moscow's COVID-19 lockdown.

Like Russia, governments in China, India and South Korea have used facial recognition to help trace contacts and enforce quarantine; other countries probably have, too. In May, the chief executive of London's Heathrow airport said it would trial thermal scanners with facial-recognition cameras to identify potential virus carriers. Many firms also say they have adapted their technologies to spot people wearing masks (although, as with many facial-recognition performance claims, there is no independent verification).

Researchers worry that the use of live-surveillance technologies is likely to linger after the pandemic. This could have a chilling effect on societal freedoms. Last year, a group set up to provide ethical advice on policing asked more than 1,000 Londoners about the police's use of live facial recognition there; 38% of 16–24-year-olds and 28% of Asian, Black and mixed-ancestry people surveyed said they would stay away from events monitored with

© 2020 Springer Nature Limited. All rights reserved.

live facial recognition. Some people who attend rallies have taken to wearing masks or camouflage-like 'dazzle' make-up to try to confuse facial-recognition systems. But their only 'opt-out' option is to not turn up.

We're all in the database

Another concern, especially in the United States, is that the watch lists that police use to check images against can be enormous – and can include people without their knowledge. Researchers at the Center on Privacy and Technology at Georgetown University in Washington DC estimated in 2016 that around half of all Americans were in law-enforcement face-recognition networks, because many states allow police to search driver's-licence databases.

And earlier this year, *The New York Times* revealed that software company Clearview AI in New York City had scraped billions of images from social-media sites and compiled them into a facial-recognition database. The firm offered its service to police in and outside the United States.

"The Clearview scandal threw into relief what researchers had long thought was possible," says Ben Sobel, who studies the ethics and governance of AI at the Berkman Klein Center at Harvard University in Cambridge, Massachusetts. "Technology capable of recognizing faces at scale is becoming more accessible and requiring less sophistication to run."

Social-media sites such as Twitter, Facebook and YouTube have told Clearview to stop scraping their sites, saying it breaches their terms of service. And several lawsuits have been filed against the firm, including under an Illinois law that allows individuals in that state to sue firms who capture their biometric information – including from the face – without their consent. In June, the European Data Protection Board issued an opinion that Clearview's service breaches the GDPR – but no action has yet been taken. Clearview, which stopped selling some of its services this year after media coverage, told *Nature* that its "image-search engine functions within the bounds of applicable laws".

> "TECHNOLOGY CAPABLE OF RECOGNIZING FACES AT SCALE IS BECOMING MORE ACCESSIBLE."

Clearview isn't the only firm to harvest online images of faces. A company called PimEyes in Wrocław, Poland, has a website that allows anyone to find matching photos online, and the firm claims to have scraped 900 million images – although, it says, not from social-media sites. And NtechLab launched the FindFace app in 2016 to permit face-matching on the Russian social network VK. The company later withdrew the app.

It now seems impossible to stop anyone from privately building up large facial-recognition databases from online photos. But in July, researchers at the University of Chicago in Illinois unveiled a piece of software called Fawkes that adds imperceptible tweaks to images so that they look the same to the human eye, but like a different person to a machine-learning model. If people 'cloak' enough of their facial images through Fawkes, they say, efforts such as Clearview's will learn the wrong features and fail to match new, unaltered images to its models. The researchers hope that photo-sharing or social-media platforms might offer the service to protect users, by applying the software before photos are displayed online.

Calls for regulation

In September 2019, the London-based Ada Lovelace Institute, a charity-funded research institute that scrutinizes AI and society, published a nationally representative survey[3] of more than 4,000 British adults' views on FRT. It found that the majority of people supported facial recognition when they could see a public benefit, such as in criminal investigations, to unlock smartphones or to check passports in airports. But 29% were uncomfortable with the police using the technology, saying that it infringes on privacy and normalizes surveillance, and that they don't trust the police to use it ethically. There was almost no support for its use in schools, at work or in supermarkets. "The public expects facial-recognition technology in policing to be accompanied by safeguards and linked to a public benefit," the survey concluded.

Many researchers, and some companies, including Google, Amazon, IBM and Microsoft, have called for bans on facial recognition – at least on police use of the technology – until stricter regulations are brought in. Some point admiringly to the GDPR, which prohibits processing of biometric data without consent – although it also offers many exceptions, such as if data are "manifestly public", or if the use is "necessary for reasons of substantial public interest".

When it comes to commercial use of facial recognition, some researchers worry that laws focused only on gaining consent to use it aren't strict enough, says Woodrow Hartzog, a computer scientist and law professor at Northeastern University in Boston, Massachusetts, who studies facial surveillance. It's very hard for an individual to understand the risks of consenting to facial surveillance, he says. And they often don't have a meaningful way to say 'no'.

Hartzog, who views the technology as the "most dangerous ever to be invented", says if US lawmakers allow firms to use facial recognition "despite its inevitable abuses", they should write rules that prohibit the collection and storage of 'faceprints' from places such as gyms and restaurants, and prohibit the use of FRT in combination with automated decision-making such as predictive policing, advert-targeting and employment.

The Algorithmic Justice League, a researcher-led campaigning organization founded by

Activist Darya Kozlova in Moscow has her face painted with features said to confuse cameras.

YURI KADOBNOV/AFP/GETTY

© 2020 Springer Nature Limited. All rights reserved.

THOMAS PETER/REUTERS

A software engineer at Hanwang Technology in Beijing tests a facial-recognition programme that identifies people wearing face masks.

computer scientist Joy Buolamwini at the Massachusetts Institute of Technology in Cambridge, has been prominent in calling for a US federal moratorium on facial recognition. In 2018, Buolamwini co-authored a paper showing how facial-analysis systems are more likely to misidentify gender in darker-skinned and female faces[4]. And in May, she and other researchers argued in a report that the United States should create a federal office to manage FRT applications — rather like the US Food and Drug Administration approves drugs or medical devices[5].

"What a federal office would do is provide multiple levels of clearance before a product can enter the market. If the risks far outweigh the benefits, maybe you don't use that product," says Erik Learned-Miller, a computer scientist at the University of Massachusetts in Amherst who co-authored the report.

In China, too, people have expressed discomfort with widespread use of facial recognition — by private firms, at least. An online survey of more than 6,000 people in December 2019 by the Nandu Personal Information Protection Research Centre, a think tank affiliated with the *Southern Metropolis Daily* newspaper in Guangzhou, found that 80% of people worried about lax security in facial-recognition systems and 83% wanted more control over their face data, including the option to delete it. Chinese newspapers have run articles questioning FRT use, and the government is bringing in tighter data-protection laws. But the debate doesn't usually question the use of cameras by the police and government, and the data-protection laws don't put limits on government surveillance, says Graham Webster, who studies China's digital policies at Stanford University in California.

Europe's data-protection rules say that police can process data for biometric purposes if it's necessary and subject to appropriate safeguards. A key question here, says Fussey, is whether it would be proportionate to, for example, put tens of thousands of people under video surveillance to catch a criminal.

So far, British judges have suggested they think it might be, but only if the use of the technology by police has tighter controls. Last year, a man named Ed Bridges sued police in South Wales, alleging that his rights to privacy had been breached because he was scanned by live facial-recognition cameras on two occasions in Cardiff, UK, when police were searching crowds to find people on a watch list. In August, a UK court ruled that the actions were unlawful: police didn't have enough guidance and rules about when they could use the system and who would be in their database, and they hadn't sufficiently checked the software's racial or gender bias. But judges didn't agree that the camera breached Bridges' privacy rights: it was a 'proportionate' interference, they said.

The EU is considering an AI framework that could set rules for biometrics. This year, a white paper — a prelude to proposed legislation — suggested that special rules might be needed for 'high-risk' AI, which would include facial recognition. Most people and firms who wrote into a consultation that followed the document felt that further regulations were needed to use FRT in public spaces.

Ultimately, the people affected by FRT need to discuss what they find acceptable, says Aidan Peppin, a social scientist at the Ada Lovelace Institute. This year, he has been helping to run a citizens' biometrics council, featuring in-depth workshops with around 60 people across the country. Participants provide their views on biometrics, which will inform a UK review of legislation in the area. "The public voice needs to be front and centre in this debate," he says.

Antoaneta Roussi is a freelance journalist in Nairobi. Additional reporting by **Richard Van Noorden**.

1. Kak, A. (ed.) *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute, 2020).
2. Feldstein, S. *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace, 2019).
3. Ada Lovelace Institute. *Beyond Face Value: Public Attitudes to Facial Recognition Technology* (Ada Lovelace Institute, 2019).
4. Buolamwini, J. & Gebru, T. *Proc. Mach. Learn. Res.* **81**, 77–91 (2018).
5. Learned-Miller, E., Ordóñez, V., Morgenstern, J. & Buolamwini, J. *Facial Recognition Technologies in the Wild: A Call for a Federal Office* (Algorithmic Justice League, 2020).

© 2020 Springer Nature Limited. All rights reserved.