JOHANNES EISELE/AFP/GETTY

Police patrol a food market at night in Kashgar in China's Xinjiang province.

Crack down on genomic surveillance

Yves Moreau

Corporations selling DNA-profiling technology are aiding human-rights abuses. Governments, legislators, researchers, reviewers and publishers must act.

Across the world, DNA databases that could be used for state-level surveillance are steadily growing.

The most striking case is in China. Here police are using a national DNA database along with other kinds of surveillance data, such as from video cameras and facial scanners, to monitor the minority Muslim Uyghur population in the western province of Xinjiang.

Concerns about the potential downsides of governments being able to interrogate people's DNA have been voiced since the early 2000s (ref. 1) by activist groups, such as the non-profit organization GeneWatch UK, and some geneticists (myself included). Partly thanks to such debate, legislation and best practices have emerged in many countries around the use of DNA profiling in law enforcement[2]. (In profiling, several regions across the genome, each consisting of tens of nucleotides, are sequenced to identify a person or their relatives.)

Now the stakes are higher for two reasons. First, as technology gets cheaper, many countries might want to build massive DNA databases. Second, DNA-profiling technology can be used in conjunction with other tools for biometric identification – and alongside the analysis of many other types of personal data, including an individual's posting behaviour on social networks. Last year, the Chinese firm Forensic Genomics International (FGI) announced that it was storing the DNA profiles of more than 100,000 people from across China (FGI, known as Shenzhen Huada Forensic Technology in China, is a subsidiary of the BGI, the world's largest genome-research organization). It made the information available to the individuals through WeChat, China's equivalent of WhatsApp, using an app accessed by facial recognition.

With stringent safeguards and oversight, it is legitimate for law-enforcement agencies to

use DNA-profiling technology. But these uses can easily creep towards human-rights abuses. In October this year, the US Department of Homeland Security announced that it would authorize the mandatory collection of DNA samples from immigrants in federal custody at the US border, including children and those applying for asylum at legal ports of entry. The resulting DNA profiles will be available through a database called CODIS (Combined DNA Index System), which includes the profiles of convicted offenders and individuals arrested for serious offences. Such treatment could reinforce debunked claims that immigrants are more prone to criminal behaviour than the general population.

A much broader array of stakeholders must engage with the problems that DNA databases present. In particular, governments, policymakers and legislators should tighten regulation and reduce the likelihood of corporations aiding potential human-rights abuses by selling DNA-profiling technology to bad actors — knowingly or negligently. Researchers working on biometric identification technologies should consider more deeply how their inventions could be used. And editors, reviewers and publishers must do more to ensure that published research on biometric identification has been done in an ethical way.

Government monitoring

In Xinjiang in China, police collected biometric information (including blood samples, fingerprints and eye scans) from nearly 19 million people in 2017, in a programme called 'Physicals for All'. This was part of a suite of measures that are being used by the Chinese government to control the Uyghur ethnic group[3].

Other nations are building massive DNA databases or considering doing so. In 2015, Kuwait passed a law mandating DNA profiling of its entire population. Foreigners living in Kuwait and even visitors were to be included. In January this year, Kenya passed a law that would have enabled the government to require all citizens to submit any biometric information, including DNA profiles, to a national database.

Both cases have hit obstacles. Kuwait's Constitutional Court overruled the 2015 law two years later, because of concerns about how the database could be used in violations of privacy and due process. And, thanks to a decision taken by Kenya's High Court in April, DNA is now excluded from national efforts to collect biometric data.

But these and other examples indicate that governments keep being tempted to hoover up their citizens' DNA data[4].

Corporate responsibility

One way to reduce the likelihood of massive DNA databases being misused is to change the behaviour of the companies that invest in DNA-profiling technologies (see 'Ethical divesting').

US and European corporations are still the dominant providers of such technologies. The deployment of DNA-surveillance infrastructure in Xinjiang, for example, was enabled by the Chinese government buying products from — and working with — the US company Thermo Fisher Scientific in Waltham, Massachusetts. The firm is currently the global leading supplier of DNA-profiling technology in law enforcement. Thermo Fisher Scientific researchers have worked with China's Ministry of Justice, and with researchers at the People's Public Security University of China, which falls directly under the Ministry of Public Security, to tailor the technology specifically for use in Tibetan and Uyghur populations[5]. (Thermo Fisher Scientific did not respond to a request for comment). However, in February, after two years of public outcry and intense pressure from high-profile US senators, the company announced that it would stop selling its DNA-profiling technology in Xinjiang.

"Governments keep being tempted to hoover up their citizens' DNA."

Marketing and lobbying by technology suppliers is often behind pushes for the broadest possible use of DNA profiling. In 2016, for instance, a representative of a US lobbying firm working for Thermo Fisher Scientific described in a conference presentation the development of universal DNA databases as "inevitable". He noted that the expansion of these to "Western countries or other countries with democratic forms of government" faced "significant hurdles", such as the "open and public parliamentary process" and the "culture of being influenced by opposition and protests" (see go.nature.com/337pjce).

Restrictions on the use of technologies or services provided by corporations are currently too weak. Take export controls: either they do not pay due attention to these sensitive technologies, or they have loopholes that often render them useless. For example, US laws forbid the export of fingerprint-recognition technology to some destinations or users deemed problematic by the US government, such as the Chinese police. But the United States does not restrict the export of more-invasive DNA-profiling and facial-recognition technologies. Meanwhile, the European Union does not regulate the export of fingerprint technology, even though the dominant global suppliers are European.

Export controls for biometric technologies could be improved relatively easily. The US Department of Commerce is currently considering revising regulations for emerging technologies[6], such as Internet censorship and video surveillance, to try to reduce the likelihood of companies doing business with problematic buyers. Last month, it barred Xinjiang police forces and eight Chinese technology companies from buying US products or importing US technology because of their role in the repression of Uyghurs.

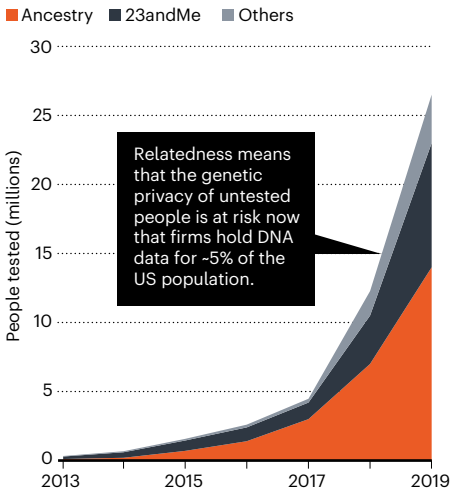
Some regulatory initiatives are promising and could provide a deterrent if enforced. The 2017 EU directive on non-financial reporting (named 2014/95) has mandated that large companies listed on stock markets document their social and environmental impacts in their annual reports for shareholders and the public. Since 2017, France's corporate 'duty of vigilance' law has required all French companies employing more than 5,000 people in the country to actively monitor their impacts on human rights, the environment and so on (see go.nature.com/2o8tcvn).

In the United States, several human-rights lawyers have attempted to revive the Alien Tort Statute (28 U.S.C. § 1350) over the past 20 years. Produced in 1789 but never deployed, this law could enable a foreign individual to make a civil liability claim against a domestic corporation in US courts. A carefully crafted Alien Tort Statute could provide a way to hold companies to the same standards, whether they are operating at home or abroad.

Ultimately, international laws must be established that clearly stipulate the human-rights responsibilities of corporations. For the past decade, a United Nations working group has been drafting a treaty to regulate the activities of transnational corporations with regards to human rights and the environment (see go.nature.com/35qnehe). If it is not crippled by lobbying, this could eventually become a powerful tool to promote

DNA TESTING FOR ALL

An increasing number of people are having their DNA analysed by consumer-genomics companies.



SOURCE: *MIT TECH. REV.* 2019 (HTTPS://GO.NATURE.COM/2MHTJED)

ethical business practices. Yet companies are only part of the story when it comes to the potential misuse of DNA databases.

Research ethics

The chain of technology development leads from fundamental to applied research to the products that enable the abuses. More academics working on biometric identification technology should reflect on the potential misuses of their inventions and engage with society. For instance they can contribute to mainstream media, participate in public debates or join ethics boards.

Recent events indicate that publishers and scholars might be paying insufficient attention to the sources of biometric-identification research. For example, in August last year, after several Human Rights Watch and media reports about the surveillance abuses in Xinjiang, Springer Nature published the proceedings of a biometrics conference held in the province. (Springer Nature has been the publisher of the proceedings of the Chinese Conference on Biometric Recognition for nine years; *Nature* is editorially independent of its publisher.) One of the conference papers, on technologies for recognizing various languages in images, described how "Uyghur information" (referring to the Uyghur language script) could be detected in images that might be used to evade Internet censorship[7]. Another paper described how products from Thermo Fisher Scientific and the Chinese firms Hisign, Megvii and iFlytek are being used to build a population-scale database for DNA, fingerprint, face and voice information in a major Chinese city[8].

In July this year, researchers from Imperial College London announced the results of an open competition on facial recognition. (The winners presented their work at a conference in Seoul in October.) Before a reporter from the non-profit news platform Coda pointed it out, one of the sponsors of the conference had been a Chinese artificial-intelligence start-up called DeepGlint, which in 2018 set up a joint research laboratory with the Xinjiang police. The conference organizers removed DeepGlint as a sponsor in August.

Over the past eight years, three leading forensic genetics journals — *International Journal of Legal Medicine* (published by Springer Nature), and *Forensic Science International* and *Forensic Science International: Genetics Supplement Series* (both published by Elsevier) — have published 40 articles co-authored by members of the Chinese police that describe the DNA profiling of Tibetans and Muslim minorities, including people from Xinjiang. I analysed 529 articles on forensic population genetics in Chinese populations, published between 2011 and 2018 in these journals and others. By my count, Uyghurs and Tibetans are 30–40 times more frequently studied than are people from Han communities, relative to the size of their populations (unpublished data). Half of the studies in my analysis had authors from the police force, military or judiciary. The involvement of such interests should raise red flags to reviewers and editors.

In short, the scientific community in general — and publishers in particular — need to unequivocally affirm that the Declaration of Helsinki (a set of ethical principles regarding human experimentation, developed for the medical community) applies to all biometric identification research (see go.nature.com/34bypbf). Unethical work that has been published in this terrain must be retracted.

Privacy concerns

DNA databases in local police forces are proliferating, even in countries that have democratic governments and well-established legal protections for citizens' privacy[9]. By August this year, for instance, the Office of the Chief Medical Examiner of New York City held more than 82,000 genetic profiles. At the same time, there has been a growth in consumer and recreational genomic services, such as the US corporations 23andMe in Mountain View, California, and Ancestry in Lehi, Utah (see 'DNA testing for all'). Medical DNA sequencing is also becoming routine[10].

Currently, only some consumer-genomics companies have willingly shared people's DNA data with law-enforcement agencies. And in many countries, patients' data are confidential.

But to deploy DNA surveillance across a group of people, you need profiles from only 2–5% of that population, because biological relationships can be inferred[11,12]. And as genealogy and medical databases mushroom, law enforcers and others are increasingly tempted to tap into them[13]. In 2017 in the Netherlands, the Ministry of Health drafted a bill that would have allowed police to obtain people's DNA information from hospitals in some limited cases. It was abandoned following public outcry.

And June saw what might be a game changer in the United States. The Orlando Police Department obtained a warrant that allowed it to search the entire DNA database of the GEDMatch genealogy website, based in Lake Worth, Florida. Because consumer-genomics companies already hold DNA data for an estimated 5% of the US population, unfettered access to these data by law-enforcement agencies would simply spell the end of genetic privacy in the United States.

All of us must beware a world in which our behavioural, financial and biometric data, including our DNA profiles, or even entire genome sequences, are available to corporations — and so potentially to law enforcers and political parties. Without the changes outlined here, the use of DNA for state-level surveillance could become the norm in many countries.

ETHICAL DIVESTING

Investors could help to ensure ethical use of the products of DNA profiling firms.

Public outcry can lead to divestment. Since March this year, for example, major US funds such as Goldman Sachs have divested all their shares from the Chinese surveillance company Hikvision, because of concerns about the use of the company's products in human-rights breaches.

Investors could even be motivated to scrutinize company ethics, thanks to studies over the past five years or so indicating that 'good' corporate social responsibility practices tend to correlate with better financial performance over the long term.

Pressure from investors — and the public in general — might be increasingly powerful. Take Thermo Fisher Scientific's February announcement that it would stop selling its DNA profiling technology in Xinjiang, China. Although Chinese authorities can easily transport such technology from elsewhere in the country, it is significant that a major corporation publicly acknowledged "the importance of considering how [its] products and services are used — or may be used — by [its] customers". **Y.M.**

The author

Yves Moreau is a computational biologist specializing in human genetics and professor of engineering at the Catholic University of Leuven (KU Leuven), Leuven, Belgium.
e-mail: yves.moreau@kuleuven.be

1. Wallace, H. M., Jackson, A. R., Gruber, J. & Thibedeau, A. D. *Egypt. J. Forensic Sci.* **4**, 57–63 (2014).
2. Forensic Genetics Policy Initiative. *Establishing Best Practice for Forensic DNA Databases* (Forensic Genetics Policy Initiative, 2017); available at http://dnapolicyinitiative.org/report
3. Ramzy, A. & Buckley, C. *The New York Times* (16 November 2019).
4. Nelkin, D. & Andrews, L. *Sociol. Health Illn.* **21**, 689–706 (1999).
5. Wang, Z. *et al. Sci. Rep.* **6**, 31075 (2016).
6. Bureau of Industry and Security. *Fed. Regist.* **83**, 58201–58202 (2018).
7. Aizezi, Y., Jiamali, A., Abdurixiti, R. & Ubul, K. in *Biometric Recognition. CCBR 2018* (eds Zhou, J. *et al.*). *Lecture Notes in Computer Science* **10996**, 709–718 (Springer, 2018).
8. Zhu, W. J., Zhuang, C. Z., Liu, J. W. & Huang, M. in *Biometric Recognition. CCBR 2018* (eds Zhou, J. *et al.*). *Lecture Notes in Computer Science* **10996**, 198–205 (Springer, 2018).
9. Mercer, S. & Gabel, J. D. *N.Y.U. Ann. Surv. Am. L.* **69**, 639–698 (2014).
10. Ratner, M. *Nature Biotechnol.* **36**, 484 (2018).
11. Erlich, Y., Shor, T., Pe'er, I. & Carmi, S. *Science* **362**, 690–694 (2018).
12. Guest, C. *Am. U. L. Rev.* **68**, 1015–1052 (2019).
13. O'Doherty, K. C. *et al. BMC Med. Ethics* **17**, 54 (2016).