GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Association for Progressive Communications (APC),
Article 19, and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch

2019

Global Information Society Watch 2019
Artificial intelligence: Human rights, social justice and development

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

GISWatch 2019 advisory committee
Namita Aavriti (APC)
Rasha Abdul Rahim (Amnesty International)
Alex Comninos (Research ICT Africa)
Malavika Jayaram (Digital Asia Hub)
J. Carlos Lara (Derechos Digitales - América Latina)
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)
Andrew Lowenthal (EngageMedia)
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)
Valeria Milanes (Asociación por los Derechos Civiles)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch.
We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)
Anita Gurumurthy and Nandini Chami (IT for Change)
Rasha Abdul Rahim (Amnesty International)

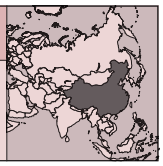
APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19
for their support for Global Information Society Watch 2019.

Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

CHINA

ALGORITHMIC OPPRESSION WITH CHINESE CHARACTERISTICS: AI AGAINST XINJIANG'S UYGHURS



Chinese University of Hong Kong Faculty of Law/ Strathclyde University Law School
Angela Daly
www.law.cuhk.edu.hk/en

Introduction

The ways in which artificial intelligence (AI), in particular facial recognition technology, is being used by the Chinese state against the Uyghur ethnic minority demonstrate how big data gathering, analysis and AI have become ubiquitous surveillance mechanisms in China. These actual uses of facial recognition will be compared with the rhetoric on AI ethics which is beginning to emerge from public and private actors in China. Implications include the mismatch between rhetoric and practice with regards to AI in China; a more global understanding of algorithmic discrimination, which in China explicitly targets and categorises Uyghur people and other ethnic minorities; and a greater awareness of AI technologies developed and used in China which may then be exported to other states, including supposed liberal democracies, and used in similar ways.

Context

Digitisation in China and China's digital industries are now of global importance, given the huge market of over a billion people, high levels of connectivity and use of digital services such as mobile payments (which outstrips take-up in Western markets), and development of a home-grown internet service industry centred on Baidu, Alibaba and Tencent to rival Silicon Valley's Google, Amazon, Facebook and Apple. Digitisation in China has performed important roles in socioeconomic development, with private sector actors' activities aligned with the Chinese Communist Party (CCP) government's goals, and in compliance with government censorship rules.[1]

The next phases of digitisation are rapidly being implemented in China, notably the full roll-out of the Social Credit system by 2020. The system includes a number of data-gathering and analysis techniques including facial recognition applications in public places and algorithmic decision making. AI is viewed as a highly strategic area of development by the Chinese government, and China rivals only the United States (US) in its AI technology research and development, and also implementation.[2]

However, digitisation and the implementation of AI so far in China have exhibited serious concerns for human rights. Similarly to the ways in which AI and algorithms in the US reinforce existing racial and gender inequalities,[3] and how surveillance and other forms of data gathering are specifically targeted at racial and religious minorities across the West,[4] intensified practices of data gathering, analysis and AI implementations are being directed at the majority-Muslim Uyghur people and other minorities in the Xinjiang Uyghur Autonomous Region in northwest China (also known as East Turkestan), "amplify[ing] systems of inequality and oppression."[5]

The Uyghurs, a Turkic-language speaking group who predominantly reside in Xinjiang, have been subject to repression from the Chinese state, including the internment of up to a million people in detention camps.[6] While the Uyghurs socially, religiously and culturally have strong affinities with their Central Asian neighbours, politically and economically they have been connected to China since the Qing Dynasty annexation of their territory in 1755, aside from two brief periods of independence in the 20th century, culminating in the incorporation of Xinjiang into the People's Republic of China in 1949.[7] The territory is geographically located close to other politically vola-

1 Arora, P. (2019). Benign dataveillance? Examining novel data-driven governance systems in India and China. *First Monday*, *24*(4).

2 Lee, K. F. (2018). *AI Superpowers: China, Silicon Valley and the New World Order*. Boston: Houghton Mifflin Harcourt.

3 Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press.

4 See, for example, Mann, M., & Daly, A. (2019). (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television and New Media*, *20*(4), 379-395. https://eprints.qut.edu.au/123774/1/North-In-South.pdf

5 Arora, P. (2019). Op. cit.

6 Zenz, A. (2018). New Evidence for China's Political Re-Education Campaign in Xinjiang. *China Brief, 18*(10). https://jamestown.org/program/evidence-for-chinas-political-re-education-campaign-in-xinjiang; Mozur, P. (2019, 14 April). One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. *The New York Times*. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

7 Aktas, I. (2015). Uighur Separatism and Human Rights: A Contextual Analysis. In M. Kosmala-Mozlowska (Ed.), *Democracy and Human Rights in East Asia and Beyond – Critical Essays*. Warsaw: Collegium Civitas Press.

tile regions such as Tibet, Afghanistan and Kashmir, thereby exposing it to the influence of "wider Asian power politics", and is also endowed with natural resources.[8] Xinjiang is also a key connection point for China's Belt and Road Initiative (BRI), a trade policy aimed at strengthening "Beijing's economic leadership through a vast programme of infrastructure building throughout China's neighbouring regions."[9] A Uyghur separatist or pro-independence movement exists, and for some time has been under Chinese state surveillance. The security situation has been heightened by sectarian riots in Urumqi (the capital of Xinjiang) in 2009 between Han Chinese and Uyghurs, and a series of attacks (mainly involving knives and vehicles) on Han Chinese perpetrated by Uyghurs since 2000.[10]

AI and surveillance in China

Government surveillance activities in China have existed at least since the birth of the current state in 1949. However, since 2013, when Xi Jinping came to power in China, censorship, surveillance and monitoring of electronic communications, as well as the gathering of big data and analysis of citizens' communications and activities, have intensified as a means of shoring up the CCP party-state against challenges, [11] "rapidly" turning China into "an information or surveillance state".[12]

Surveillance cameras, especially used by the government, are now prevalent in China, and increasingly incorporate facial recognition and "intelligence analysis" (flagging objects or "events of interest").[13] China's very large population and the facial data generated from it via these cameras, coupled with government support for industry endeavours in this area, have fuelled research into machine learning and the implementation of algorithm-powered facial recognition technology.[14] In 2017 it was reported that the Chinese government's "Skynet" video surveillance initiative (accompanied by the more recent "Sharp Eyes" programme) had been completed. This is the largest initiative in the world to monitor public spaces and details such as the "gender, clothing, and height" of people coming into the surveillance cameras' vision.[15]

8 Ibid.

9 Cai, P. (2017). *Understanding China's Belt and Road Initiative.* Lowy Institute for International Policy. https://hdl.handle.net/11540/6810

10 Aktas, I. (2015). Op cit.

11 Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy, (30)*1, 53-67.

12 Leibold, J. (2019). Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement. *Journal of Contemporary China* (forthcoming).

13 Qiang, X. (2019). Op. cit.

14 Ibid.

15 Ibid.

Surveillance in Xinjiang

While these technologies and other surveillance programmes have been rolled out throughout the country, the Uyghur minority in Xinjiang has been specifically targeted:

> China's western Xinjiang region, home to the Uyghurs, has effectively become "a 'frontline laboratory' for data-driven surveillance." Cameras are ubiquitous in Xinjiang, and their view extends well outside urban centers. The methods employed in this province may well foreshadow the nationwide implementation of similar "predictive-policing tactics" in the months to come. Xinjiang is also the place in which DNA-collection efforts have taken their most extreme form.[16]

This use of surveillance technology, in particular AI-enabled facial recognition, takes place amidst increasing repression of Uyghurs and other minority groups in Xinjiang. Since 2017, a major "re-education campaign" has been taking place in the territory, involving the large-scale "extrajudicial" internment of at least tens of thousands of people in re-education camps, with the ostensible aim of "de-extremification" and ideological "assimilation" of the Uyghur and other minorities to a *de facto* Han Chinese/atheist CCP norm.[17] The CCP has "constructed a sophisticated multi-layered network of mass surveillance in Xinjiang" which "includes both covert and overt monitoring as well as the categorization, exhortation and disciplining of its population in the name of safety, civility and progress."[18]

Leibold notes that the surveillance assemblage in Xinjiang includes both "machine and human-driven systems that do not always fit together nor form a coherent whole."[19] Despite the government's wish for a seamless and ubiquitous form of monitoring and control, there are still practical obstacles including "poor technological integration and human coordination", and

16 Ibid.

17 Zenz, A. (2019). 'Thoroughly reforming them towards a healthy heart attitude': China's political re-education campaign in Xinjiang. *Central Asian Survey*, *(38)*1, 102-128.

18 Leibold, J. (2019). Op. cit. See also Human Rights Watch's work reverse engineering an app used by police in Xinjiang to collect information about individuals and communicate that information with the authorities' Integrated Joint Operations Platform which aggregates this data and "flags" individuals who are deemed to be potentially threatening. Human Rights Watch. (2019, 1 May). China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

19 Leibold, J. (2019). Op. cit.

the cost and technical difficulty in updating and maintaining surveillance equipment in Xinjiang given its "harsh arid climate, where surveillance systems remain susceptible to decay, sabotage and obsolescence."[20] Furthermore, the facial recognition technologies developed in China also exhibit errors and inaccuracies like facial recognition systems developed elsewhere, including in identifying individuals and in particular in categorising them by ethnic group.

Chinese AI and corporate involvement

That being said, Xinjiang retains a "laboratory" status for the trial of Chinese-made surveillance technologies including those that use AI methods, in particular facial recognition technology. The Urumqi train station was the first to use fully automated gates incorporating facial recognition technology in 2016, and various companies such as Taisau (based in Shenzhen) provide cutting-edge technology for smart-gates implemented throughout the region in public spaces.[21] Facial recognition is also used in smart cameras throughout Xinjiang, including in mosques, provided by companies such as Hikvision (based in Hangzhou).[22] Hikvision has received contracts to provide surveillance equipment, including with facial recognition capacity, in Xinjiang, totalling over USD 290 million.[23] It was reported that Hikvision previously offered options to identify minorities but this was phased out in 2018.[24]

Facial recognition start-ups SenseTime and Megvii (Face++) are also reported to be providing their systems to surveillance operations in Xinjiang.[25] *New York Times* reporters were shown a database provided by SenseNets which "contained facial recognition records and ID scans for about 2.5 million people, mostly in Urumqi, a city with a population of about 3.5 million."[26] Meanwhile, local technology companies have been benefiting from the heightened surveillance activity in Xinjiang, such as Leon Technologies based in Urumqi, which in 2017 saw a huge increase in earnings.[27] Beijing-based CloudWalk has also advertised facial recognition technology which it claims can recognise "sensitive" groups of people,[28] and university researchers in Xinjiang have conducted research into "ethnic" aspects of facial recognition templates distinguishing "Uyghur" features.[29]

Some of these companies have received funding from larger, including foreign, investors such as Qualcomm, which has invested in SenseTime, while Kai-Fu Lee's Sinovation Ventures has invested in Megvii.[30]

It is not only in Xinjiang where facial recognition is being used against Uyghur people. It was reported that Chinese East Coast cities are using facial recognition cameras to detect Uyghurs in these locations as well.[31] Police in other Chinese provinces, including in the prosperous Guangdong Province in the south of the country, have meanwhile expressed interest in the surveillance technologies and applications tested and implemented in Xinjiang.[32]

Export of Chinese surveillance technology

Products and services developed in China have started to be exported to other countries, including by companies which have been active in providing surveillance technology and facial recognition capabilities in Xinjiang. Such recipient countries include Ecuador (with its notable ECU-911 system), Zimbabwe, Pakistan and Germany.[33]

In the context of the US-China trade war, at the time of writing the US is considering adding several surveillance companies including Hikvision, Megvii and Dahua to a blacklist, with their participation in Xinjiang facial recognition surveillance activities being part of the justification.[34]

20 Ibid.

21 Ibid.

22 Ibid.

23 Rollet, C. (2018, 23 April). Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang. *IPVM*. https://ipvm.com/reports/xinjiang-dahua-hikvision

24 Mozur, P. (2019, 14 April). Op. cit.

25 Ding, J. (2018, 24 September). ChinAI Newsletter #29: Complicit - China's AI Unicorns and the Securitization of Xinjiang. https://chinai.substack.com/p/chinai-newsletter-29-complicit-chinas-ai-unicorns-and-the-securitization-of-xinjiang

26 Buckley, C., & Mozur, P. (2019, 22 May). How China Uses High-Tech Surveillance to Subdue Minorities. *The New York Times.* https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

27 Rajagopalan, M. (2017, 17 October). This Is What a 21st Century Police State Really Looks Like. *BuzzFeed News*. https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here

28 Mozur, P. (2019, 14 April). Op. cit.

29 Zuo, H., Wang, L., & Qin, J. (2017). XJU1: A Chinese Ethnic Minorities Face Database. Paper presented at IEEE International Conference on Machine Vision and Information Technology (CMVIT). https://ieeexplore.ieee.org/abstract/document/7878646

30 Mozur, P. (2019, 14 April). Op. cit.

31 Ibid.

32 Buckley, C., & Mozur, P. (2019, 22 May). Op. cit.

33 Mozur, P., Kessel, J. M., & Chan, M. (2019, 24 April). Made in China, Exported to the World: The Surveillance State. *The New York Times*. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

34 Bloomberg. (2019, 23 May). U.S. weighs blacklisting five Chinese video surveillance firms over treatment of Uighurs. *Japan Times*. https://www.japantimes.co.jp/news/2019/05/23/asia-pacific/u-s-weighs-blacklisting-chinese-surveillance-firms/#.XXgjTWbQ_IU; Kharpal, A. (2019, 26 May). US takes aim at Chinese surveillance as the trade war becomes a tech war. *CNBC*. https://www.cnbc.com/2019/05/27/china-mass-surveillance-state-technology-at-center.html

AI, law and ethics in China

In principle there are legal protections for the Uyghurs as a recognised minority "nationality" in the Constitution of the People's Republic of China. Article 4 guarantees the equality of all nationalities, protects against discrimination and also protects their rights to use their languages and practise their customs. Freedom of religious belief is also guaranteed by Article 36 of the Constitution. In the case of the targeted use of facial recognition against Uyghurs and other minorities in Xinjiang, "[p]olicies and administrative decisions on both central and provincial levels, however, often contradict the legal protection."[35] Furthermore, individuals are not able to enforce constitutional rights through the court system in China if the rights concerned are not also prescribed in civil laws.[36]

Ironically, Chinese government agencies, companies and universities have been active recently in the global trend towards formulating and issuing statements on AI ethics.[37] Yet the discriminatory ways in which state organs, companies and academics have researched, developed and implemented facial recognition in China would seem not to comply with Article 3 ("Fair and just") of the recent Artificial Intelligence Industry Alliance (AIIA) draft Joint Pledge on Artificial Intelligence Industry Self-Discipline, nor Principle 3 ("Fairness and justice") of the National Governance Committee for the New Generation Artificial Intelligence's Governance Principles for the New Generation Artificial Intelligence.[38]

This gap between stated ethical principles and on-the-ground applications of AI is not unique to China and can be observed in many other countries, including supposed liberal democracies in the West. However, this gap does demonstrate the weakness of unenforceable ethics statements and suggests that "ethics washing" is not a phenomenon confined to the West.[39] In any case, China's ambitions to become the world leader in AI by 2030 and also the leading role it is taking, along with the European Union, in formulating AI ethics initiatives, should be viewed critically given these highly unethical uses of facial recognition domestically.

Conclusion

The uses of cutting-edge AI, especially facial recognition, and other digitised technologies to keep Uyghur and other ethno-religious minorities in Xinjiang under the eyes of a watchful state can be viewed as a particularly acute and racist form of "digital social control" in the context of the increasingly authoritarian rule of Xi Jinping.[40] There is the potential for such monitoring techniques to be rolled out to the broader Chinese population and also beyond through the export of facial recognition technology developed in the Xinjiang "laboratory" worldwide. While so far China's Christian minority has not been subject to the same level of repression as Uyghurs, who tend to be predominantly Muslim, there are reports that Chinese authorities have also tried to install cameras in Christian churches.[41]

The extreme surveillance and re-education measures affecting large swathes of the Uyghur population in Xinjiang are not only disproportionate but also unethical. In particular, the ethnically and religiously targeted use of facial recognition technology against Uyghur people and other minorities in Xinjiang demonstrates the way in which, despite the official rhetoric on AI ethics, AI technologies are being used in China and in different parts of the world to reinforce and at times also exacerbate existing inequalities. In this sense, "algorithmic oppression" is not a phenomenon confined to the US or the West, but is also taking shape in other locations, notably China. The fact that China's AI industry rivals only the US, and the fact that other countries, including Germany, are importing surveillance technologies from China, should give all of us cause for concern.

35 Aktas, I. (2015). Op. cit.

36 While specific provisions of the PRC Constitution may be cited and mentioned in court reasoning, they cannot be used as a direct reason for a ruling.

37 Daly, A., Hagendorff, T., Li, H., Mann, M., Marda, V., Wagner, B., Wang, W., & Witteborn, S. (2019). *Artificial Intelligence, Governance and Ethics: Global Perspectives*. The Chinese University of Hong Kong Faculty of Law Research Paper No. 2019-15. https://ssrn.com/abstract=3414805

38 Webster, G. (2019, 17 June). Translation: Chinese AI Alliance Drafts Self-Discipline 'Joint Pledge'. *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-ai-alliance-drafts-self-discipline-joint-pledge; National Governance Committee for the New Generation Artificial Intelligence. (2019, 17 June). Governance Principles for the New Generation Artificial Intelligence – Developing Responsible Artificial Intelligence. *China Daily*. https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html?from=groupmessage&isappinstalled=0

39 Wagner, B. (2018). Ethics as an escape from regulation: From ethics-washing to ethics-shopping? In E. Bayamlioglu, I. Baraliuc, L. A. W. Janssens, & M. Hildebrandt (Eds.), *Being Profiled: Cogitas ergo sum*. Amsterdam: Amsterdam University Press. https://www.aup.nl/en/book/9789463722124/being-profiled-cogitas-ergo-sum

40 Shan, W. (2018). Social Control in China: Towards a "Smart" and Sophisticated System. *East Asian Policy*, *10*(1), 47-55.

41 Ma, A. (2018, 11 December). China rounded up 100 Christians in coordinated raids and banned people from talking about it on social media. *Business Insider*. https://www.businessinsider.com/china-rounds-up-christians-bans-discussion-2018-12; Yan, A. (2017, 3 April). In 'China's Jerusalem', 'anti-terror cameras' the new cross for churches to bear. *South China Morning Post*. https://www.scmp.com/news/china/policies-politics/article/2084169/chinas-jerusalem-anti-terror-cameras-new-cross-churches

Action steps

The following advocacy priorities are necessary in China:

- Mass surveillance and data gathering targeted at Uyghur people and other minorities in Xinjiang by Chinese authorities and companies should cease immediately, along with the more general repression of these minority groups including internment in re-education camps.
- Chinese authorities and companies developing and implementing facial recognition technologies and other AI applications should be held to account for the unethical ways in which they may be used as a tool of oppression. In particular, they should be judged against the AI ethics principles which have begun to proliferate in China from companies and academic researchers to expose the mismatch between rhetoric and practice.
- The export and use of AI and surveillance technologies from China which may have been developed in the Xinjiang laboratory should be blocked by other countries, and campaigned against by civil society internationally.
- Campaigns against unethical AI should not hesitate to call out unethical developments and uses of AI wherever that may be, in the US, Europe, China, India and elsewhere. Legally enforceable ethical standards for AI must be implemented everywhere. The problem of unethical AI is global. There should be a worldwide ban on the use of facial recognition technologies.

GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building "smart cities"? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called "killer robots".

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH
2019 Report
www.GISWatch.org

APC
ARTICLE 19
Sida