Arendt's Algorithm: AI's Disenfranchising Effect on Refugees as Examined through China's Uighur Population

Gideon Salutin

"*Automation is a new revolution,*
threatening to interrupt the life cycle
in unpredictable ways."

Hannah Arendt, *Cybernetics and Automation*, 1964

Introduction: Big Data Meets Big Brother (Botsman, 2017)

In 2018, Alibaba Chairman Jack Ma advised China's Central Politics & Law Committee that "the future legal and security system cannot be separated from the internet and Big Data" (Bloomberg, 2016). Simultaneously, many Uighurs were being imprisoned in labour camps, caught by the same Big Data legality that Ma was advising. Uighurs are a Muslim ethnicity largely based in China's Xinjiang region, with independent languages and customs from their neighbouring Han Chinese populations. Perceived differences between the two groups including religion, diet, and customs have generated increasing rifts between the two groups, making intergroup socialization very difficult (Han, 2010). They have also intensified widespread Han beliefs that Uighurs are backwards, savage "others", that must eventually be "civilized" (Allen-Ebrahimian, 2019).

While state repression has been enforced in Xianjiang since the Qing dynasty, current security mechanisms are implemented by Beijing, the communist party, and regional police. It is important to keep in mind that, beyond cultural differences and political rhetoric, Xinjiang holds serious economic interest for the Chinese state. It shares international borders with eight countries, all of whom maintain important markets for Chinese industry. It also enjoys the country's largest oil and gas reserves, 80% of its precious metals, one third of its petroleum and two thirds of its coal (Cunningham, 2012). This may be the reason the state has cracked down so hard on this people rather than other historically separatist ethnicities such as the Hui.

The integration of state security and communal distrust has reduced Uighur culture such that many now meet international standards of Internally Displaced Persons (IDPs) and/or international refugees. Within Xinjiang, internal displacement accelerated under Chen Quanguo, who increased surveillance and security over the Uighur minority when he became party secretary of the region in 2016. Chen established a security surveillance mechanism by which the state monitors Uighurs and arrests those it finds suspicious (Pitel, Shepherd, and Klasa, 2020). Many end up in "re-education camps" where they are tortured, humiliated, forced to eat pork, learn mandarin, and sing the praises of the Chinese state. Most stay there for years, and if they survive to their release ("graduation") they are followed, forbidden to maintain familial connections, and often barred from returning home, leaving many in a state of constant homelessness and/or nomadism. This has led to Xinjiang's "Palestinianization"—a term which speaks to its escalating social tensions backed up by settler colonial state policies and security forces(Han, 2010). Recent migration of Han Chinese individuals *en masse* to Xinjiang mirrors Israeli migration into Palestine, and implements similar preferential policies, discrimination, and political repression which Palestinians currently endure. This has provoked many Uighurs to flee Xinjiang, meeting even the UNHCR's limited definition of a refugee. Today China pressures ASEAN and Central Asian neighbours to deport refugees back to China (Yeoh, 2018). The state has also proven capable of reaching Uighurs directly by phone or internet, as occurred to Shawn Zhang after arriving in Vancouver (Yeoh, 2018). This constrains their freedom of mobility while inducing a state of terror. Today's refugees are witnessing that global reach of which Hannah Arendt

warned when she wrote that "Unlike their happier predecessors, [modern refugees] were welcomed nowhere and could be assimilated nowhere" (Arendt, 1951, p. 267). These refugees are not fleeing war but persecution, and through technology, this persecution is capable of pursuing them.

Behind this action is a crisis rhetoric which aligns itself with Western ideology. Since 9/11, China has positioned itself with the United States, claiming to suffer from Uighur "terrorism" and tying Uighur organizations to Al Qaeda. In what Xi Jinping has labelled "the people's war on terror" China has deftly allied itself with a coalition, methodizing global islamophobia into state repression. According to Maya Wang, senior China researcher at Human Rights Watch (HRW), by linking riots and separatist struggles with Middle Eastern terrorism, the country has managed to ramp up state surveillance in the area (Liu, Liu, Yang, and Wang, 2020). China has thus profited by aligning its own politics with the narrative power of Western discourse.

But surveillance appears to have changed since the cloak-and-dagger years of the Gestapo or KGB. Today, crisis rhetoric is used not to staff secret police but to collect data. The internet has produced a data trail which can be exploited by states to monitor residents' behaviour. This is combined with traditional bureaucratic archives including identity cards, home addresses, health records, and financial documents to better staff surveillance tools (Qiang, 2019). As Tazzioli writes: [t]he traceability of migrants' movements and the readable body of the migrant generated through the extraction of biometric traces are combined by state authorities with what data itself cannot say" (Tazzioli, 2020, p. 69). Data surveillance—or *Dataveillance (Qiang, 2019)*—can be

partially understood as a rational response to the massive amounts of public data generated daily—so called "Big Data."

Artificial Intelligence (AI) tools are able to comb through Big Data to produce "actionable knowledge" which is can then be utilized by military security apparatuses (Ali et al., 2016). Through machine learning, computers collect data and produce their own algorithms to perform tasks automatically. Predictive Analytics schools hope to use these computers not only to respond to data, but predict future trends based on past experiences (Ali et al., 2016). This has proven particularly dangerous when applied to criminal justice and security, but that has not stopped global leaders from supporting such initiatives. In 2009 then-UN Secretary General Ban Ki Moon started the UN Global Pulse (UNGP) initiative, aiming to harness Big Data for human development (Ali et al., 2016). In 2015 the UNHCR harnessed this idea to predict crises in Syria (Ali et al., 2016). Such methods are dangerous, and leverage human safety against the human rights to property and privacy. They are the same defences that have been used by the Chinese state which uses predictive analytics to arrest Uighurs before they commit "acts of extremism." In the global refugee regime, states are expanding surveillance of refugees under the guise of AI technology, enhancing governmentality while minimizing their own responsibility as decided by the 1951 Refugee Convention. Uighur IDPs and refugees act as an example of this trend, due to the intensive surveillance they are submitted to by the Chinese state.

An Ad Hoc Panopticon

China's Integrated Joint Operations Platform (IJOP) operates in Xinjiang by collecting Big Data and alerting authorities to those it deems potentially harmful to the CCP regime. It does so through two major devices: the mobile phone, and the camera. These act as tools of disablement constraining Uighur mobility and settlement.

Uighurs are now obligated to carry smartphones, on which police mandate "nanny apps" to monitor Uighurs through their devices. The Jingwang ("cleansing the web") app not only tracks Uighurs' movement, but also records and extracts all messages, internet use, contacts, photographs, and files. These are then amalgamated by IJOP which uses keyword searches to compare the data to its list of potential crimes, which include prayer, visiting banned websites, and other petty accusations (see Appendix 1.1 for more detail) (Pitel, Shepherd, and Klasa, 2020). IJOP then decides who is considered a threat and will thus be arrested, and who will simply continue to be monitored. Cameras, meanwhile, have been equipped since 2011 to recognize facial features and match them with government archives, which can be used to track individuals' movements or find suspect refugees. By 2022, China hopes to have 2.76 billion surveillance cameras feeding into its national panopticonic network. In many ways, facial recognition technology acts as a perfect analogy for the IJOP system. It puts minorities on display, while masking those who are observing, be they individuals, computers, or basic algorithms. Like all panopticons, it is one way, causing sincere psychosocial stress for Uighurs. As Fanon wrote in 1965 "There is not occupation of territory, on the one hand, and independence of persons on the other. It is the country as a whole, its history, its daily pulsation that

are contested [...] Under these conditions, the individual's breathing is an observed, an occupied breathing. It is a combat breathing" (Fanon, cited in Tazzioli, 2020, p. 49).

This was my understanding of Xinjiang until very recently. It is the story Beijing likes to deny; that Uighurs are under a constant state of surveillance, under penalty of prison camps, torture, and death; that Uighurs must be careful with every step to avoid imprisonment at the hands of an omniscient, omnipresent algorithm. Such a world enforces a sense of terror ensuring communal complacence in the face of settler colonialism, limiting outcry by international refugees alongside internally displaced Uighur civilians.

In reality, the technology is far less effective than the state claims. Phone-based trackers in China have been shown to place individuals up to 2km away from their actual location (Liu, Liu, Yang, and Wang, 2020). Voice recognition has proven very dubious, and is often vulnerable to mistakes (Qiang, 2019). "To the outside world," Liu writes, "China can often seem like a monolith, with edicts from Beijing ruthlessly implemented by the rest of the system. The coronavirus pandemic has also demonstrated a much messier reality… The state's ability to access personal data is at times limited" (Liu, Liu, Yang, and Wang, 2020). John Phipps, who recently wrote about Xinjiang for *The Economist* confirmed these limitations (Phipps, 2020). "Uighurs insist on reminding me that even though this is sometimes called a perfect surveillance state, it's not perfect. It's enforced by humans who make mistakes."[1] In reality China's system is limited by the

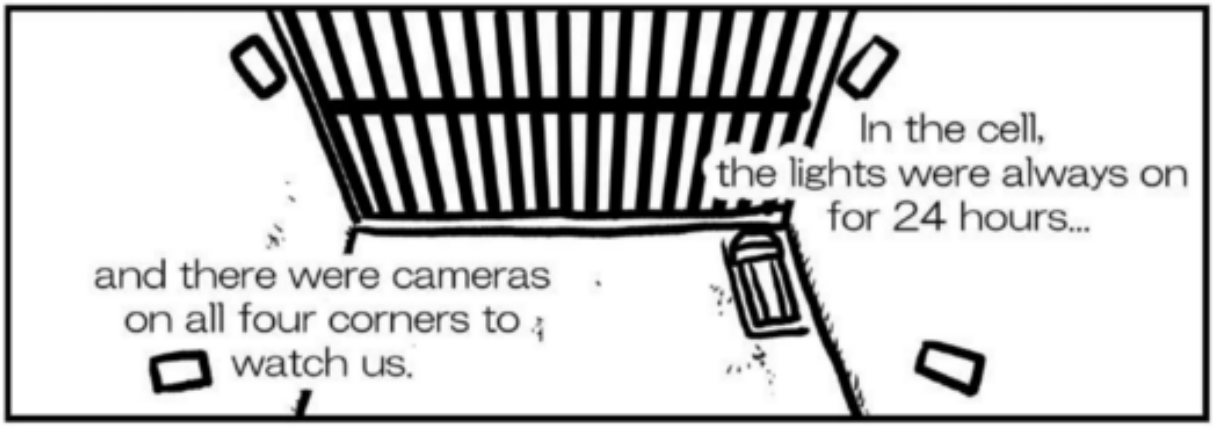
[1] John Phipps (journalist) in discussion with the author, April 2020.

capabilities of current technology. Recognizing this, the state has embraced its own incapacity to establish order.

In doing so they have implemented a regime reliant on what Elizabeth Dunn calls *adhocracy*: "a form of power that creates chaos and vulnerability as much as it creates order" (Dunn, 2012, p. 2). Understanding the coercive power of the state, alongside the ad-hoc nature of IJOP's algorithm, refugees are more likely to obey strict regulations. Surveillance and its repercussions appear random and uncoordinated, increasing psychosocial fears of a state-sponsored panopticon. But unlike Bentham's original panopticon, which failed to address state bias, this adds a level of racialization relating to Islamophobic crisis rhetoric. "The seeming randomness of investigations resulting from IJOP isn't a bug but a feature" Samantha Hoffman, an analyst for an Australian policy think tank, described to the ICIJ. "That's how state terror works. Part of the fear that this instills is that you don't know when you're not OK" (Allen-Ebrahimian, 2019). This is not to say that AI and surveillance technology is not dangerous, but that its implementors have chosen to amplify its danger to better meet their goals. Rather than attempt to be everywhere, China settled for being anywhere.

Case studies may be useful in understanding the coercive effect this can have. After serving an algorithm which sends refugees to prison camps, cameras continue to pursue them. As Sayragul Sautbay, a former detainee explained: "I received a uniform and was taken to a tiny bedroom with a concrete bed and a thin plastic mattress. There were five cameras on the ceiling—one in each corner and another one in the middle… The only room that didn't have cameras was the Black Room, which was used to torture

the prisoners (Stavrou, 2020). The state continues their panopticonic mental projection inside prison camps. This many cameras in this positioning are more than could possibly be necessary. But this overload encourages a sense of being observed, therefore encouraging mental breakdowns and indoctrination. Sautbay's description defends this theory. Notice that she did not just report cameras, but cited the exact number and their position, which clearly had long-term effects on her memory. The use of surveillance technology inside the camps did not only aid in punishing Uighur detainees, but helped to prevent any insubordination. Such a tactic enforces a level of compliance with camp security that overt violence cannot reach, including self-censorship and paranoia.



A panel from a manga written from the transcribed testimony of former Uighur detainee Mihrigul Tursun, who, like Sautbay, emphasized the amount and position of security cameras. One can observe from the panel that this amount is unnecessary for security, and I argue it is to enforce psychosocial repression (Tomomi, 2019)

The same tactics are applied to attempted coverage of the issue. Serene Fang, who worked for PBS's *Frontline*, explored Xinjiang in 2003. She described how Chinese police eventually confronted her with recordings of her journey:

> We thought we weren't being watched. We thought we did not raise any red flags. But as I learned on my second trip, they had watched us almost the entire way. Not only did they watch us in China, but they also crossed the border and watched us and the people we interviewed in Kazakhstan... They also *wanted to let me know* that they knew a lot about me. I had no idea that they had followed me the whole first trip. So I think part of it was to let me know that I couldn't come here and do this, that this particular part of China was very closely observed (Fang, 2015) [italics added for emphasis].

She further described one of her sources, who came to her with information on political repression. "He sat in our hotel room trembling, for close to an hour, and refused to be videotaped… he didn't feel very safe where we held the interview, which was in his hotel room" (Fang, 2015). Maintaining senses of omniscience encourages dread among refugees, limiting any advocacy they might attempt. John Phipps described similar issues, warning me about common mistakes when interviewing these refugees. "Remember that Uighurs grew up *self-policing*, conscious of being watched. What Updike said about "celebrity being a mask that eats into the face" applies to them. You can't just ask them about spies and informants. You have to be aware" [italics added for emphasis].[2] By limiting journalistic coverage of refugees, China inhibits one of their main paths of advocacy while dismantling the potential for a Uighur narrative.

Tazzioli claims that states abuse technology to harness the image of the refugees, and the Uighur case exemplifies her understanding of technology and the state. (Tazzioli, 2020). In this case, tech is being used to make refugees *extremely* visible, both to the general public by visualizing them as terrorists, and to themselves, intimidating them into silence by constantly keeping them under surveillance. There is no time in Xinjiang

---

[2] John Phipps (journalist) in discussion with the author, April 2020.

that Uighurs feel they are not on display—that an image of their likeness is not in some room being made—helping to limit any insubordination that might result. As individuals they are expected to have personal rational reactions in fear of surveillance mechanisms, and therefor comply with state terror. Through this hypervisibility, racial distinctions and Uighur's social positionality are strengthened. Just as invisibility can limit refugee narratives, so too can their over-visibility.

Traditional sources like DNA, health records, and financial documents all combine with technological sources to create this terrified reaction. "This hasn't been a tech triumph," explained Ryan Manuel, director of research firm Official China, "this has been a triumph for the party and their old school methods" (Liu, Liu, Yang, and Wong, 2020). It is to "old school methods" that we now turn.

End of the (online) Rights of Man

Apart from psychosocial terrorism, artificial intelligence serves the state by absolving it of responsibility for refugees. Lack of accountability, or overlapping accountabilities, is a major cog caused by the global AI machine, and mirrors the same overlap in the human rights regime pointed out by Hannah Arendt in 1951 (Arendt, 1951). Hin-yan describes a "practical responsibility gap" in the AI regime in which the manufacturers of an autonomous learning machine are incapable of predicting its future behaviour (Hin-Yan, 2017). This not only muddies the waters of blame for AI actions, but complicates the very logics of cause and effect. As systems grow more autonomous, human control recedes, along with culpability for its work.

By demanding an algorithm act as a detective and jury in Xinjiang, China ensured blame on police or the state would be comparatively weakened. We (as citizens and academics) tend to have limited understandings of robotics. We don't know how programs work, how they are made, or how much autonomy they have. The same is largely true for politicians in power. Hin-yan describes this as a "regulatory lag" in which emergent technologies exist, for some time, under a state of libertarianism, as policy-makers do not understand its inner workings enough to regulate them (Hin-Yan, 2017). This gives surveillance technology "effectively lawless—or at any rate law-free—territory" according to Shoshanna Zuboff, who recently authored a book on the subject (Naughton, 2019). Neither Uighurs nor the international community are capable of demanding advocacy against an enemy no one understands. This leaves those persecuted under AI effectively stateless, without protection from any law in this regard. When Gay McDougal, head of the UN Committee on the Elimination of Racial Discrimination, describes Xinjiang's camps as a "no rights zone" he fails to realize the entire region suffers this reality, due to the shifting of discriminatory mechanism from law enforcement to algorithms (Yeoh, 2018).

Arendt warned of increasing police violence when individuals are not recognized as a state responsibility. In Xinjiang's case, algorithms through IJOP have taken the place of police, acting as a coercive regulator of Uighur mobility. One need only replace "police" with "algorithm" in Arendt's *Origins of Totalitarianism* to see a perfect description of Uighur predicaments right now:

> Since the man without a state was "an anomaly for whom there is no appropriate niche or framework of the general law"—an outlaw by definition—he was completely at the mercy of the [*algorithm*], which itself did not worry too much about committing a few acts in order to diminish the country's burden of indésirables…This was the first time the [*algorithm*] had received authority to act on its own, to rule directly over people; in one sphere of public life it was no longer an instrument to carry out and enforce the law, but had become a ruling authority independent of government (Arendt, 1951, pp. 283-287).

But Arendt's warning should not be understood to mean the police acted independently. Instead, those officers in the early 20th century followed the logic of the state, which dismissed minorities and often acted against them in order to maintain their power. As it did with the police, the state now acts through algorithms to accomplish its ambitions. Similar to the police, algorithms like IJOP are a reflection of state logic.

China, like other states today, manages to avoid responsibility for refugees through language and misunderstandings. Language used by program developers in the public and private sector to describe new technology like AI is often obfuscating, masking realities in dense jargon unintelligible to most people (Sadowski, 2018). This similarly applies to scholars studying new technology, who find themselves incapable of reporting on the subject, disrupting traditional linkages between academia, the press, and state policy (Forsythe, 2001). On top of language, misunderstandings of AI programs obstruct public knowledge. As discussed by Kostakis, actors too often escape blame by pretending their algorithm is natural, rational, amoral, or apolitical, and acts without the prejudices of humanity (Kostakis and Giotitsas, 2014). In reality, algorithmic codes can be extremely biased, resulting from the programmer's intentions. Its output is dependent on the data one puts into the machine and the analysis one hopes to make. One case of

bias was famously documented when an AI in the United States encouraged arresting more African Americans as they made up a higher portion of the convicted population (Feldstein, 2019). In reality, algorithms risk entrenching preconceived racial biases against the refugee "other" and is a major reason why they should be distanced from the refugee regime. I believe China is aware of this, and is utilizing such biases against Uighur citizens while absolving itself in the process. The state is not to blame, but an unbiased algorithm.

Felicity Schaeffer studied this effect within anthropological history. The defences of algorithmic discrimination against refugee populations mimic the naturalist defences used in phrenology and early anthropology to implement colonialism. Now, rather than biological explanations for criminal behaviour among "uncivilized" populations, states use math and logic to colonize Uighur territory. These algorithms maintain colonial binaries related to racial otherness, but relegate such social forces into natural or automatic reactions which the computer effortlessly calculates. The state relies on the algorithms to speak for refugee lives, and to pass judgement on them (Schaeffer, 2018). This speaks to the idea of the "lying refugee," who must be investigated through algorithmic decision making and Big Data, rather than their own testimony. Once again, we see Xinjiang's Palestinianization in action, creating a generation of refugees while colonizing their territory and subjugating those IDPs remaining—led by the state, but implemented through algorithmic decision-making.

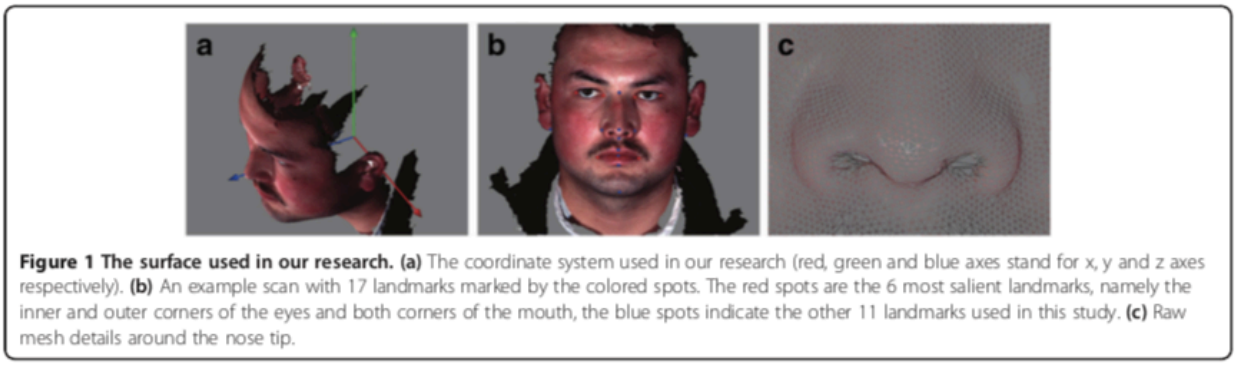


Figure 1 The surface used in our research. (a) The coordinate system used in our research (red, green and blue axes stand for x, y and z axes respectively). **(b)** An example scan with 17 landmarks marked by the colored spots. The red spots are the 6 most salient landmarks, namely the inner and outer corners of the eyes and both corners of the mouth, the blue spots indicate the other 11 landmarks used in this study. **(c)** Raw mesh details around the nose tip.

A figure from a section of Guo et al.'s investigation of facial recognition. I argue that this technology mirrors nineteenth century phrenology, and applies similar logics to amplify modern colonialism and displacement. (Guo, Mei, and Tang, 2013).

Coverage of this ad hoc panopticon largely ignores its human side to focus on the technological marvel that is IJOP. I empathize with the inclination. New technology like artificial intelligence is an extremely appealing subject—flashy, sexy, and unknown. But journalists and academics often find themselves mired in these worlds, unaware that they are simply masking typical state behaviour. In this case, technology has intensified state power over mobility and repression, but by focussing on methods, researchers ignore the actors involved.

"If you want to challenge an algorithmic decision in a court of law," anthropologist Petra Molnar asks, "is it the designer, the coder, the immigration officer, or the algorithm itself which is liable?" (Molnar, 2019, p. 8). Her question is important considering our security institutions' expanding reliance on automated systems. Evidence of bias in algorithms is difficult to determine, and lies outside traditional jurisprudence. This is accompanied by algorithms increasingly deciding state policies, just as police did in Arendt's era. The current refugee regime was programmed to prevent human-ordered

atrocities. "The primary responsibility for safety and security lies with states" The Global Compact on Refugees reads (UNHCR, 2018). As a result, it is possible this regime is incapable of punishing actors for abuses decided by algorithms. To solve this problem, they must understand the decision-making power of the state in its algorithm's conclusions. The illegibility of a computers' program should not be understood as apoliticality among the computer programmers.

Conclusion: Today's Refugee Regime

The advent of artificial intelligence meant refugee populations would increasingly be under threat from international regimes, and have less outlets through which to combat them. Global surveillance mechanisms like the Five Eyes program use AI to review and process findings (Lin-Greenberg, 2020). This embroils questions of accountability in the refugee regime within similar questions asked of artificial intelligence. Either dismissive of these complications or aware of their obfuscational power, today's global refugee regime increasingly utilizes AI at the expense of refugee populations.

The state increasingly relies on AI to draw its borders. Many refugee applications are now determined by automated decision-making algorithms which review the information and output their response. Lie detecting hardware is now deployed at European borders, which process individual's facial movements and voice patterns to analyze whether they are lying, failing to recognize stress, anxiety, or fear—feelings that are often emoted through similar movements (Molnar, 2019). In 2018, the US

Immigration and Customs Enforcement (ICE) reformatted its immigration software to automatically detain *any* migrants, including those with no criminal background, amplifying its ability to arrest and terrorize refugee populations (Oberhaus, 2018). Like IJOP, officers continue to repress refugees, but are now merely following the orders of an algorithm, avoiding direct culpability. This dismantles refugee paths to repatriation, nationalization, and resettlement. In 2012 Australia deployed the EMBRACE mechanism to help decide applications in Australia's Refugee Review Tribunal (Nissan, 2017). This "decision-support system" replaces court procedure with an algorithm that reiterates the two hundred most common arguments used in immigration law and automatically assesses each's applicability to a current case. The Refugee Review Tribunal is then advised based on its findings (Stranieri, Zeleznikow, and Yearwood, 2001). These increasingly dehumanize the refugee, ignored state responsibility under the 1951 Refugee Convention, and distanced state workers from the refugee process. Further, states avoid "old school" asylum hearings in which a judge or jury would meet a refugee, which often generated feelings of compassion and solidarity. The ethical expectations associated with refugee claims, traditionally examined at these hearings, are swept under a rug of algorithmic decision-making. Here, AI acts as a tool to help absolve the state of responsibility shifting blame to agentless computer algorithms just as China escapes blame for the work of the IJOP. This is representative of Tazzioli's point that in achieving their ambitions states often utilize their *will not to govern* as a political technology, passing the buck to others or ignoring major dilemmas (Tazzioli, 2020). As discussed, this technology is not advanced enough to act of its own accord, but acts as an

obfuscating mechanism for the state to avoid direct responsibility—a duplicitous agovernmentality.

In humanitarian circles, artificial intelligence is similarly lauded for its applicability to emergencies. Here we can once again observe crisis rhetoric, as AI is implemented to streamline aid during crises to the detriment of refugee populations. Cameras implemented in Azraq Refugee Camp, Jordan, demanded refugees scan their irises before they could be allotted daily food rations (Molnar, 2019). When the New Humanitarian investigated this site, they found refugees extremely disturbed by these iris scans, but felt obliged to comply at the risk of going hungry (Staton, 2016). Here refugees felt monitored, forced to decide between their right to privacy and their need for food. This mirrors the complacence evident in Xinjiang, where Uighurs were forced to give up any semblance of privacy to avoid coercive repression. Elsewhere, the same decisions must be made by those in crisis. Data aggregation engines like CrisisNet and the Global Database of Events collect Big Data for local governments and international institutions to serve them during humanitarian crises. For example, during Haiti's 2010 earthquake, these agencies collected local statistical registries from refugees, alongside their humanitarian data, social media posts, imagery from handheld phones, and Facebook and WhatsApp messages, declaring ownership over all this private data without the consent of the subjects involved. Such theft constitutes humanitarian imperialism, in which staff utilize a crisis to justify their invasion. As Zuboff writes, these organizations "unilaterally claim human experience as free raw material for translation into behavioural data" through the "trojan horse of technology" (Naughton, 2019). This

risks terrorizing, dehumanizing, and disempowering global refugees, who are increasingly left without any authority over their data and movements.

This is not to claim AI should be barred from migrant issues—indeed it can increasingly help aid workers plan for various events. But its implementation without refugee consent tends to terrorize refugee populations, while its implementation without public understanding allows the state to avoid culpability for its effects. This constitutes a new form of violence, one traditionally based in state interests, but implemented by code. Algorithm's aren't apolitical. We must dissolve the false barrier between algorithm and actor. Whether in Xinjiang, Australia, America, or Jordan, they embody the politics of their programmers and implementers. The state, in this case, is coded.

Appendix

1.1: List of Potential Crimes in Xinjiang understood by IJOP

1. Breaking family planning laws
2. Travelling to one of 26 'sensitive' countries
3. Being involved in the 2009 protests in the city of Urumqi
4. Going on a hajj pilgrimage
5. Being related to someone who is detained
6. Being an 'untrustworthy' individual
7. Providing a place for 'illegal' worship
8. Secretly taking religious texts from the mosque to pray at home
9. Owning a passport
10. Growing a beard
11. Being a 'wild' (unofficial) Imam
12. Using a virtual private network—software that allows access to websites banned by China
13. Owning 'illegal' books
14. Getting married using a fake marriage certificate
15. Reading scripture to a child aged under 16
16. Visiting a banned website
17. Donating money to a mosque
18. Disobeying local officials
19. Praying in a public place
20. Calling someone overseas
21. Having previously served time in prison
22. Downloading violent videos

Bibliography

Stavrou, D. (2020, March 1). *At the mind's limits, by David Stavrou with Sayragul Sauytbay.* Harper's Magazine. https://legacy.harpers.org/archive/2020/03/at-the-minds-limits/.

Ali, A., Qadir, J., ur Rasool, R., Sathiaseelan, A., Zwitter, A., and Crowcroft, J. (2016). Big data for development: Applications and techniques. *Big Data Analytics, 1*(2), 1-24. http://dx.doi.org/10.1186/s41044-016-0002-4.

Allen-Ebrahimian, B. (2019, November 9) Exposed: China's operating manuals for mass internment and arrest by Algorithm. *International Consortium of Investigative Journalists.* https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/.

Arendt, H. (1951). *Origins of Totalitarianism.* Schocken Books.

Bloomberg Editorial, (2016, October 24). *Alibaba's Jack Ma urges China to use data to combat crime*. Bloomberg News. https://www.bloomberg.com/news/articles/2016-10-24/alibaba-s-jack-ma-urges-china-to-use-online-data-to-fight-crime.

Botsman, R. (2017, October 21). *Big data meets Big Brother as China moves to rate its citizens.* Wired. https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

Cunningham, C. P. (2012) Counterterrorism in Xinjiang: The Etim, China, and the Uyghurs. *International Journal on World Peace, 29*(3), 7–50.

Dunn, E. C. (2012). The chaos of humanitarian aid: Adhocracy in the republic of Georgia. *Humanity: An International Journal of Human Rights, Humanitarianism, and Development, 3*(1), 1-23.

Fanon, F. (1965). *A Dying Colonialism.* Grove Press.

Feldstein, S. (2019) The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy, 30*(1), 40–52. http://dx.doi.org/10.1353/jod.2019.0003.

Forsythe, D. E. & Hess, D. (Ed.). (2001). *Studying those who study us: An anthropologist in the world of artificial intelligence*. Stanford University Press.

Guo, J., Mei, X., & Tang, K. (2013). Automatic landmark annotation and dense correspondence registration for 3D human facial images. *BMC Bioinformatics, 14*(1). 1-12. http://dx.doi.org/10.1186/1471-2105-14-232.

Han, E. (2010). Boundaries, discrimination, and interethnic conflict in Xinjiang, China'. *International Journal of Conflict and Violence, 4*(2), 245–56.

Hin-Yan, L. & Zawieska, K. (2017). From responsible robotics towards a human rights regime oriented to the challenges of robotics and artificial intelligence. *Ethics and*

Information Technology; Dordrecht, 22(4), 1–13. http://dx.doi.org/10.1007/s10676-017-9443-3.

Kostakis V. & Giotitsas, C. (2014). The (a)political economy of Bitcoin. *TripleC: Communication, Capitalism & Critique, 12*(2), 431–440.

Lin-Greenberg, E. (2020). Allies and artificial intelligence: Obstacles to operations and decision-making. *Texas National Security Review, 3*(2). 57-76. https://doi.org/10.26153/tsw/8866.

Liu, Q., Liu, N., Yang, Y., & Wong, S. (2020, April 2) China, Coronavirus and surveillance: The messy reality of personal data. *The Financial Times*. https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca.

Molnar, P. (2019). New technologies in migration: Human rights impacts. *Forced Migration Review, (61),* 7–9.

Naughton, J. (2019, January 20). "The goal is to automate us": Welcome to the age of surveillance capitalism. *The Observer.* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

Nissan, E. (2017). Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement. *AI & Society, (32)*3, 441–64. http://dx.doi.org/10.1007/s00146-015-0596-5.

Oberhaus, D. (2018, June 26). ICE modified its "risk assessment" software so it automatically recommends detention. *Vice* (blog). https://www.vice.com/en_us/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention.

Phipps, J. (2020, October 15). "If I speak out, they will torture my family": Voices of Uyghurs in exile. *The Economist*. https://www.economist.com/1843/2020/10/15/if-i-speak-out-they-will-torture-my-family-voices-of-uyghurs-in-exile.

Pitel, L., Shepherd, C., & Klasa, A. (2020, February 17). The Karakax list: How China targets Uighurs in Xinjiang. https://www.ft.com/content/e0224416-4e77-11ea-95a0-43d18ec715f5.

Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy, (30)*1. 53–67. http://dx.doi.org/10.1353/jod.2019.0004.

Sadowski, J. (2018, August 6). Potemkin AI. *Real Life*. https://reallifemag.com/potemkin-ai/.

Schaeffer, F. A. (2018). BioRobotics: Surveillance and the automation of biological life. *Catalyst: Feminism, Theory, Technoscience, (4)*1, 1-12. http://dx.doi.org/10.28968/cftt.v4i1.29635.

Serene F. (2005). Interview With Serene Fang: Secret Meetings and an Unexpected Arrest. Part 2. *Frontline World*. https://www.pbs.org/frontlineworld/stories/china401/fang2.html.

Stranieri, A., Zeleznikow, J., & Yearwood, J. Argumentation structures that integrate dialectical and non-dialectical reasoning. *The Knowledge Engineering Review, (16)*4. 331–48. https://doi.org/10.1017/S0269888901000248.

Staton, B. (2016, May 18). Eye spy: Biometric aid system trials in Jordan. *The New Humanitarian*. http://www.thenewhumanitarian.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.

Tazzioli, M. (2020). *The Making of Migration: The Biopolitics of Mobility at Europe's Borders*. Sage Publications Ltd.

Tomomi, S. (2019, November 26). *What has Happened to Me*. https://imgur.com/a/jEjDd9X

UNHCR. (2018, June 26). Global compact on refugees. Final Draft. *UNHCR*. https://www.unhcr.org/en-us/events/conferences/5b3295167/official-version-final-draft-global-compact-refugees.html.

Yeoh, E. K. (2018). Brave new world meets nineteen Eightyfour in a new Golden Age: On the passing of Liu Xiaobo, advent of big data, and resurgence of China as world power. *Contemporary Chinese Political Economy and Strategic Relations, (4)*2, 593-764, XII-XIII.