Rebecca Uliasz

Algorithmic Vision and Proxy Portraiture, or, I thought I was seeing patterns

Duke University, Computational Media, Arts & Cultures, Durham, NC
rebecca.uliasz@duke.edu

Algorithmic vision and Proxy portraiture, or, I thought I was seeing patterns

Abstract:

Algorithmic vision, the computational process of making meaning from digital images or visual information, has changed the relationship between the image and the human subject. In this paper, I explicate on the role of automated vision as a technique of algorithmic governance, the organization of a population by algorithmic means. The ontological status of the portrait image has undergone a paradigmatic shift with the hegemonic use of automated facial recognition technologies towards predatory policing and profiling practices. By way of example, I argue that algorithmic vision is a site where multiple meanings of "vision" are at play, altering the way a human subject is represented through data. I will explore the paradox between the *operative image*, the image that acts but is not seen by human eyes, and what Louise Amoore calls an "emergent subject," a subject that is made visible through algorithmic techniques (Amoore 2013). Algorithmic vision reveals subjects to power in a mode that requires a new approach towards critiquing the role of the human in automated decision making systems.

Keywords:

algorithmic vision; big data; digital image; biometrics; biopower; operational image

Declarations:

Funding (not applicable), conflicts of interest (not applicable), availability of material (not applicable), code availability (not applicable)

"Portraiture," the act of making a portrait of one's self or someone else, has a nuanced meaning in an era of mass social media amidst of a swell of digital images that ubiquitously flood our everyday sensorium. A portrait, especially a self-portrait, a representation of the self, has relations to the term "profile" in its colloquial use. I take a photo of my face, I post it to my Instagram story. I am adding to my profile, myself as data, an outline of myself sketched through a series of loosely connected points. My portrait dissolves into an abstract contour composed from the lines between likes, clicks, status updates, my depiction in datafied form.

1. *Does one have a right to an image of one's face?*

I kept coming back to this question last spring when I learned about the controversy surrounding a dataset created by the Duke University Computer Science. DukeMTMC (Multi-Target, Multi-Camera), a large-scale database of images of students and faculty captured by Duke researchers using a university sanctioned campus surveillance camera system in 2014, was previously one of the largest and most frequently utilized datasets for video re-identification, a process that uses computer vision and artificial intelligence to identify and track targeted individuals within live video feeds (Tomasi et al. 2016).

Duke researchers claim that the project, funded by the US Army Research Office and National Science Foundation, was originally intended to improve systems for motion detection of objects in video, regardless of "whether [the objects] are people, cars, fish or other" (Tomasi et al. 2016), and was subsequently made available for download on the Duke Computer Vision research website. The dataset was recently taken down, after it came under fire in April 2019 for ethical and privacy violations following an exposé by researcher Adam Harvey that prompted Duke's Institutional Review Board to revisit the terms of the collection and use of the image data (Harvey and LaPlace 2019). Harvey's research reveals that the dataset has been irreversibly implemented in computer vision, body tracking, and facial recognition systems by academic, governmental and military institutions across the globe. Significantly, the dataset has been traced to research papers published by Chinese AI SaaS companies associated with the surveillance techniques used by the Chinese military to target and monitor the activities of Uyghur populations in remote northwest China. As Harvey points out, this implementation doesn't stray too far from the original motivation of the Duke researchers, who published a subsequent paper in 2017 titled "Tracking Social Groups Within and Across Cameras." And yet the context makes all the difference.

While this dataset is no longer available through official Duke affiliated websites, by the time it was taken down it had already been cloned into many databases around the world. When I learned of this episode, I easily recovered an edited version from a publicly linked cloud drive. When scrolling through the dataset, which contains images of students entering and leaving academic buildings and places of worship, one might see how this information could easily be weaponized to target and discriminate against marked individuals. In Harvey's analysis, this is but one example of "an egregious prioritization of surveillance technologies over individual rights" (2019). As I sifted through thousands of blurry images, hardly discernable faces aside from a pair of glasses here, a baseball cap there, I wondered exactly *who's* individual rights were actually at stake?

Here, I found the paradox of the DukeMTMC controversy as it was criticized in the terms of contemporary discourse around data, surveillance, and individual privacy, especially with regards to images of one's face, to be a common one. If say I, a white female graduate student at Duke University, found an image of myself in this dataset, what harm would come to my rights as a result? Considering the role that big data plays in the Chinese Communist Parties' (CCP) current policing and detainment of Uyghurs in Xinjiang territory, can we not claim that the human rights of the surveilled populations are much more compromised in this situation? While a detailed consideration of the CCP's ongoing exploitation of Uyghurs as a systemic function of geopolitical and economic initiatives is beyond the scope of this essay, here I consider the role of the DukeMTMC dataset in propagating techniques of governance through a synergy of government, corporate, and academic aims.[1] The paradox around contemporary demands for rights to one's personal data and ethical regulations regarding the future use of personal information becomes clear when we realize that, in regard to the DukeMTMC case, we don't actually *see* ourselves reflected in the algorithmic system on a personal level. It does not index us as individuals. In other words, our images break from representation in the sense that they no longer mean what they appear to mean, and sometimes don't even appear at all.

2. How do we see a photograph of a face?

For Barthes, to have one's portrait taken is to experience a microdeath, to feel oneself slide from subject to object position. When we pose for a portrait, we enter a "closed off field of forces," a closing in of self that at once over codes us in a field of representations and affirms us to a future viewer. When we look at a photo of a face, we witness the conquest of a subject by the apparatus of photography, an obfuscation of self, undertaken in order to represent oneself to the world (Barthes 1980).

The conquest of the world as a picture is articulated by Vilém Flusser in his *Towards A Philosophy of Photography* (2000). The photographic universe, he tells us, is characterized by an inversion in the Cartesian model—concepts no longer signify the universe, but rather the universe is programmed to signify concepts. The camera, the first apparatus for changing symbolic meanings in the world, "knows everything and is able to do everything in a universe that was already programmed in advance for this knowledge and ability" (2000: 68). The photograph has a future effect, it casts a magic spell. It has the ever-developing ability to program culture in its image through constraining possibility and habituating action.

Enter what Flusser calls the technical image, that illusory abstraction that appears to be a direct index of reality but is really a meta abstraction of text, which is itself already an abstraction of a traditional image. Although they appear to touch the real, technical images are 'encoded' with concepts of the world. They project those concepts back out onto the world, inhibiting humans their capacity to understand reality. Here, we are met with the crisis of representation, an overabundance of information, and a multiplication of signification. Characteristic of the technical image is its ability to create information, to create *new* meaning out of thin air (or rather, un-photographed, un-informed nature). This raises the ur-question of Flusser's explication, and a paradox that maps onto our contemporary computational regime—if there is no deeper meaning underlying cultural existence, how do we separate noise from information without slipping into mass paranoia?

Although Barthes tells us the slippage of the photograph occurs in the failure to distinguish between the thing and its representation, how does the digital image complicate the status of the thing? The slippery ontology of the digital facial image warrants further contemplation in a moment where digital images have gained new significance in the operations of global capitalism and algorithmic governance. Paradoxically, as images of faces are amassed in digital form, the face recedes from our sight. As we are flooded with news of global terror, domestic injustices validated by surveillance technologies, and predatory commercial practices grounded in data, ironically,

[1] For an in-depth analysis of the systemic invisiblization and separation from mainstream culture of the Uyghur population as a political and economic strategy of the CCP, see Danika Cooper's "Invisible Desert."

we lose touch with the ability to see the images that are said to be at the root of it all. Images disappear from sight with their absorption into data sets—the universe of raw matter through which algorithms come to know reality. It is in this vanishing act that digital images function as one component of *algorithmic vision.*

3. So how does an algorithm see?

A technical aside, deep learning, as described by Ian Goodfellow, is an advanced form of machine learning that uses a layered neural network to perceptualize patterns in order to train a classification algorithm (Goodfellow et al. 2016). Deep learning techniques, writes Goodfellow, are intended to simulate the intuitive reasoning methods that humans use to make decisions in the real world, where complex variables and incomplete information negate the possibility of relying on a precodified means for arriving at complex decisions. Such algorithms require the "ability to reason in the presence of uncertainty" – where there is unobservable or incomplete information, deep learning algorithms rely on random variables derived from probability theory. Deep learning algorithms vary widely in their methods and applications but Goodfellow outlines 4 key components each must have—a dataset, a cost function, an optimization procedure and a model (2016: 151). Each of these components work in tandem to train an algorithm to classify the objects it 'sees" in an efficient and precise manner.

One type of algorithm often used in image recognition applications is called a Convolutional Neural Network, which specializes in processing data in a grid like topology. While explaining the specificity of these algorithms is beyond the scope of this paper, important to their design is the use of convolutional layers called tensors that are used to weight input data according to a specific array of parameters This array is referred to as the *bias* and is used to produce what is called a feature map. Other layers of the neural net perform an operation called pooling, which down samples information to reduce dimension, retaining only the features deemed most important to the algorithm. In sum, input data is initialized with random weights and processed through a set number of convolutional and pooling layers and the output is compared to the expected result to calculate error. This calculated error is then propagated backward into the hidden layer(s) in order to tune the learning algorithm, the process repeated a specified number of times or until the desired error rate is achieved. Crucial to this operation is the introduction of randomness—the multiplication of data by any number of possible states—in order to infer patterns within information. In a way, CNN algorithms act as a playground for programmers to tweak the variables of weighted layers until the economically precise outcome is derived.

Here, it becomes clear that with algorithmic vision, meaning is derived through an iterative logic of pattern finding. This method of making meaning through empirical perception of patterns implicitly refers to "vision" in its etymological sense. In the Western tradition, not only does the Latin *videre* connote the privileged sense for rational knowledge of an outside world, but as Orit Halpern notes, it also has an evidentiary implication (Halpern 2015). Algorithmic vision has a magical capacity to construe evidence from possibly meaningful correlations, patterns read into data.

Algorithmic vision, explains Hito Steyerl, alters the relationship between realism and veracity. Where optical media have a certain veneer of objectivity, for Steyerl, "the verisimilitude of vision is not based on assumptions about objective hardware but on the replication of brain functions (or what are currently believed to be brain functions)" (2018: 10). Algorithmic vision is "intelligent" to the extent that it simulates the scientific understanding of an intelligent human brain. A stable and absolute human is necessary for "artificial" intelligence to be born in its image. The "big" in big data should be emphvasized here, as the sheer magnitude of information to sort through motivates a technological model of vision that can exceed human capacities. An enhanced model of the human mind gives rise to techniques for making decisions in the face of incommensurable amounts of information, a means for rendering a clear path forward.

Seeing like an algorithm requires what Amoore calls a risk calculus—a derivative form used by state power that incorporates uncertainty in order to array possible futures. Amoore explains that techniques of governance have shifted post 9/11 to algorithmic means of calculating possible futures states (Amoore 2013). This sensibility shot through with the anxiety of potential catastrophe gave authority to new calculation techniques to incorporate unaccountable contingencies. Amoore explains that in the absence of sufficient data, the security algorithm "if a and b, in association with c, then x" is used to ontologically associate unknown values (2013: 59). This abstraction involves a continuous disaggregation and reaggregation of noncausal data, a constant shuffling the relations until a pattern deemed significant emerges.

Algorithmic patterning, ironically, facilitates decision making processes based on what is *not* present. Akin to Foucault's biopolitics, algorithmic vision creates a norm through imposing connections between data points that it decides are related in some way. Thus, anything that falls outside of this mutable norm is considered an anomaly. Algorithmic vision, noted by Matteo Pasquinelli, operates in two co-dependent modalities: pattern recognition and anomaly detection, which he calls "two sides of the same coin of algorithmic governance" (2015: 3). Abstraction and concretization work in tandem, proliferating mass apophenia, the hallucination of patterns in meaningless information.

This same trick of inducing actionable patterns is found in the violent policing of Uyghur populations in China. Enacted through Xi Jinping's "people's war on terror", algorithmic profiling doubly correlates religious extremism with all expressions of Uyghur Islam, and all Uyghur Muslims with quantifiable biometric characteristics. Through invasive surveillance practices like the Integrated Joint Operations Platform (IJOP) which monitors Wi-Fi, CCTV cameras and government IDs, governmental officials have both detained targeted individuals in "re-education" centers and submitted them to further biometric profiling so as to both form a comprehensive data print of the individual, and feed data back into their system to train the machine learning algorithms that are designed to target Uyghurs' physiognomy. Drawing together information that ranges from "the color of a person's car, to their height down to the precise centimeter" to activities that would otherwise be considered lawful, like "not socializing with neighbors", officials use the IJOP to flag individuals it deems high risk in order to prompt further investigation (Human Rights Watch 2019: 2). In the name of preempting "unsafe actors," the Chinese government has adopted a strategy enforced through techniques of risk—in other words, the Chinese government defines the category of risk, and feeds a system data until it is trained to automate decision making, crystalizing an ad hoc instrumental technique of reason. President Xi's "stability maintenance" initiative exemplifies an automated risk calculus that takes the entire Uyghur population as a testbed for techniques of data extraction for market potential (Byler 2019). The logic of pattern recognition is found in a 2016 researcher police report on the operations of IJOP:

> *if* a person usually only buys 5 kilos of chemical fertilizers, *but* suddenly [the amount] increased to 15 kilos, *then* we would send the frontline officers… to check its use. If there is not a problem [they would] input that into the system and lower the alert level (Ningning 2016, emphasis mine).

Where there is incomplete information on each citizen, the IJOP performs a continuous disaggregation and reaggregation of noncausal data, constantly shifting the relations until a pattern deemed significant emerges. Algorithms fracture and fragment a dataset, to the extent where it has very little to do with its underlying referent. It is recombined and projected forward to the effect that a new visualization is made to emerge—a diagram of the lines that cut across the dataset rather than what is contained within.

The government calls upon knowledge provided by data analytic and security companies. These companies then can make use of infinite troves of data to form infinite correlations between samples, generating an essentially infinite number of proprietary algorithms to sell to government and corporate contractors. Among theses government contracted companies are Chinese AI SaaS SenseTime and SenseNets, both of which Harvey linked to the DukeMTMC case (2019). Researchers from both companies published a paper that proposes a method of training a neural network that uses DukeMTMC to perform feature composition analysis on pedestrian images taken in crowded or noisy public spaces to overcome problems of occlusion—it fills in what cannot be seen by the machine eye. In a sense, the circulation of DukeMTMC has enabled the expression of state power that acts through *something that literally does not exist in the collected dataset,* it fills in a gap. The preemptive techniques of algorithmic vision here act through the very contingent relations they produce. An unknown risk yields to the constitution of a subject.

The creation of a proxy—or a stand in that represents an unknown value—allows for the visualization of a portrait of a subject through non-visual means (Chun 2018). Algorithmic hallucination of subjects as a function of biopolitical control. Amoore's risk calculus is again at play in the creation of a mutable norm that prioritizes economic precision over truth so that action can be taken in the present moment. Amoore explains how border technologies express this risk calculus in a space of unknown possibilities by drawing data from diverse sources, like fingerprints, linguistic analysis, travel habits, and financial records, in order to attach risk factors to individual subjects who are not part of this database already. Sovereign decisions are made at the border on individuals that are created as subjects of governance by the "life signatures" that are inferred onto them. The "biometric border" she explains, creates an emergent subject through the combination of fragments (2013). The subject is made to emerge through a correlation of elements composed of other subjects, objects, and the relations between them. She is drawn up in a profile that is taken as a governable body. She is visualized, in the sense that she is assembled in the process

of mechanically revealing something that isn't actually present. Subjects are disaggregated and reaggregated as proxies made out of data hallucinated into the shape of a face.

The proxy, in order to come to stand in for a human being, requires a few components to work in tandem. First, as noted, it requires disaggregated information from which connections and patterns may be derived. But it also requires discursive regulation. Risk calculation might be an economic technique, but it is also a political one. In order to provide justification for tactics used to systematically quantify and exclude human life, an affective state of uncertainty and possibility of impending danger must be the norm. Danika Cooper notes the similarities between the "War on Terror" discourse evoked in the United States after September 11, and the People's Republic of China's treatment of the Uyghur population around this same time (2020). The role of national governments in labeling certain populations "terrorists" in both cases positions those populations as a threat to national security and the well-being of the nation as a whole.[2] The looming threat of attack is given as justification for mass surveillance and the targeting of marked bodies through often violent means.

The means of governance are validated by the ends, which are given as necessities, created through the cloud of uncertainty fashioned through political discourse. In this vein, corporate media and the circulation of information become some of the most potent tools for crafting what is and is not made visible in a given regime. Considering our contemporary moment of social media oversaturation, information overload, and overabundance of digital images that are questioned on the grounds of their "truth" value, what is the role of visual culture in crafting a discourse of risk when images have ceased to have a relationship with truth?

4. The problem with proxies

Something has changed with our facial images. When they disappeared, they came back bounded by a thin green box. For digital images to be made useful in training an object recognition algorithm, they must be organized in accordance to some type of knowledge system, that is, they must be arranged in a taxonomic form. A taxonomy applies names to objects in order to reify them as part of an epistemology. In data sets, the labor of naming things is often done through hired mechanical turk work. Anonymous taggers in various countries might classify thousands of images for microscopic payments. Here, the act of applying a name to an object creates that object as an addressable data point within a sea of information. Uncertainty is resolved through information science and data analytics. The bounding box follows this logic—more than a means to name an object, it is a means to bring this object into being as one that is ontologically stable and addressable, and therefore useful as raw material, also known as data. When amassed by institutional powers, often United States academic universities or military initiatives, it is known as big data. Boxes, in their supreme ability to standardize according to a norm, give form to the "governing of databased bodies" on a larger-than-life scale (Browne 2015).

This act of standardization of digital images might be likened to industrial standardization. Standardization, as we know, has roots in the design of the industrial factory, where specialization is forsaken in the name of efficiency. For these disappeared facial images to become productive of capital, they need to be addressable as governable units so that they might be coordinated to ensure maximal efficiency. Standardization is also a technique historically used by the state to regulate a population through bureaucratic means, like censuses and identification cards. However, as techniques of governance become more and more like those of the post-industrial factory, that is, automated and bound to information technology, we experience what has been called algorithmic governance.

Matteo Pasquinelli indicates four fields of governance transformed or amplified by algorithms—enemy recognition in warfare, sociology and criminology, labor exploitation, and fear of singularity (2015). These fields have been underscored as technologies used by the carceral state used to create uncertainty and incite paranoia as a means of control (Amoore, Steyerl, Apprich). Particularly, these modes of governance are scrutinized for their predatory practices that depend on their preemption of racialized subjects (Wang, O'Neil). If Flusser's technical image had the magic ability to program racist discourse into society through an oversaturated informational-visual milieu, algorithmic vision incites hallucination, multiplying and justifying modes of predatory practices where it sees fit.

[2] The Human Rights Watch confirms the "Strike Hard Campaign", on behalf of the CCP, asserts their purpose as "safeguarding social stability". Police and local officials in the Xinjiang region are required to submit "unusual" activity, or information "related to stability" to the platform in order to help identify "violent terrorists" and those who "challenge state security, ethnic unity and social stability." (Human Rights Watch report)

The use of algorithmic vision as a hegemonic way of seeing begets urgent aesthetic and political problems. Writes Jackie Wang:

> If what we can perceive with our senses delimits what is politically possible, then how do we make legible forms of power that are invisible? How can we imagine ourselves out of a box that we don't even know we're stuck inside? Like a character in a Franz Kafka story, we are called into presence, managed, confined, and punished by an authority that we struggle to locate or identify, and every time we embark on a quest for answers, there is just infinite deferral and postponement. (2017: 52)

As Wang notes, we cannot *see* the images that are taking effect on us, so how can we begin to understand what rationale they are following? These images do not adhere to cultural critique or symbolic analysis because they complicate our given philosophical notions of the links between visuality and knowledge. Noting this disjuncture as it played out in the development of automated warhead technologies, filmmaker Harun Farocki describes "operative images" as "images that do not represent an object, but are part of an operation" (2004). In Farocki's well cited account, operative images are those that actually *do* something in the world by providing a program for action. Key to the operative image is that it maintains an unclear relationship to its object—its representational aspects are considered somewhat arbitrary to the information it contains.

While the types of real time target tracking and missile guiding systems that Farocki scrutinized still appeared to the human controller in the form of visualizations, an emerging paradigm in media theory takes the operative image to have vanished completely. Artist Trevor Paglan coins "invisible images" to describe those images "made by machines for machines" that effectively take humans "out of the loop" (2016). Machine readable images become literally divorced from human sensibility—a feedback loop that constantly reconfigures the distribution of the sensible at any given moment. With machine learning, operative images are notably "black boxed", that is, they are part of an operation shielded from the human eye. These images are operational abstractions of information that may be patterned according to a given logical method—they are an expression of a paranoid machine that functions to establish order within the incomputable mess of the world.

If the modern state has historically controlled the mechanisms that make one legible through record keeping, these conditions no longer describe the techniques of governance that operate via algorithmic vision, where power is expressed through regulating what is and isn't made visible. Here, the digital image has lost its veracity—its operative function is rather to produce doubt as a condition that allows for speculation and acting upon unknown futures. Thus*, error and disinformation take on a productive function* through the operative image through granting sovereign authority to decide in the absence of sufficient information. Here, we find ourselves at an impasse. That is, if algorithmic vision has the capacity to perceive what is beyond the limits of the human, yet politics exists in the realm of the sensible, how can we account for automated decisions made on human lives that appear utterly *senseless?* If we accept the total dissolution of truth and meaning altogether, ontological uncertainty becomes a tool for hegemonic power to wield with no limit.

5. I thought I was seeing patterns

In Farocki's video work "I Thought I Was Seeing Convicts," we, the viewer, are guided to consider the surveillance techniques used by a high security prison in Corcoran. Farocki juxtaposes images together, showing us footage from security cameras alongside visualizations used by an analytics corporation to calculate the purchasing patterns of customers in a supermarket. "What can be accelerated and increased in prison?", Farocki wonders. Body scan diagrams appear in the lower corner of the screen, bringing to mind the type of procedure familiar to anyone who has ever had to pass through the TSA. What can be accelerated and increased in prison?

Here, an astute viewer notices the time stamps on the security footage might assume the meeting of these live feeds in some sort of center control center where this footage might be recorded and sorted to accumulate a profile of a certain inmate. Foucault's panopticon levels up and gains an ability to see through both space and time. We learn that the profiles are amassed as evidence to determine what a specific inmate should and should not have access to, the yards they are permitted to occupy, and the inmates they are allowed to interact with. These images are not seen by the inmates, but may be used by guards, for example, to place two inmates from opposing gangs in the same yards, resulting in deadly stand offs that are preempted by the guards for their own entertainment.

For Farocki, the security camera stands in metaphorically for the gun. Inmates need not be accosted with literal guns in order to be made to die. They are convicted on the basis of patterns drawn by guards through the

accumulation of data. A proxy of the inmate is sent in to stand off in the yard. Farocki reveals that this black box of decisions that caused one man to take another's life contained nothing but a human corruption of power. With the black box oft evoked in describing machine learning algorithms, maybe we find something more like Flusser's black box, where the capture of the subject is made though the combinations of a priori categories encoded into the software of the apparatus. The camera for Flusser is a series of nested metaprograms, each obscuring the function of the next from the human user. The mechanics of the production of the subject of the image are invisiblized, and the image-subject and photographer alike are programmed by the restrains of the camera. However, distinct from Farocki's prison security booth, this black box must remain opaque to function and perhaps if we were to attempt to see the images inside, they might not look like very much to us.

But there is another type of seeing at play in algorithmic vision. Vision has multiple meanings, and in this case, it is not just a mechanical program that epistemologically frames a subject, but it is also an operation. In this sense, algorithmic vision is closer to what Deleuze calls *visibilités*, or non-discursive processes that are discursively enacted to make subjects visible to power in certain assemblages (Deleuze 1988). Put differently, v*isibilités* brings together power and its object in a way that makes the object visible in a determined way at any given moment. An evocation of futurity, where determination and realization are allowed to remain open until the moment they are closed in upon by power. In this sense, the subject known to computer vision is never out of the loop, so to speak, but a point along a continuum of images that constitute the assemblage from which individuals might be imaged again and again. Making an image of a subject is an operation necessarily enacted by algorithmic vision to capitalize upon virtual potentiality.

So what of the ontological status of the operational image within algorithmic vision? When the image is considered within with in the concrete discourses of visuality and representation, we might agree that the image has vanished from sight. However, to expound upon the operational nature of these images is to position them within a technical universe where potential images have the capacity to act on each other. To see like an algorithm is *not to perceive an image of something or someone*, but to produce a world of relations, the grounds from which subjects are made, seen, and named.

Contemporary modes of algorithmic governance move beyond the constitution of subjects through calculated modes of recognition. With algorithmic governance, the power to subjectify meshes with the ideology of development and innovation. A teleology of capital acceleration brings state and corporate aims into alliance such that the production of a subject becomes a quite arbitrary operation undertaken for the ongoing fine tuning of a post-sovereign megastructure. Does an image of a face mean anything at all?

Here, we return to the inconsistencies evoked in the usage of the facial image within algorithmic vision. So much as the DukeMTMC images are anonymized in their disappearance into a dataset used to train technologies that are future oriented, a cruel indexicality is at play in the vision technologies used by the Chinese Communist Party to identify and track individual citizens. The IJOP system used to monitor the Uyghur population in Xinjiang functions doubly to take into account biometric information that is made available through mass surveillance alongside information that is *unknown* or hallucinated from this data. Chinese citizens are at once identified via facial images and created as emergent subjects that are programmatically restrained based on a hidden calculus. Moreover, the various actors that constitute this assemblage of power that prescribes these "life signatures" are multidimensional in their motives. The IJOP serves as a platform of governance, yet the discourse of risk serves to hide economic incentives[3]. The role of algorithmic vision technologies is key in the apparatus that images a population in order to render them invisible. The digital facial image, while linked to a real body, has the power to remake the body as a function of sovereign power, a life signature given form through a recognized face. A suspension of basic legal rights is justified through technological means. How does this very real repression of rights, restriction on religious expression, and literal immobilization of a population move us to think differently about the anxieties around the fragmented roles of identificatory images within systems of automated vision?

Maybe it is possible that our visual paranoia and ontological mistrust characteristic of the post truth era proliferate from our own critical inability to elucidate the connection between vision, the subject and truth in the first place. If we've managed to simultaneously distance ourselves from the truth value invested in vision given through

[3] Beyond the scope of this article, the CCP's policing of the Xinjiang Uyghur Autonomous Region has been associated with government initiatives to extract valuable resources from the area, not limited to its key geographical location which would strategically allow the CCP to its Belt and Road Initiative. For more reporting see (Dahir 2018; Byler 2019; Buckley and Mozur 2019; Human Rights Watch 2019)

European natural philosophy yet critically consider our own conditions through the lens of those same humanist philosophical methods as they are concretized by technoscience, we make ourselves over and over in the same image. To claim the eradication of the human in the machine is to produce a conceptual blind spot, allowing for exploitation and extraction to falsely appear an unfortunate side effect of technoscience, as opposed to paradigmatic. A more useful consideration might be to articulate the philosophical presuppositions of the human given through the very models of perception birthed by cybernetic science. To what extent do we need to modify out understandings of humanism in light of systems that do not have a "human in the loop"? The tension between the human and inhuman contained within every system might be a starting point for critical thought to find new ways to challenge the visions created by systems of algorithmic governance.

Reference List

Agamben, Giorgio. (2005) *State of Exception.* Chicago: University of Chicago Press.

Amoore, Louise. (2019) Doubt and the Algorithm: On the Partial Accounts of Machine Learning. *Theory, Culture & Society* (SAGE) 36 (6): 147-169.

Amoore, Lousie. (2013) *The Politics of Possibility: Risk and Security Beyond Probability.* Durham, NC : Duke University Press .

Apprich, Clemens, Hito Steyerl, Wendy Chun, and Florian Cramer. (2018) *Pattern Discrimination.* University of Minnesota Press.

Barthes, Roland. (2010) *Camera Lucida: Reflections on Photography* . Hill and Wang .

Browne, Simone. (2015) *Dark Matters: On the Surviellance of Blackness* . Durham: Duke University Press.

Buckley, Chris, and Paul Mozur. (2019) "How China Uses High-Tech Surveillance to Subdue Minorities." *New York Times* . May 19. nytimes.com.

Byler, Darren. (2019) "China's hi-tech war on its Muslim minority." *The Guardian.* August 11. theguardian.com.

Chun, Wendy. (2018) "On Patterns and Proxies, or the Perils of Reconstructing the Unknown." *e-flux Architecture: Accumulation.*

Cooper, Danika. (2020) "Invisible Desert." *e-flux Architecture: New Silk Roads.*

Dahir, Abdi Latif. (2018) "China is exporting its digital surveillance methods to African governments." *Quartz Africa.* November 1. Accessed May 2019.

—. (2018) "More African governments are trying to control what's being said on social media and blogs." *Quartz Africa* . July 17. Accessed May 2019.

Deleuze, Gilles. (1988) *Foucault.* University of Minnesota Press.

(2000) *I Thought I Was Seeing Convicts.* Directed by Harun Farocki.

Farocki, Harun. (2004) "Phantom Images." *PUBLIC* 29: 12-22.

Flusser, Vilém. (2000.)*Towards a Philosophy of Photography.* Reaktion Books.

Foucault, Michel. (1995) "Panopticism." In *Discipline and Punish: the Birth of the Prison*, 195-230. New York: Vintage Books.

—. (2009) *Security, Territory, Population* . London : Palgrave Macmillan .

—. (2008) *The Birth of Biopolitics* . New York: Palgrave Macmillan .

Francesco Solera, Simone Calderara, Ergys Ristani, Carlo Tomasi, and Rita Cucchiara. (2016) "Tracking Social Groups Within and Across Cameras." *IEEE Transactions on Circuits and Systems for Video Technology* 441-453.

Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. (2016) *Deep Learning.* MIT Press.

Halpern, Orit. (2015) *Beautiful Data: A History of Vision and Reason since 1945.* Durham: Duke University Press.

Harvey, Adam, and Jules LaPlace. (2019) "DukeMTMC." *MegaPixels: Origins, Ethics, and Privacy Implications of Publicly Available Face Recognition Image Datasets.* https://megapixels.cc/.

Human Rights Watch. (2019) "China: Big Data Fuels Crackdown in Minority Region." *Human Rights Watch.* hrw.org.

—. (2019) "China's Algorithms of Repression." *Human Rights Watch.* hrw.org.

Murgia, Madhumita. (2019) "Who's using your face? The ugly truth about facial recognition." *The Financial Times* . September 18. ft.com.

Ningning, Zhang. (2016) "Big data "out of traffic"." *Southern Magazine.* October 25. epaper.southcn.com.

O'Neil, Cathy. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* New York: Crown.

Ong, Aihwa. (2006) *Neoliberalism as Exception: Mutations in Citizenship and Sovereignty.* Durham : Duke University Press .
Paglan, Trevor. (2016) "Invisible Images (Your Pictures Are Looking at You)." *The New Inquiry.* December 8. Accessed May 2019.
Pasquinelli, Matteo. (2015) "Anomaly Detection: The Mathematization of the Abnormal in the Metadata Society." *transmediale.* Berlin.
Ristani, Ergys, Francesco Solera, Roger Zou, Rita Cucchiara, and Carlo Tomasi. (2016) "Performance Measures and a Data Set for Multi-Target, Multi-Camera Tracking." *European Conference on Computer Vision workshop on Benchmarking Multi-Target Tracking.*
Saticky, Jake. (2019) "A Duke study recorded thousands of students' faces. Now they're being used all over the world." *The Chronical.* June 12. dukechronical.com.
Sound Vision Foundation. (2019) *About Uighurs.* saveuighur.org.
Steyerl, Hito. (2014) "Proxy Politics: Signal and Noise ." *e-flux journal* .
The Economist. (2018) "A web of silk: China talks of building a "digital Silk Road"." *The Economist.* May 31. Accessed May 2019.
Wang, Jackie. (2017) *Carceral Capitalism.* Cambridge: MIT Press.