1 Enclosure

In mid-2017 a Uyghur man in his twenties, whom I will call Alim, went to meet a friend for lunch at a mall in his home city in the Uyghur Region. At a security checkpoint at the entrance, Alim scanned the photo on his government-issued identification card and presented himself before a security camera equipped with facial recognition software. An alarm sounded. The security guards let him pass, but within a few minutes he was approached by officers from the local "People's Convenience Police Station" (Ch: *bianmin jingwuzhan*), one of more than 7,000 rapid-response police stations that have been built every 200 or 300 meters in the Turkic Muslim areas of the region.[1] The police contractors took him into custody.[2]

Alim's heart was racing. Several weeks earlier, he had returned to China from studying abroad. As soon as he landed, he was pulled off the plane by

police officers responding to a nationwide warrant for his arrest. He was told his trip abroad meant that he was now under suspicion of being "untrustworthy" (Ch: *bufangxin*). Policing contractors and health workers then administered what they call an "all people's health check" (Ch: *quanmin tijian*), which involves collecting several types of biometric data, including DNA, blood type, fingerprints, voice signature, and face or iris scan—a process that all adults in Xinjiang are expected to undergo. Then they transported him to one of the hundreds of "detention centers" (Ch: *kanshousuo*) that dot Northwest China.

Since 2017 as many as 1.5 million Turkic Muslims have moved through hundreds of these centers on their way to long prison sentences or internment in a growing network of massive reeducation camps that Chinese state media has described as "transformation through education" (Ch: *jiaoyu zhuanhua peixun*) facilities. These fortified "smart" camps center on training Uyghurs and Kazakhs to disavow their Islamic identity and embrace secular allegiance to the state in China (Zhu 2017). They forbid the use of the Turkic language and instead offer coercive instruction in Mandarin, which is now referred to as "the national language" (Ch: *guoyu*) instead of "the language of the Han" (Ch: *hanyu*) (Smith Finley 2019). These goals are enforced and facilitated by technology. Much of the training is delivered via TV monitors in cells and classrooms. The cells where detainees are held are monitored by cameras and sound-recording equipment, which prevents the use of the Uyghur language and other forms of autonomy. Sleeping at the wrong time, getting up from small plastic stools without permission, not participating in language study, or speaking Uyghur is often met with spoken commands from the speaker system mounted on the walls of the cell. If a detainee wants to make a request, the detainee must speak into an intercom and camera mounted on a wall.

Alim was relatively lucky: he had been let out of the detention center after only two weeks. He later learned that a relative had intervened in his case, which was why he was not sent on to a camp. But what he did not know until police contractors arrested him at the mall was that he had been placed on a blacklist maintained by the Integrated Joint Operations Platform (IJOP, or *yiti hua lianhe zuozhan pingtai*), a regional data system that collects data from tens of thousands of checkpoints throughout the region. Attempts to enter public institutions such as hospitals, banks, parks, or shopping centers, or to cross beyond the checkpoints of the dozen city blocks that were under the jurisdiction of the contractors in his section of the "urban grid" (Ch: *gexian*), could register as a "micro-clue" (Ch: *wei xiansuo*) of deviant behavior. The system had profiled him and predicted that he was a potential terrorist. The contractors told Alim he should "just stay at home" if he wanted to avoid detention again. Although

he was officially free, his biometrics and his digital history were being used to bind him in place. "I'm so angry and afraid at the same time," he told me.

Alim and nearly fifteen million other Muslims in the region were confronted by a system of overlapping enclosures. The enclosure system was premised on forms of devaluation that shaped the programmatic language of the system. It mobilized digital information drawn from ubiquitous digital interactivity and surveillance in the built environment. Taken together, this system produced a "digital enclosure" (Andrejevic 2007) of minoritized people that controlled their daily activity both inside and outside of the camp and prison system. To a certain extent, this model of enclosure resembles models of carceral urbanism and banishment of ethno-racial minorities around the world. What makes the case in Northwest China unique, beyond its shear scale, is that the digital enclosure of Uyghur and Kazakh space also harnesses state power and private textile manufacturers to hold Muslims in place in factories—producing a permanent underclass of ethno-racial minority industrial workers. Rather than banishing populations to human warehousing spaces such as peripheral ghettos or prisons, in this context terror capitalism works to explicitly reeducate the population as industrial workers and implement a forced labor regime. In this version of digital enclosure, state authorities and Chinese corporations want not just Turkic Muslim natural resources and the biometric data of their bodies; they want their disciplined, laboring bodies as well.

This chapter uses the conceptual framing of a digital enclosure to consider the way Turkic Muslim society has been enveloped by a surveillance system. This allows me to consider the way novel enclosures are produced and, in turn, construct frontiers in capital accumulation and state power.[3] This system began with the construction of 3G cellular wireless networks that produced expanding digital overlays which endowed the Turkic Muslim world with interactive capabilities across time and space. As Mark Andrejevic notes, "Such networks might be described as physical enclosures to the extent that they define a particular space and are able to both provide functionality and gather information within the confines of the geographically delimited area they cover" (Andrejevic 2007, 300). Yet, importantly, the system is not exclusive to the pinging tower of a cellular network. Instead, as GPS tracking capacity is built into smartphones and automated biometric systems begin to assess patterns of movement, digital enclosures become multidimensional. They become a complex matrix of overlaid enclosures with a wide range of spatial scales and information analytics. Only very long sentences with multiple clauses can show how the system enveloped and enclosed Turkic Muslim society: China Mobile cellular networks overlapped Huawei Wi-Fi networks; the

social network of Tencent WeChat groups could be compared with keyword assessments of QQ email; GPS movement analysis of Baidu mapping systems combined with the jurisdictional boundary checkpoint face scans, ID checks, MAC address identification of China Electronic Technology Company data doors, and the real-time license and face tracking of Sensetime-enabled camera systems, the Yitu pattern analysis of video streams collected from across the network made individual locations searchable in real time ("China's Algorithms" 2019; Byler 2020a). These passive interactive surveillance systems were supplemented by forcible data collection through Meiya Pico and Fiberhome plug-in automated assessments of smartphone software and content history by police contractors; metal detector manual scans for unauthorized electronic devices in Turkic Muslim homes; and biographical assessments that drew on banking histories, medical histories, and household registration data. Taken together, all of these various forms of information produced a digital enclosure of unprecedented scale and depth.

This chapter directs a conceptual framing of "original accumulation" (Marx [1846] 1978; Byrd et al. 2018) as seen in "digital enclosures" toward an analysis of colonial-capitalist frontier making.[4] In doing so, it turns a frame that has been used primarily to understand majoritarian consumerist populations in European and American contexts, to their effects among minoritized populations in China. It shows how this capitalist conversion device produced a regime of truth with which to transform the existing social order. In what follows, I first define digital enclosures as an ongoing process of original accumulation, then describe the way the digital enclosure developed over time in the Uyghur region before turning to ethnographic accounts of its implementation and effects. Ultimately, I argue that digital enclosures have shaped the conditions of Turkic Muslim social life, opening them up to an unfree labor regime.

Enclosure as Process

Land enclosure is central to the history of capitalism because it marks a shift to expropriation of land and labor from marginalized, often Indigenous or ethnoracialized, populations, through the imposition of a new contract-based legal regime of property possession and wage labor. In a classical Marxist account, this is described as an enforced separation of laborers from their land and autonomous subsistence and thus a removal from the "means of production" (Marx [1846] 1978). This process of "original accumulation" is something Marx described as a threshold moment in the history of European and American capitalism. Yet, as numerous other scholars have noted (Robinson 1983; D. Harvey

2005; Fraser and Jaeggi 2018), this process must be regarded as a continuously expanding frontier. Original accumulation did not stop with bounded historical moments at the beginning of colonization. Instead, expropriation of land and labor, outside of freely agreed-upon contracts, is a continuing feature of capitalism itself. As an institutionalized social order it continues to expand through the dispossession of ethno-racial others in order to reproduce this order (D. Harvey 2005; Fraser and Jaeggi 2018). In fact, though differently expressed in various historical moments and situations, colonialism is always a feature of the capitalist social order (Coulthard 2014; Byrd et al. 2018). This means that minoritized people, their way of life, and their ancestral lands are continually and more fully enclosed in service to resource extraction and new labor regimes (Robinson 1983). In order for this to happen, minoritized people must either be removed or immobilized, making their land and labor available to be claimed and regulated. With their land placed in service to natural resource extraction, industrial farming, real estate speculation, and other modes of privatization, such laborers are made dependent on the wage labor market. In this way, enclosure produces frontiers of capitalist accumulation.

Importantly, land enclosure is but one example of the more general form of "original accumulation," understood as an accumulation of claims over existing forms of life and material that previously have not been put to work in the expansion of capital and empire (Andrejevic 2007; Byrd et al. 2018). This process of expropriation can move into any domain seen as potentially productive. A speculative gaze produces forms of separation from the means to autonomous social life in the domains it encloses. It seeks to normalize this separation through legal regimes, state authority, or opaque surveillance and prediction systems, which are structured on economic growth. One of the integral achievements of capitalist systems has been the ability of those who benefit from the system to normalize enclosures and the distribution of property, knowledge, and power that is created by it (Andrejevic 2007, 303). The same can be said of the ethos of enclosure in the emerging terror-capitalist economy in Northwest China. The harvesting of Turkic Muslim social networks and biometrics in service to a counterterrorism surveillance economy places state contractors and police in control of the means of their social interaction, individual information, and, ultimately, economic productivity and social reproduction.

Terror capitalism mobilizes a process of digital enclosure in the service of capitalist-colonial expropriation. The arrival of digital surveillance extends the logic of the prison, workhouse, and factory "to encompass spaces of leisure, consumption, domesticity, and perhaps all of these together" (Andrejevic

2007, 301). For populations that are undesired, and underemployed—primarily Black and Brown people in European and North American contexts—the digital enclosure results in a process of digitizing and punishing bodies coded as deviant (Fassin 2013; Roy 2019; Jefferson 2020). This process, described by Ananya Roy (2019) as "racial banishment," simultaneously produces a "possessive investment" in valued, economically productive populations whose lives are deemed deserving of state protections (Lipsitz 1998, quoted in Roy 2019, 228). Continuing, Roy writes: "Banishment as exile is dispossession and in turn such dispossession secures sovereign possession" (2019, 228). Systems of ethno-racial supremacy inherent in capitalist-colonial frontier making rely on legal protections to secure possession of protected populations and expropriation from those who are devalued. These forms of entitlement and banishment produce colonial dispossession, which in turn produces openings for expropriation and capital expansion.

In the context of Chinese terror capitalism, the "second enclosure" movement of digital expropriation—defined by James Boyle as an "enclosure of the intangible commons of the mind" (2003, 37)—produces a systemic extraction of social data from minoritized "bad Muslim" populations who have been deemed outside of civil rights protections. State capital is used to mobilize an army of police contractors who act as low-level data technicians in service to the data-harvesting mission of private companies. Up to this point, the model of enclosure resembles models of carceral urbanism and banishment of ethno-racial minorities—described by Roy (2019) and Jefferson (2020)—around the world. What makes the case in Northwest China unique is that, there, the enclosure produces an unfree proletarianization of Muslim populations and at the same time institutionalizes a new social order.

The digital enclosure intensified the goals of biopolitical security that center around assuring the movement of goods, services, and biometric data while blocking the movement of objects, bodies, and data that could disrupt this circulation. Using the example of a seventeenth-century town in France, Foucault (2007) argues that biopolitical security attempts to increase the circulation of what is deemed "good" within a market economy while decreasing the circulation of that which is deemed "bad," such as disease, crime, and unassimilable bodies. The shaping power of this technology is used to regulate the population in hopes of producing lower rates of fear, higher rates of economic growth, and greater power among the protected population. From the perspective of those in control of the apparatus, security is a positive project that emphasizes protection of essential life processes rather than a negative

process of excluding objects and expropriating the labor of people deemed undeserving of civil rights.

In the Chinese context, leading technology companies have been mandated by state capital to control the social environment while at the same time achieving global advantage in particular domains of technological and economic development. Most importantly though, their task is to build a social management surveillance system with no blank spots. They are to move from being able to visualize the haze of the world to being able to "truly see" (Ch: *xueliang*) and "clear" (Ch: *qinglang*) the social world. That is, they are to scale-up their ability to recognize the patterns of the social world by increasing image fidelity and deep learning capacity (Yi Ou Intelligence 2017). As in Brian Larkin's framing of related systems (2008), unintelligible noise must become decoded signals. Taken together, the mandates of state capital, the rapid prototyping and development of techno-political systems, and a subject Muslim population in China produce terror capitalism as an expropriation of minoritized Muslim social life through the conversion devices of a private technology industry.

The Uyghur Digital World

The Uyghur digital world has not always been experienced only as a space of enclosure. When I began my first year of fieldwork in 2011, the region had just been wired with 3G networks and social media was just beginning to be used in urban locations. When I returned for a second year in 2014, it seemed as though nearly all adults had smartphones. Based on figures associated with Uyghur-language app downloads, approximately 45 percent of the Uyghur population of twelve million were using smartphones (Byler 2016). Many had begun to use the app WeChat to share recorded oral speech and video on a daily basis to connect with friends and family in rural villages. They also used their phones to buy and sell products, read about what was happening in the world, and network with Uyghurs throughout the country and around the globe.

Social media allowed young Uyghur migrants to develop a sophisticated urban persona within tightknit yet dispersed social networks and begin to influence the world around them through forms of mass circulation. "I liked WeChat a lot," a young Uyghur named Mahmud told me, "You could see the 'moments' of other people and you could chat as a group. You could send videos, or have a video call with anyone you wanted wherever they were, as long as they were also on the internet." Mahmud, whose story of dispossession I tell in chapter 3, began to spend as much as 200 yuan ($30) per month on his

LG smartphone data plan—much more than he spent on food or clothes. Like many young Uyghurs, he came to view WeChat as an indispensable part of his social role in the Uyghur world. It also allowed for forms of media virality and audience impact. Uyghur filmmakers could now share short films and music videos instantly with hundreds of thousands of followers. Overnight, Uyghur English teachers such as Kasim Abdurehim and pop stars such as Ablajan, non-state-sponsored cultural figures who were subsequently labeled "untrustworthy," developed followings that numbered in the millions.

Most unsettlingly, from the perspective of the state, unsanctioned Uyghur religious teachers based in China and Turkey developed a deep influence. Islamic faith and the Uyghur language have always been seen by state authorities, and some Han settlers, as sources of civilizational "backwardness" and resistance to Chinese cultural norms since the modern Chinese colonization of the region began in the nineteenth and twentieth centuries (Schluessel 2020). Indeed, land-based traditions, Islamic faith, and modernist Turkic identity formed the basis of the independent East Turkestan republics that predated the founding of the People's Republic of China and the decades of settler colonization that followed (Thum 2014; Brophy 2016). These three elements, combined with a deep-seated attachment to the built environment of Uyghur civilization—courtyard houses, mosque communities, and Sufi shrines—produced knowledge systems that resulted in Uyghur forms of distinction and difference from the Han population that had arrived in waves since 1949. They had always been Muslim but, because of the way the state in China had limited their access to Islamic knowledge and other Muslim communities, many young Uyghurs had little opportunity to actively explore this side of their history and knowledge system. There were virtually no Islamic schools outside of state control, no permitted imams who were not approved by the state. Children under the age of eighteen were forbidden to enter the mosque. Even lyrical oral epics, known as *dastans*, that told Uyghur origin stories were increasingly regulated by the state (A. Anderson and Byler 2019).

Social media opened up a virtual public–private space to explore what it meant to embody a Native and Muslim contemporaneity (Harris and Isa 2019). It confirmed that the first sources of their identity had always been their faith, their claim to a "Native" (Uy: *yerlik*) way of life, the closest English approximation of the way Uyghurs commonly refer to themselves. Social media gave Uyghurs a way of developing their sociality in both economistic and non-economistic ways. Seemingly overnight, it became common for migrants to the city to advertise their commodities on WeChat, in other internet forums,

or in markets and stores. In 2014, as I was walking through street bazaars, I often saw hand-stenciled signs advertising honey, cooking oil, rice, wheat, and other commodities with the inscription YERLIK. By advertising their goods as yerlik, or "of the land," they intended to signify several things. First, they were conveying a sense of authenticity, that the commodities were made by hand, building on traditions that had been carried forward by generations of craftspeople. Second, they were making a claim to belonging and building the future of a particular Native community and sacred landscape. Yerlik medicine, for instance, was often associated with particular locations in Khotan Prefecture, a region on the border with Pakistan that was famous for medicine. The Uyghur homeland is immense, covering a land area equal to California, Arizona, New Mexico, Utah, and Nevada combined, so there is a good deal of variation within Native identifications. Third, yerlik goods were also a way of staking a position within a larger imagined community of Uyghurs and the global Muslim community. Yerlik commodities were by definition halal and had the added benefit of strengthening the economy and social reproduction of the contemporary Uyghur nationality.

Through their exposure to the outside world and the efflorescence of online culture, millions of Uyghurs felt called to think in new ways about the piety of their Islamic practice and the future of Native traditions while at the same time they learned about self-help strategies, entrepreneurship, and new music styles. They began to imagine escaping an oppressive policing and economic system that restricted many of their basic freedoms, by banning the open discussion and practice of Islam and Uyghur history, restricting access to passports, and openly promoting systematic job discrimination and land seizures. Social media allowed them to realize that they were part of the global Islamic world and the broader Turkic community. As practitioners of Sunni Islam inflected by Sufi traditions and speakers of Uyghur, a Turkic language, they began to appreciate alternative modernities, fully formed Turkic and Islamic societies with rich histories of culture and aesthetics, where they were seen as full members. These alternative contemporaneities could stand in opposition to the modernity that centered on reified forms of Han cultural values that the Chinese policing and economic system was forcing on them. Rather than being seen as perpetually lacking Han cultural fluency and appearance, these systems of value allowed them to be seen as cosmopolitan and contemporary. They could embrace the halal standards of the Muslim world, wear the latest styles from Istanbul, and keep Chinese society at arm's length. Imported food, movies, music, and clothing from Turkey and Dubai became markers of distinction.

Women began to veil themselves. Men began to pray five times per day. They stopped drinking and smoking. Some began to view music, dancing, and state TV as influences to be avoided.

The Han officials I met during my fieldwork in 2015 referred to this rise in religious piety and ethnic pride as the "Talibanization" of the Uyghur population. Along with Han settlers, they felt increasingly unsafe traveling to the region's Uyghur-majority areas or encountering pious Turkic Muslims. They cited the first alleged Uyghur-led act of political violence that was reported outside of the Uyghur region in October 2014, when a family of three Uyghurs drove a truck into a crowd in Beijing's Tiananmen Square, killing themselves, two civilians, and injuring 42 others. They followed this with graphic descriptions of a horrific knife attack in the railway station of Kunming, in which a group of Uyghur young people killed 31 civilians and injured over 140 more. Then, a suicide bombing in Ürümchi in April 2014 left three Uyghur perpetrators dead and 79 civilians injured. Another attack occurred one month later, when two Uyghurs used SUVs armed with improvised explosives to kill 43 civilians and wound more than 90. The officials cited these incidents and other localized protests and conflicts with police and Han civilians, as a sign that the entire Uyghur population was falling under the sway of terrorist ideologies that they correlated with religious piety and ethnic pride.

The Rise of the Digital Enclosure

In fact, the beginnings of the enclosure, and the turn to religious piety it precipitated, began as early as 2009. In the summer of that year, Uyghur university and high school students took to the streets of Ürümchi demanding justice as Uyghur-Chinese citizens for the mob-instigated lynching of two migrant Uyghur workers and the wounding of sixty more who had been sent to a factory in Southern China. The way this incident of perceived sexual harassment was able to escalate so quickly remains a mystery. Perhaps the Han migrant workers felt disadvantaged due to the government aid the Uyghur workers had received in getting jobs at the factory. Perhaps there were other racially charged incidents that led up to this violence. As Huang Cuilian, the "Han girl" whose alleged harassment triggered the violence put it, "I was lost and entered the wrong dormitory and screamed when I saw those Uyghur young men in the room. . . . I just felt they were unfriendly so I turned and ran."[5] She then recalled how one of them stood up and stamped his feet as if to chase her, "I later realized that he was just making fun of me."

In response, Uyghur high school and college students used Facebook, Renren, and Uyghur-language blog sites in urban internet cafés to organize a protest demanding justice for Uyghur workers who were killed by Han workers in the lynching. Videos of the mob killing featured jeering crowds urging the Han workers to kill the Uyghurs. In order to demand state protection from such lynchings, Uyghurs marched through the streets waving Chinese flags and demanding that the government respond to the deaths of their Uyghur comrades. The protestors were violently confronted by armed police. Thousands of Uyghurs responded, turning over buses and beating Han passersby. In the end, over 190 people were reported killed, more than two-thirds of them were Han. During the weeks that followed, hundreds, perhaps thousands, of young Uyghurs were disappeared by the police ("Enforced Disappearances" 2019). In response to the incident, the internet was shut down in the region for over nine months.

Over time, state authorities realized that, as powerful as the rise of Uyghur social media was in organizing social life, it also presented them with a new means of control. Soon after the internet came back online in 2010—now with the notable absence of Facebook, Twitter, and other non-Chinese social media applications—state security, research institutes, and private industry collaborations began a series of projects to break Uyghur internet autonomy. One of the most troubling aspects of the internet regime, from the perspective of state authorities and the technologists they funded, was the audio and image sharing function of the new Chinese app WeChat. Since WeChat allows for oral speech to be recorded and images of text to be uploaded and rapidly circulated through social networks, up until 2014 Uyghurs had used this virtual social space as a semiautonomous public sphere in which to discuss Islam and politics—something that deeply worried state authorities.

In response to these concerns, state authorities mandated a counterterrorism project that offered many private companies a novel space to rapidly prototype predictive policing tools and experiment with biometric surveillance systems. For instance, the AI Champion iFLYTEK developed tools to automate the transcription and translation of Uyghur-language audio into Chinese where it could then be analyzed for precriminal and criminal content (Li and Cadell 2018). The computer-vision analytics company Sensetime worked on a joint venture with a subsidiary called Sensenets to track the movements and behaviors of over 2.5 million inhabitants of the Uyghur region using face surveillance technologies (Cimpanau 2018). A rival computer-vision company, Megvii, developed tools to support surveillance-video analytics ("Niaokan" 2017), while another computer-vision company Yitu, using a project called

Dragonfly Eye, drew on a dataset of over 1.5 billion faces to automate the detection of Uyghur faces.[6] Another AI Champion HikVision, a market-oriented subsidiary of the SOE military supplier China Electronics Technology Company, received nearly $300 million in Private Public Partnership contracts to develop "Safe City" surveillance systems with "zero blank spaces" throughout Uyghur-majority areas, from mosques to the interiors of reeducation camps (Rollet 2018).

As the leaders of these firms noted,[7] in a post-9/11 world Chinese tech firms are not alone in using surveillance technology to automate policing of populations deemed dangerous. However, because of the state capital they were given and the mandate that came with it, firms in Xinjiang have tremendous latitude to experiment with these technologies without fear of legal or civil resistance. China's counterterrorism and cybersecurity laws obligate Chinese social media and technology companies to provide policing agencies with complete access to user data and to host internal Communist Party committees who provide company oversight. As Ryan et al. (2019) have shown, technology companies have one of the highest proportions of such committees in the private sector. Furthermore, the widespread private contracting of public services throughout the Chinese economy has produced a market structure in the technology sector in which the majority of profits and company growth come not from consumer products and services, as in the current Western contexts described by Zuboff (2019), but from state-driven techno-political projects that assure the productivity of social bodies. While many European and North American technology firms have their origin in a post-WWII military-industrial complex, in the post-Cold War context most firms are now privatized and, in fact, in some ways beyond the full control of the state (Masco 2014; Jefferson 2020). This is less the case in China where state-managed technology companies are increasingly placed in service to state power. In 2016 approximately $52 billion of the security technology market in China was structured around state-managed projects, while $32 billion came from security products and $6.8 billion came from alarm systems (Yi Ou Intelligence 2017). As the scholars Martin Beraja, David Y. Yang, and Noam Yuchtman have shown through a large-scale study of private technologies used in public policing in China (2020), state capital investment in data-intensive technologies is essential for the success of these private computer-vision companies. They show that public policing systems, particularly in Xinjiang, generate far more data than similar systems in closed or private environments. This is precisely why Chinese AI Champions have been able to surpass many firms based in Europe and North America

when it comes to facial recognition technologies. In their work, Beraja, Yang, and Yuchtman (2020) demonstrate a causal effect of access to more government data on new commercial software production and, in turn, the economic effects of this market structure. Ultimately, they show that the Chinese technology industry is shaped via state capital used in surveillance projects.

In effect, Ürümchi and the rest of the Uyghur homeland have become an experimental space for the Chinese techno-security industry and the authoritarian statecraft it supports. In 2016 and 2017, the state invested an estimated $7.2 billion specifically in the Xinjiang information security industry as part of an increase of public security spending of over 90 percent.[8] Over those same years the state awarded an estimated $65 billion in private contracts to build infrastructure and $160 billion more to government entities in the region—an increase of nearly 50 percent. The majority of this increase in construction spending was centered on the building of detention facilities and related systems.[9] As a report from the leading Chinese tech journal *Leiphone* noted in 2017, "The current security industry in Xinjiang is positioned exactly right in terms of market opportunity."[10] As a spokesperson for the Xinjiang policing company called Leon Technology put it, 60 percent of the world's Muslim-majority nations are part of China's premier international development project, the Belt and Road Initiative, so there is "unlimited market potential" for the type of population-control technology they are developing in Xinjiang.[11] The People's War on Terror offered an opportunity to experiment with and develop computer-aided policing and computer-vision and sound recognition.

As part of this techno-political and economic development, broadly defined antiterrorism laws were introduced by Chinese authorities, turning nearly all Uyghur crimes—from stealing a Han neighbor's sheep to protesting land seizures—into forms of terrorism and conflating religious piety, which the new laws referred to as "extremism," with religious violence (Bovingdon 2010; Roberts 2020). As the laws were implemented, the Xinjiang security industry mushroomed from a handful of private companies to over one thousand companies that utilized hundreds of thousands of workers ranging from low-level Uyghur security guards, to Han camera and telecommunications technicians, to coders and designers, to intelligence workers.[12] Drawing directly on lessons learned in the war in Iraq and the role of Silicon Valley companies in monitoring Muslim populations as part of US Countering Violent Extremism programs, local Chinese authorities in the Uyghur region began outsourcing their policing responsibilities to private and state-owned technology companies in order to enhance their surveillance capacities (Byler 2020a). For example, Alibaba and

iFLYTEK, two of the most powerful companies in China, took on new roles in countering the threat of Turkic Muslim violence through assessments of calls, traffic, shopping, dating, email, chat records, videos, language, and voiceprint detection (Xinhua 2014). The Uyghur region led the country in contracts given to private technology firms to develop surveillance and analytics tools as part of Safe City projects that supported the system of Turkic Muslim reeducation (Essence Securities 2017). As these infrastructures were designed and implemented, signs of Islamic behavior ranging from wearing a beard or veil to one's internet activity became evidence of latent insurgent tendencies. An ethnoracialized Islamophobia was institutionalized through the digital enclosure.

In a prelude of what was to come as the political and economic system gained momentum, state authorities worked with technology firms to introduce a passbook system that forced hundreds of thousands of rural-origin Uyghur migrants to return to their villages. This digitized instantiation of ethno-racial banishment (Roy 2019) or urban cleansing (Appadurai 2000), used a new card system, referred to as a People's Convenience Card (Ch: *bianminka*). It required Uyghur migrants to petition local police for what they referred to as a "green card." This card, which was equipped with a QR code, allowed police officers to scan and pull up the personal data of the individual during spot checks. Based on informant interviews with both migrants and state police, only around 10 percent of approximately 300 thousand Uyghurs who were living in Ürümchi at that time were able to obtain the card. Without it they were not permitted to travel beyond the checkpoints of their home counties. According to a report published by a government official in 2013, the total number of around 412,000 internal Muslim migrants in Xinjiang needed to be "transformed" (Ch: *zhuanbian*) through compulsory legal education and training (Wu 2013).[13] The Uyghur countryside became what many referred to as an "open air" prison. As one aspect of this "transformation" approach, state authorities detained thousands of the most pious Uyghurs among both returning migrant populations and populations already in rural areas, and sent them to newly established reeducation camps. They also dispatched hundreds of thousands of police and government officials to monitor the families of those who had been taken and conducted regular inspections of homes looking for signs of religiosity (Byler 2018b).

In 2017 state authorities and technology companies intensified this strategy. Rather than doubling down simply on security, banishment, and selective detention—what was referred to as a "hard strike" (Ch: *yanda*) policy—a new regional party secretary named Chen Quanguo mainstreamed the approach of "reeducating" (Ch: *zai jiaoyu*) the hearts and minds of Uyghurs. As Chinese

policing theory documents show (Byler 2019), this approach drew in part on a version of what the US general David Petraeus (Petraeus, Amos, and McClure 2009) described as "winning the hearts and minds" of those whose society had been destroyed. This transformation was to be achieved by detaining untrustworthy segments of the population and training them in Chinese and political ideology while simultaneously forcibly assigning the remaining population to low-wage factory jobs. In an ethno-racialized and colonial form of "repressive assistance" used elsewhere in China (Pan 2020), these "de-extremification" (Ch: *qu jiduanhua*) efforts and "poverty alleviation" (Ch: *fupin*) projects attempted to enclose the population, eliminating unwanted religious and cultural elements in their social life. At the same time, the system introduced forms of dependency by forcing many Uyghurs to either sign work contracts or face camp internment. In Petraeus's infamous field manual, counterinsurgency is framed as a primarily political transformation, or regime change, that accompanies full-spectrum intelligence and systematic detentions, and, at times, assassinations. For Chen, the Petraeus project was made significantly easier by the fact that there was no statistically significant armed insurgency among the supposed insurgents, Uyghurs, and he had a standing reserve of millions of Han settlers and Uyghurs that state and corporate proxies could mobilize as intelligence workers and reeducators.

Importantly, Chinese state authorities and policing theorists imagined that counterinsurgency could be taken much farther in this context (Brophy 2019; Byler 2019). It could produce not just a change in political loyalty but an epistemic transformation of Uyghur sociality itself. State authorities and contractors continually referred to Uyghurs as "separatists, extremists, terrorists," and demanded that state workers and community members provide "enemy intelligence" (Ch: *diren qingbao*) about the Uyghurs they encountered. Yet, unlike the US War on Terror, in China the enemy had no weapons, they had no formal organization, and they had little international support. In large part Uyghurs were the enemy simply because of their unassimilable difference—their allegiance to Islam, their attachment to land-based Turkic identifications, the otherness of their physiognomy—and the fear all of this inspired.

In Xinjiang, the officials used public health euphemisms to attempt to accomplish their transformational purposes. Local authorities began to describe separatism, extremism, and terrorism as three interrelated ideological diseases in need of a cure (Roberts 2018). In order to detect the spread of the disease and excise the cancerous cells, they said they needed surgical precision (Grose 2019). Because the viral spread of Turkic Islam was so deep and entrenched, they realized they needed a system of purpose-built digital en-

closures to detect the growth of Uyghur Islam and political identity and diagnose the needed level of treatment, which ranged from imprisonment to reeducation. Rather than just monitoring and preventing potential terrorism, authorities attempted to transform Uyghurs themselves by cutting out what government workers have referred to as the "tumors" of "untrustworthy" (Ch: *bu fangxin*) elements through a process of retraining and reeducation.[14]

This turn toward transformation coincided with the rise of Chinese technology breakthroughs in AI-assisted computer vision systems. Drawing on state-supported research, the Chinese startup company Meiya Pico began to market programs and equipment that could detect Uyghur-language text and Islamic symbols embedded in images to local and regional governments. They also developed programs to automate the transcription and translation of Uyghur voice messaging. Other companies—such as Dahua, Hikvision, Yitu, Sensetime, and Cloudwalk—advertised software programs and equipment to government and security firms that attempted to automate the identification of Uyghur faces based on physiological phenotypes. The AI-assisted technology that was introduced in 2017 aimed to both intensify the digital enclosure system and free up security labor for other tasks: the work of transformation. According to a Leon Technology spokesperson, such AI systems would, "on the scale of seconds," automatically flag suspicious behavior such as illegal Islamic dress or individuals who were on special surveillance watchlists.[15] These systems allowed searches of Uyghur internet histories looking for flagged materials such as the word *Allah*, images of someone praying, or messages sent to someone who had a family member living abroad. They matched this personal behavior data to banking and school records, job histories, medical histories, and family planning histories, looking for predictors of aberrant behavior that ranged from having too many children, to leaving one's house through the back door ("China's Algorithms" 2019). It looked for unusual patterns in electricity usage, or driving a car registered to someone else. The platform fed on personal behavior and archives of individual lives, turning them into biometric data and digital code, in order to continue to learn the patterns and variations of Uyghur life and become more robust as a universal security system that operated at the level of the social life of an entire population.

Police Contractors as "Data Janitors"

As the ethnographer Lilly Irani (2015, 2019) has noted, cutting-edge technology systems everywhere in the world are nearly always trained by low-wage technicians. In European and North American contexts, much of this work is done

through platforms like the Amazon-hosted contractor network Mechanical Turk. Many of these "data janitors," as Irani refers to them, are tasked with training AI algorithms to recognize and digitize material objects, behaviors, and people. Often they are forced by class, race, gender devaluation, and citizenship status into these jobs (Amrute 2016). Once in these positions it is often difficult to opt out or demand better work conditions. As anthropologists of policing and prisons in Western contexts have shown (Rhodes 2004; Fassin 2013), the same holds true for low-level prison and policing work. Often those who enforce state violence come from ethno-racial minority and lower-class positions. They are in fact placed in service to what Chandan Reddy (2011) describes as practices of subjectification, or subject making, in which ethno-racially heterogeneous workers are mobilized through processes of disidentification with their own interests to build new frontiers of capital accumulation and state power. In Northwest China, Turkic Muslim young men, the most deeply vulnerable population in the reeducation project, are coerced through economic and policing pressure into "freely" contracting with surveillance system employers who enact the general enclosure system over their own societies.

The integration of these various platforms was serviced by the state-owned Fortune Global 500 company China Electronics Technology Group with support from many leading Chinese tech firms. Building the dataset and setting its parameters required a great deal of labor and technical training ("China's Algorithms" 2019). Nearly ninety thousand police contractors and other state workers were hired (Greitens et al. 2019). The lowest-level police contractors (Ch: *xiejing*), who were hired primarily from Muslim minority populations themselves, worked to perform spot checks, which centered on actively profiling passersby, stopping Turkic young people and demanding that they provide their state-issued ID and open their phone for automated inspection via spyware apps and external scanning devices (Byler 2020b). Policing contractors were also responsible for monitoring face scanners and metal detectors at fixed checkpoints. Turkic Muslims were required to carry a smartphone if they had registered a SIM card in the past. At checkpoints the phone was matched to the ID of the carrier, allowing systems to perform a hard reset of individual movement in real time and space multiple times per day. All these activities ensured that Uyghurs continued to build the dataset, making extremism-assessment algorithms more and more precise.

One of the police contractors who conducted these checks was a young Kazakh man named Baimurat. He was in one of the first groups of contractors who were hired from across the region. In an interview he said that because he was a college graduate he was "considered very well qualified." As a result he

was given the highest level salary available to contractors, around 6,000 yuan per month ($1,000), which is far above the minimum wage of around 1,800 yuan. Others in his cohort, who were considered less qualified because of their educational background, were paid closer to 2,500 yuan. For Baimurat, who had struggled to find work for which he was qualified in the past, taking the job was a choice he felt he could not refuse. Not only would he be able to provide for his family but he would also be able to protect them from the reeducation system. "We were given uniforms," he said. "Then we started doing different kinds of training. It was really strict, as if we were planning for a war." Around this time, he said the local authorities started building People's Convenience Police Stations, the type of surveillance hub where Alim, the young man whose story frames this chapter, was interrogated. Then the county officials who had hired them divided the contractors up and stationed them at one of the ninety-two stations that were built in the county. He said:

> Inside that station there were screens. We sat facing the screens, and you could see the places where the cameras were pointed. We had to sit there monitoring them all the time. If we failed to notice an alert or stopped looking, we would be punished. But still we thought it was a good job just sitting there.

Over time, the kind of surveillance labor they did began to shift. First, the contractors were sorted based on their Chinese-language ability and other proofs of their loyalty and knowledge of the extremism parameters of the reeducation system. Baimurat said:

> They made us do other exercises like reciting rules about participating in the camp system. We had to recite things related to law. There were quotes from Xi Jinping on the walls of the station. We had to learn these by heart. We were not allowed to go outside for the patrol until we successfully recited the quotes from Xi Jinping.

It is important to note here that, although they were ostensibly *private* security contractors, data janitors such as Baimurat were obligated to articulate themselves to Xi Jinping and the language of the state in order to carry out their work as police technicians. Interestingly, when questioned about Baimurat's role in the system, a state spokesperson described Baimurat as a security officer employed by a shopping center rather than the state police.[16] This flexible use of private-public positioning recalls the slippage described by Rofel and Yanagisako (2018) in the way the state is often inscribed in ostensibly private industries. Baimurat's contractor status meant that he could be denied state

authorization at a moment's notice. Yet, at the same time, he was not free to quit. "If we were tired and wanted to quit, they would tell us if you are exhausted you can take a rest, but then you must come back. If you quit the job, then you will end up in the 'reeducation camps' too." Interviews with another Muslim minority police contractor and the relatives of other police contractors I interviewed in the region in 2018 confirmed this policy.

Around the middle of 2017, police contractors began to actively fine-tune the programming of the system using assessment tools which scanned through files that were hidden on Muslim smartphones. Baimurat continued:

> I worked there for six months. Then they handed out devices to check pedestrians and car drivers. When we scanned their ID card (and phone) with it, we got information about whether or not the person had worn a veil, had installed Whatsapp, had traveled to Kazakhstan, all sorts of things like that. We could stop every car on the street and check them. When we stopped them, we asked the people inside to show their phones and ID cards. If there was something suspicious like I mentioned before, we needed to inform [the leaders].

Higher-level officers and "older brother and sister volunteers," most of whom were Han, were given the job of conducting qualitative assessments of the Muslim population as a whole—providing the more complex interview-based survey data for the deep-learning system of the integrated platform (Byler 2018b). Neighborhood police officers, contractors, and "relative" assistants assessed the Muslim-minority people to determine whether they should be given a rating of "trustworthy," "average," or "untrustworthy" (Smith Finley 2019). They determined this by categorizing the person using ten or more categories: whether or not the person was of military age, if they were Uyghur, if they were underemployed, if they prayed regularly, if they possessed unauthorized religious knowledge, if they had a passport, if they had traveled to one of twenty-six Muslim-majority countries, if they had overstayed their visa, if they had an immediate relative living abroad, or if they had taught their children about Islam in their home. Those who were determined to be untrustworthy were then sent to detention centers where they were interrogated, asked to confess their precrime violations such as teaching their children about Islam or fellow Uyghurs how to pray or read the Quran, and name others who were also untrustworthy. In this manner, and with the help of tech-enabled cyber-violation detections, the parameters of the techno-political system determined which individuals should be slotted for the "transformation through education" internment camps.

These assessments were an iterative process. Many Muslims who passed their first assessment were subsequently detained because someone else who had been detained had named them as untrustworthy or because automated systems or police contractors detected micro-clues of aberrant behavior. Years of WeChat history made freely available to government agencies was used as evidence of the need for Uyghur suspects to be transformed. Over one million Han and Uyghur "volunteers" were forced, through threats of demotion and prosecution, to adopt rural Uyghur and Kazakh families to conduct a series of weeklong assessments as uninvited guests in Uyghur and Kazakh homes (Byler 2018b). As a way of enforcing this "no mercy" policy, in 2017 state authorities "opened more than 12,000 investigations into party members in Xinjiang for infractions in the 'fight against separatism,' more than 20 times the figure in the previous year."[17] Over the course of these weeks, the state workers tested the trustworthiness of the Turkic Muslim population that remained outside of the camp system, by forcing them to participate in haram activities such as drinking, smoking, and dancing. As a test, they brought their Uyghur hosts food without telling them whether the meat used in the dishes was halal or not. These "big sisters and brothers" specifically targeted the families of those who had been shot or taken away by the police over the past decade. They looked for any sign of resentment or lack of enthusiasm in Chinese patriotic activities. They gave the children candy so that they would tell them the truth about what their parents thought. The qualitative data they gleaned was added to their biometric profile in the region-wide integrated database.

This data allowed intelligence workers and the surveillance system a way of tracking, reporting, and analyzing their progress in reeducation. Scanning Uyghur faces and phones for reasons to subtract them became a numbers-based calculus. The more data, the better for subtracting. For instance, in one neighborhood in Ürümchi in early 2019, the IJOP reported that, up to that point, sixty "wild imams" had been detained out of a total of 669 detainees (Byler 2021; Grauer 2021). Of these detainees, 348 were being held in interrogation centers while 184 had been sent to the camps. Over the course of one week, 1,585 people who were relatives of the "Three Category" detainees had received daily visits from intelligence workers and 326 elementary students who had a parent in detention had been monitored by their teachers. In addition, intelligence workers and police contractors reported that, over that same week, the IDs of 256 people had been manually scanned using "investigation tools" and 367 smartphones had been scanned using "counter-terrorism swords" (Byler 2020b). The result of all these investigations and micro-clues they had received from the IJOP was that four people were detained for joining

a "Qur'an Alphabet" WeChat group in 2017. Thousands of IJOP police reports from other nearby communities—which I reviewed for *The Intercept*—revealed similar week-to-week assessments in the growth and implementation of terror capitalism across the region. Throughout the system, exhortations to meet intelligence quotas were reiterated.

Caught in the Digital Enclosure

At the center to which he was sent, Alim—whose story I began in the introduction to this chapter—was deprived of sleep and food, and subjected to hours of interrogation and verbal abuse. "I was so weakened through this process that at one point during my interrogation I began to laugh hysterically," he said when we spoke. Other detainees report being placed in stress positions, tortured with electric shocks, and submitted to long periods of isolation. When he wasn't being interrogated, Alim was kept in a fourteen-square-meter cell with twenty other Uyghur men, though cells in some detention centers house more than sixty people. Former detainees have said they had to sleep in shifts because there was not enough space for everyone to stretch out at once. "They never turn out the lights," Mihrigul Tursun, a Uyghur woman who spent several months in detention, told me.

The religious and political transgressions of these detainees were frequently discovered through social media apps on their smartphones. Perhaps their contact number had been in the list of WeChat followers in another detainee's phone. Maybe they had posted, on their WeChat wall, an image of a Muslim in prayer. It could be that in years past they had sent or received recordings of Islamic teachings that matched indicators of up to 53,000 specific signs of extremism that algorithms attempted to detect (Byler 2020b). Maybe they had a relative who had moved to Turkey or another Muslim-majority country and had added them to their WeChat account using a foreign number. The mere fact of having a family member abroad, or of traveling outside China, as Alim had, often resulted in detention.

Another one of these former detainees, an ethnic Uyghur cross-border shuttle trader from Kazakhstan named Gulbahar Jelilova, said in a series of interviews that, in the cells where she was held in the capital of the Uyghur region, Ürümchi, the women ranged between the ages of fourteen and seventy-eight (Byler 2018c). While the middle-aged women in her cell, such as herself, were often said to be guilty of having their WeChat numbers listed in the phones of other detainees, the younger women were often said to be guilty of sharing images of Islamic practice or Quranic verses via social media. One

young woman told Gulbahar that she was detained because she had posted a picture of a person praying. She told her, "I just liked this picture and put it on my WeChat." A twenty-five-year-old said that her interrogators had shown her that they had found four extremist images in her WeChat account. She told Gulbahar, "I deleted them a long time ago, but somehow they restored them. They were just pictures of women in veils. In one of them a little girl is holding her hands up in prayer." Now the woman was in the detention center for her association with images that she thought she had deleted years before AI-assisted tracking of religious imagery was a possibility.

Gulbahar's own detention was connected to her digital social network and digital payment history. Sometimes simply knowing the wrong person and having an international travel history were enough to warrant an investigation. She explained:

> At 8 a.m. the police knocked on my door. They showed me their badges and then said they had a few questions to ask me. I thought they really would just ask a few questions, so I went along with them [without any attempt to resist]. As soon as we arrived at the police station they checked my phone. When they couldn't find anything, they showed me the picture of my friend and asked if I knew her. Then I realized they had already detained my friend. They found my phone number in her cell phone and pressured her daughter to call me. Then they accused me of wiring 17,000 yuan to Turkey. I said, Why would I do that? They said, take your time, think it over.

Over the next year, Gulbahar's interrogators tried many different approaches to force her to confess to a crime. She said she understood that she was only deemed guilty through inference and association, so she refused. Although the parameters of the system, recovered through both digital and human surveillance, seemed to indicate a probability of extremism, in the end, because she refused and her international connections, the enclosure lost its hold. Eventually, due to pressure placed on state authorities by her relatives in Kazakhstan, she was released.

Simply not using a smartphone and social media was also something that was flagged through assessments at checkpoints. So was attempting to destroy a SIM card, or not carrying a smartphone. In desperation, some Uyghurs buried their phones in the desert; others tied little baggies of SIM cards for phones they had used in the past high up in trees and put SD cards that had Islamic texts and teachings on them in dumplings and froze them, hoping they would not be found and that eventually they could be recovered. Others gave up on preserving Islamic

knowledge and burned data cards in secret. Simply throwing digital devices away was not an option. They might be found and traced back to the user.

Detainees were often forced to point out names of extremists listed in their phones and reveal the locations of hidden SD cards or smartphones. As in the rendition processes of the US War on Terror, the goal of this phase in the process was not so much about determining the guilt of the detainee as much as isolating individuals, fracturing all remaining forms of support, and capturing as much information as possible about the detainee's social network. Many simply disappeared, or were psychologically broken, during this phase of the process. Young men of military age were particularly susceptible to disappearance. Based on the gendered segregation in the camps themselves, it is clear that more than two-thirds of those taken were men. The enclosure that targeted Mihrigul, Gulbahar, Alim, and the many so-called terrorism suspects they met in the detention centers, removed them and Muslim contractors who enacted the system from freely chosen forms of social relations.

Digital Enclosure and Capital Accumulation

In order to understand how these surveillance technologies work as a type of digital enclosure—transcribing social life as digital code that can then be monetized by companies, it is instructive to think with Foucault regarding the general technology of biopolitical security (Foucault 2007). As I noted in the introduction, such a technology, for Foucault, is simultaneously *productive* in the way it produces new self-disciplined subjects, *symbolic* in the way it produces new regimes of truth, and *powerful* in the way it is dispersed to mediate, but not fully determine, the conduct and discipline of individuals within populations (Samimian-Darash 2016). The reeducation enclosure project attempts to produce Uyghurs who are subject, or bound, to a Chinese system of control in all aspects of their lives while simultaneously maintaining the power of Han inhabitants to move through the "green lanes" that were opened at checkpoints just for them. One of the most powerful aspects of the system is that, from the perspective of security workers, they smooth out access and make their lives more efficient. They work. The systems track Han movements as well, but in this context the tracking is experienced as largely frictionless. At most, the brief slow-down at checkpoints is experienced by non-Muslims as a hassle. Non-Muslims move through preapproved lanes, their faces acting as a code that unlocks gates, the technology extending their power and privilege as protected citizens. The overlaid and precise programming of the system combined with the profiling gaze of human surveillance technicians aimed to ensure the

smooth capture of data and the movement and security of those whose lives were valued by the system.

In the broader technology community, there is some skepticism regarding the viability of AI-assisted computer-vision technologies in China. Some experts point to an article titled "Potempkin AI" (Sadowski 2018), which highlights the failures of Chinese security technology to deliver what it promises without human assistance. They frequently bring up the way a system in Shenzhen meant to identify the faces of jaywalkers and flash them on jumbotrons next to busy intersections cannot keep up with the faces of all the jaywalkers and, as a result, the data used for public shaming is at times input manually. These experts claim that much of what looks like AI-assisted real-time policing may actually be human-assisted policing. They point out that Chinese tech firms and government agencies have hired hundreds of thousands of cheaply paid police contractors to act as "data janitors" and watch banks of video monitors (Irani 2015). Aspects of the IJOP act in quite blunt ways and are supported by the manual data imports (Leibold 2020). As with the theater of airport security in the United States, to a certain extent it is the threat of surveillance, rather than surveillance itself, that causes people to modify their behavior.

Yet, despite the role of human labor in installing and debugging the system, in general the digital enclosure worked to convert Turkic Muslim populations into parsed data streams, making them available for assessment, subtraction, and further dependency. It turned Uyghurs and Kazakhs against themselves, making them human intelligence, the translators and janitors, of a system of signals intelligence meant to transform and expropriate. Because of the ethnoracial devaluation of his social position, Baimurat felt he had no choice but to work in service to the system of enclosure even as it foreclosed other life paths for him. Furthermore, the venture capital orientation of technology development in general created marketing conditions where technology firms frequently oversold their capabilities. This was frequently combined with the "black box" effect of advanced technologies, where obfuscation of process and programming mask the errors and probabilities of algorithms, creating a smooth interface that appears endlessly precise (Albro 2018). In the Chinese context, because of the way technology firms funded by state capital act as proxies for state intervention, this overselling and black box ethos nevertheless translates into powerful forms of self-policing on the part of the surveilled.

A middle-aged Uyghur businessman from Khotan who I will call Dawut told me that this new system has turned Uyghur communities into hollowed-out worlds behind the checkpoints, the cameras, and the apps on their phones. Within the reeducation security system, everything Uyghurs do is recorded

and, through this, controlled. In this system the only kind of Uyghur life that is recognized by the state authorities and contractors is the one that the computer sees. The government officials, civil servants, and police contractors who have come to build, implement, and monitor the system do not really see them as possessing independent autonomy outside of what is permitted by the system. This makes Uyghurs like Dawut feel as though their lives only matter as data—code on a screen, numbers in camps—and they are adapting their behavior, even their thoughts, to this system as well. "Uyghurs are alive," Dawut said softly, with a sad smile. "But it is like they are ghosts living in another world." Although the enclosure system does not fully determine or control their lives, it does eat into the basic forms of social care that constitute Uyghur land-based social life. Systems of devaluation and dispossession have been codified and extended through the digital enclosure.

On November 3, 2018, Erzhan Qurban, a middle-aged Kazakh man from a small village fifty kilometers from the city of Ghulja near the Xinjiang border with Kazakhstan, was released from the reeducation camp after nine months. He had been held without charge as a precriminal who had exhibited signs of religious extremism. Speaking in 2019, Erzhan said he still does not know why he was taken.[18] Like others detained in Ghulja, the micro-clues of his preterrorism were likely the fact that he possessed a passport and had traveled to Kazakhstan, one of twenty-six Muslim-majority countries on a Chinese state watch list (see "China's Algorithms" 2019). He thought that perhaps now he would be free to return to his former life as an immigrant in Kazakhstan. Yet, later that week, he was sent to work in a glove factory in an industrial park back in Ghulja city. For the next fifty-three days, he experienced life in a reeducation garment factory that was built to "raise the quality" (Ch: *tigao suzhi*) of Turkic Muslim-minority forced laborers.

Erzhan had been detained soon after he came back to China to seek medical treatment for his daughter and care for his ailing mother in early 2018. In a 2019 interview with the German newspaper *Die Zeit*, he said:

> On the evening of February 8, 2018, they picked me up in a minibus. It was already dark and they put black plastic sacks over our heads and handcuffs on our hands. There were five young men from my village with me in the minibus. The room in which I had to stay for the next nine months was 5 meters by 5 meters and located on the third floor. On the door, a sign said "No. 12." Our floor alone accommodated 260 men. In my room, we were twelve. Later I heard that there had been more than 10,000 men detained in our camp.[19]

Erzhan was unsure exactly where the camp was located. It may have been the one that was built in the fields on the outskirts of the city, just seven kilometers from the industrial park. As has often been reported by former detainees, conditions in the camp where appalling. Describing the circumstances of his detention, Erzhan said:

> The toilet was a bucket by the window, there was no running water. In the daytime, we were sitting in rows on our plastic stools. The food was handed to us through an opening in the door. At 7 a.m., we had to sing the Chinese national anthem and then we had three minutes for breakfast. Afterward, we studied Chinese until 9 p.m. Our teachers were Kazakhs or Uyghurs. We were watched by four cameras in our room which ensured that we didn't talk to each other. Those who spoke anyway were handcuffed and had to stand by the wall. "You don't have the right to talk, because you are not humans," said the guards, "If you were humans, you wouldn't be here."[20]

Over time the grueling routine began to change his mental state. He said: "The first two months, I thought of my wife Maynur and my three children. Sometime later, I only thought about food."[21]

In May 2018, about the time that Erzhan began to detach from his social relations and think about his bodily survival, Pan Daojin, the front commander and party secretary of Yili Prefecture, arrived to inspect a newly built industrial park on the other side of town.[22] He came with an "Aid Xinjiang" delegation from Jiangsu that was tasked with providing jobs to reeducated workers. Pan, who was also from Jiangsu, had been appointed to his position in December 2016 just as the mass detentions of the reeducation system began. During the inspection of the new industrial park, he "fully affirmed the achievements" of the business leaders from Nantong City in Jiangsu who had funded the industrial park. The delegation showed off the new factory of the Jiangsu-based Solamoda Garment Group—a company that partners with Forever 21 and other international brands. They also stopped by the highly productive glove factory where Erzhan would eventually be assigned. This factory was managed by employees of the Luye Shuozidao Trading Company, a manufacturer based in Baoding city in Hebei Province.

According to the general manager of the glove factory, Wang Xinghua, speaking in a state TV interview released in December 2018, "With the support of the government, we have already 'recruited' more than 600 people" (Ili Television 2018). One of these 600 government recruits was Erzhan, who had arrived from the camp less than a month before. Continuing, General Manager Wang said

that since the founding of the new factory in 2017, "we have generated more than 6 million US dollars in sales. We plan to reach 1,000 workers by the end of this year. We plan to provide jobs to 1,500 people by the end of 2019." In fact, the glove factory in Ghulja has now far surpassed the capacity of its parent factory. Back in Hebei, the company employed less than 200 employees ("Lixian Huawei Gloves Factory" 2019). Moving manufacturing to Xinjiang made sense for the company, which sold 96 percent of its leather gloves across the border in Russia and Eastern Europe. But there were other reasons for this exponential growth. Since 2018 the state has provided subsidies to build factories and ship goods from Xinjiang. Construction of the factories was often funded by local governments in Eastern China as part of a "pairing assistance" program. Up to 4 percent of new factory sales volume was subsidized in order to cover shipping expenses from the new location.[23] A state program gave reeducation system employers five thousand yuan for each coerced worker they trained. Most importantly, as in every county in Xinjiang, there were tens of thousands of desperate, traumatized detainees like Erzhan in nearby camps. As a document from the Development and Reform Commission of Xinjiang mandates, local authorities are to "establish a development mechanism linkage between the industrial management of rural collective economic organizations and *the industry of education and training centers*"—the euphemism used for reeducation camps and associated factories (Yuan 2019; my emphasis).

Since 2017 factories have flocked to Xinjiang to take advantage of the newly built industrial parks of the reeducation camp system and the cheap labor and subsidies that accompany them. In fact, as described in the preface, in late 2018 the primary development ministry for the region circulated a statement saying that the camps or "vocational skills education and training centers" had become a "carrier" (Ch: *zaiti*) of economic stability (Xinjiang Reform and Development Commission 2018). Because of this system, Xinjiang had attracted "significant investment and construction from coast-based Chinese companies." This was particularly the case in Chinese textile and garment-related industries, since China sources more than 80 percent of its cotton in Xinjiang (Gro Intelligence 2019). In an effort motivated at least in part by rising labor costs among Han migrant workers on the east coast, by 2023 the state plans to move over one million textile and garment industry jobs to the region.[24] If they succeed, it will mean that as many as one in every eleven textile and garment industry jobs in China will be in Xinjiang ("Wages and Working Hours" 2014).

Nearly all the gloves that are made by detainees in the satellite factory of the Luye Shuozidao Trading Company are sold abroad. The company's Alibaba distribution site sells the gloves at wholesale prices ranging from $1.50 to $24.00

per pair. Some are distributed by the upscale Hong Kong–based boutique Bread n Butter, which has outlets across East Asia where they are sold for far more. In any case, the price at which these gloves are sold is more than, at a minimum, ten times higher than the wages workers are paid per pair. In an essay written in adulation of the factory complex, a Ghulja County official wrote that, when the Turkic Muslim farmers and herders arrived at the factory, they "took off their grass shoes, put on leather shoes, and became industrial workers" (Yining County Zero Distance 2018). The counterfactual imagery of "backward" (Ch: *luohou*) minority people, being given the "gift" of factory discipline through enclosure precisely captures the process of removing workers from the means of production, making them fully dependent on carceral factories.

In a video produced for state TV, a reporter repeatedly noted that the Turkic Muslim workers did not even pause to look up at the camera during the filming (Ili Television 2018). The reporter interpreted this as a sign of their excellent work ethic as newly trained "high quality" (Ch: *suzhi gao*) workers. By extracting surplus value from the reeducated workers in the form of cheaply produced commodities and skilled laborers, the factory was also investing in the value of the Turkic Muslim workers. Erzhan noted that his manager emphasized that the gloves they were making were for export so the quality of their sewing had to be very high. The training they received in "achieved quality," had to be reflected in the quality of the gloves they mass-produced.

Another Kazakh worker I interviewed in January 2020, Gulzira Auehlkhan, told me that, after her release from the camp, she was also forced by officials in her village to work in the same factory as Erzhan. At night she was held in a walled dormitory and not permitted to leave. There were checkpoints at the entrance of the dormitory and factory where her ID and face were scanned. She said, "We would have our bodies and phones checked when we arrived, in the middle of the day. When we were leaving for the dormitory at the end of the day, they would check again because they were worried we might take a needle. After we got to know them [the police contractors], we asked, 'Why are you still here watching us?'" She said she knew that the answer to this question was that they were monitoring whether or not they were acting like submissive reeducated industrial workers. This suggests that Muslims like Gulzira and Erzhan must adopt proletarian behavior and basic "achieved quality" (Ch: *suzhi*). The implied promise is that accruing such value might in turn be exchanged for positions and practices that hold greater exchange value. However, as I will show in the following chapter, this promised success is often blocked by the ethno-racial slot that bound them in the enclosure to begin with.

It appears instead that the goal of the reeducation industrial parks, and broader digital enclosure system, is to turn Kazakhs and Uyghurs into a deeply controlled proletariat, a docile yet productive unfree class—those without the social welfare afforded to the formally recognized rights-bearing working class. Another former detainee and worker named Erbaqyt Otarbai told me that in the eyes of the managers they "were like pets," trained to work on command. By turning a population of people regarded as not deserving of legal protections into productive workers, state authorities and private industrialists are simultaneously extending the market expansion of the Chinese garment industry and technology development. This system of controlled labor is "carried" forward by the reeducation system. A complex digital enclosure that held workers in place and monitored their productivity ensured that this new class of interned laborers remained a permanent ethno-racial underclass. In fact, because of this extralegal system, the only thing that protects Turkic Muslim workers from exploitation, violence, and detention, is the goodwill of their Han managers. As indicated by the behavior of the management of the glove factory, worker protections often appeared as an ethos similar to other capitalist-colonial frontier contexts—they care about their investment in the quality of Turkic worker productivity, while their bodies, social relationships, and social reproduction are viewed as disposable. In December 2018, managers at the factory ordered Gulzira to sign a one-year work contract. She was told, "If you do not sign, you would be sent back to the camp."

Conclusion

Thinking of the digital enclosure as a new frontier in capitalist-colonial expansion is a point of departure for understanding broader forms of devaluation and dispossession at work in Northwest China. This understanding of digital expropriation through data harvesting and ethno-racialized forms of population control extends Brian Jordan Jefferson's conceptualization of digitized "geographies of carcerality" (Jefferson 2020) and "digital enclosures" (Andrejevic 2007) beyond North American contexts to the way minoritized populations elsewhere are codified and criminalized because of their land-based attachments. It also extends analytics of "racial banishment" (Roy 2019) beyond dispossession as it relates to land and urban belonging, to ongoing epistemic dispossession, and new forced labor regimes in a contemporary capitalist-colonial context in Northwest China. This framing, in turn, opens up a more expansive analytic regarding the way enclosure bends the future of

minoritized populations in service to capital accumulation, state power, and the security of settler populations. The management of the Uyghur region through digital enclosure proceeds as an expropriative gaze, turning the "terrorist" bodies of Turkic Muslims into data points to be sorted and assigned values based on compliance and productivity. Ultimately, this enclosure attempts to dispossess by "digitizing and punishing" (Jefferson 2020), and through this process harvest data, and subtract *and* reeducate resistant bodies removed from the landscape, making them productive but simultaneously dispossessed, unfree, and dependent laborers. As such, the digital enclosure that overlays the Uyghur region extends a new sequence in racialization in both geographic space and digital capture.

The People's War on Terror and the techno-political terror capitalism it inspired has created its own regime of truth and economic objectives.[25] The bodies, first of Uyghur men but also women and children, have become the objects of state capital and venture investment in data harvesting and social transformation. Muslim male bodies, as the loci of terrorism, became the reason why millions of people found jobs as Chinese-language teachers, police officers, prison guards, construction workers, service sector employees, public health workers, police contractors, computer engineers, and artificial intelligence developers. Uyghur bodies and productive labor became a site of state capital investment. The counterterror digital enclosure became a growth industry at a frontier of global capitalism. As I will show in the following chapters, this contemporary colonial system was built on older and broader systems of valuation and dispossession.