Apartheid in the Shadows: the USA, IBM and South Africa's Digital Police State

Posted By *Michael Kwet* On May 3, 2017 @ 1:56 am In articles 2015 | Comments Disabled

---

"Beggars and vagrants" are not welcome in Parkhurst, a mostly white suburb of about 5,000 in Johannesburg, South Africa. Criminals of "increasing sophistication and aggression" are on the prowl, residents claim. To combat local crime, community members proposed a solution: put surveillance everywhere. Their proposal, however, was not for "traditional" surveillance. Thanks to the digital revolution, Parkhurst could now integrate facial recognition, thermal sensors, infrared tracking, and data analytics. Armed with powerful new tech, poor black "vagrants" can be watched, flagged, policed, and intimidated into submission.

"Smart" surveillance systems are being assembled quietly inside the country. The public has been kept uninformed. This is the first in-depth exposé of smart policing in South Africa.

A New "Revolution"

Two years ago, Parkhurst became one of the first SA neighborhoods to embark on the installation of their own smart surveillance system. This little community made national headlines as the first suburb in South Africa to get residential fiber Internet. Media outlets whitewashed the surveillance component.

The Parkhurst Village Residents and Business Owners Association fought for "Fibre to the Home" Internet. Their primary motivation was "modern" digital surveillance only high-speed Internet could power, said the organization's chair, Cheryl Labuschagne. That residents now have fast Internet seems to be a secondary bonus.

A Vumatel employee, Giorgio Lovino, elaborates: the fiber "connects to the CCTV [surveillance] cameras…throughout the suburb and it transmits the video feed from those cameras…to a control point where their cameras can then be monitored off-site. And it allows them to do number plate recognition, facial recognition, and all these types of surveillance activities." The CCTV system is being worked out so that it may

be affordable to the community.

Parkhurst plans to install infrared and heat-source cameras to track body movements. Labuschagne says they will use "GPS technology and so on to map where incidents occur" and determine "what movement is considered abnormal rather than typical movements in a neighborhood of people walking their dogs and so on."

Labuschagne leaves unstated what constitutes "abnormal" movements. However, iSentry, the CCTV software Parkhurst seeks, makes it explicit. Their promotional video, titled "Unusual Behavior Detection", depicts a young, black "beggar", flagged by iSentry's artificial intelligence-based video analytics. Within moments, he and an accomplice are brought to the ground by a gang of cops, semi-automatic gun pointed.

The scene appears to be staged for promotional filming as a "typical scenario" for how the system should work. That is to say, Parkhurst's 21st century policing system is advertised to target poor black people.

The iSentry system, deployed by CSS Tactical, has been installed in nearby suburbs, and is spreading to others.

Parkview Police Station Commander, Colonel Moodley, supports the "refreshing" initiative "wholeheartedly". Labuschagne proclaims she is "really really hopeful that what we've started is a revolution" in South Africa.

Smart Cities: Surveillance in the Shadows

A revolution is a number of years in the making. In 2011, the City of Johannesburg announced a draft *Growth and Development Strategy (GDS 2040)* to convert Johannesburg into a "smart city" in cooperation with the private sector. Digital technology would overhaul everything from public service delivery to crime management using "smart infrastructure" and "intelligent Video and Internet surveillance systems".

Shortly thereafter, Johannesburg began implementing "smart policing" based on new surveillance cameras and centralized police data analytics. Last year, then Mayor Parks Tau (ANC) attributed smart policing to a 22% crime reduction for 2014/15 in the wealthy central business district of Johannesburg – a whites-only area under apartheid. Tau boasted his crime-fighting tools have "face recognition technologies, number plate recognition technologies and are able to detect or anticipate when a group of people are planning a smash and grab." The City of Cape Town is similarly

following suit.

High-speed Internet is critical to smart video surveillance because it enables the transmission of high definition feeds. Computers need richly detailed images to identify words, faces, and other attributes. Blurry images will not do. Thus where there is high-speed Internet, there can also be smart surveillance.

At the helm of South Africa's high-speed Internet roll-out is Siyabonga Cwele, the former Minister of Intelligence (2008-09) and State Security (2009-14). As SA's former spy boss, Cwele supported the controversial Protection of State Information Bill which bolsters the protection of state secrets.

Cwele lists no formal credentials, industry experience or training in technology. Nevertheless, President Jacob Zuma, himself a former intelligence chief, appointed Cwele as Minister of the Department of Telecommunications and Postal Services (DTPS). This puts a former spy minister in charge of South Africa's Internet.

Speaking in the Western Cape, Cwele told South Africans they "must adapt" to a "change [in] our notions of privacy". The "fourth industrial revolution" – a term coined by World Economic Forum founder Klaus Schwab – is coming to South Africa.

Smart Policing: United States, South Africa

Across the Atlantic, smart policing is well under way. In 2016, a study published by *ProPublica* found that software commonly used in the United States to predict "future criminals" is "biased against blacks". Even though there were no racial categories programmed into the software, blacks were incorrectly ranked as "future criminals" at almost twice the rate of white defendants. The racist ranking could not be explained by prior crimes or the type of crimes committed, the study found.

In US public spaces, aerial surveillance drones and smart sensors are being used for urban population control. In 2015, the FBI disclosed it flew surveillance drones over Ferguson and Baltimore during BlackLivesMatter protests prompted by police murders of Michael Brown and Freddie Gray. Published documents reveal the FBI was utilizing infrared and night-vision cameras and keeping recordings of aerial drone surveillance footage.

Cell phones are also targeted by cops. In 2015, Baltimore residents discovered their city police department is systematically abusing "stingray" devices that trick cell phone owners into revealing their location. Evidence shows the stingray devices are

overwhelmingly concentrated in poor black neighborhoods, with disproportionate impact on people of color. Half of all US adults are now in a law enforcement facial-recognition database. One-fourth of the nation's police departments have access to face-recognition databases.

Smart policing is a controversial new component of the digital era. Using smart surveillance, computers and sensors automatically detect and interpret video feeds and other data in real-time to facilitate ubiquitous policing. As the cost of technology drops, corporate and state actors are littering cities with an array of sensors – microphones to detect gun-shots, hi-res video for face recognition, infrared and heat to evaluate bodily movements – and networking them with high-speed Internet to radically expand police power.

Utilizing advanced data analytics, those with access to the surveillance – corporations, police departments, private security firms, government spy agencies – sift through massive troves of data to hone in on groups and persons of interest. Computer software is determining where to concentrate cops on patrol to prevent "future crime", with potentially disastrous effects on civil rights.

The South African state is mirroring the US. The government has "grabber" devices that pretend to be cell phone towers in order to "track [a] phone's movements, pinpoint its location, intercept its calls, or eavesdrop on conversations" – without the cell phone owner ever knowing it. Protesters, when gathered in large groups, are highly vulnerable to grabbers.

Drone surveillance has also begun. The City of Cape Town is experimenting with aerial drones to watch over citizens. Their website even calls the program "Big Brother". A Pretoria-based company, Desert Wolf, developed a drone that can spray tear gas and fire rubber bullets at protesters. An unnamed mining company ordered 25 units.

As I reported at Counterpunch in January, South Africa-based R&D organization, the Council for Scientific and Industrial Research (CSIR), has quietly developed Cmore. A new "Jason Bourne" type surveillance system, Cmore aggregates and analyzes data from drone footage, CCTVs, cell phone data, and other inputs for maritime, park, and border policing. The CSIR considered Cmore "for police" and subsequently partnered with the South African Police Service (SAPS). Experiments include "crowd-control concept demonstrations".

Meanwhile, Johannesburg's Intelligence Operations Centre (IOC) is now outfitted with

"100 existing high impact cameras" enabled for software-based "Intelligent Video Analytics as an input into Intelligent Law Enforcement". The new anti-immigrant mayor of Johannesburg, Herman Mashaba (DA), endorsed predictive policing in April 2016, months before his election victory.

Five years prior, IBM, the major computer and surveillance partner to the apartheid state, partnered with the City of Johannesburg to define a roadmap which includes crime prevention and investigative analytics.

IBM Corporation: Apartheid Past and Present

In 2002, South Africans brought a law suit against US corporations alleging direct support for human rights violations committed by the apartheid regime. IBM, SA plaintiffs claimed, provided technology used to implement the apartheid-era racial classification system.

The USA continuously provides technology to oppressive foreign regimes. In years past, multiple US corporations played a treacherous role assisting South African apartheid. IBM has been among the worst offenders.

Beginning in the 1930s, IBM New York, under the direction of its president, Thomas Watson, Sr., supplied Hollerith punch card systems to their IBM Germany subsidiary for use by the Third Reich. IBM machines were customized for the Nazis to efficiently track and sort groups targeted for persecution and genocide. Numbers tattooed on Auschwitz inmates began as IBM punch card system identification numbers.

During apartheid, with Thomas Watson, Jr. now president, IBM New York leased its IBM South Africa subsidiary with specialized technology tailored for the apartheid state. In 1952, the apartheid regime ordered its first electronic tabulator to IBM South Africa. There is ample evidence their technology was used to categorize, segregate and denationalize blacks.

In 1965, IBM lost a bid to produce passbooks targeting the black population. However, they won the contract to build the eerie "Book of Life" issued after 1970 – a surveillance project covering additional races (e.g., coloureds, Indians, and whites).

Computer automation of the population register helped streamline the infamous "reference book" system. The reference books (scorned as "dompas" or "dumb pass") were designed to monitor and control blacks from a centralized location, the Central Reference Bureau in Pretoria.

As Keith Breckenridge's *Biometric State* (2014) details, police desired the ability to swiftly identify and locate "Natives" by their national ID or fingerprints contained in the passbooks. It was "a single, cost-effective tool that would allow the police to track elusive African suspects."

But this form of centralized surveillance had weaknesses – people would lose or burn their dompas or rip out or forge pages. An unwieldy registration backlog quickly ballooned out of control. The dystopian dream of panoptic population control by an all-seeing state failed, but the consequences were brutal. Apartheid cops used the passbook system to perpetrate mass violence and incarceration against blacks.

IBM New York, the central headquarters which provided technology and expertise to its SA subsidiary, has denied liability. Last June, they successfully fought off the law suit brought to US courts by black South African plaintiffs representing victims of apartheid. Plaintiffs included relatives of those tortured, raped, and murdered, in many instances in connection with passbook violations.

In 2011, the City of Johannesburg announced a partnership with IBM to conduct a "five-year public safety strategy in line with the city's 2040 vision of a smart city". Unlike the "dumb" passbook system, IBM's latest system is "smart": it uses "integrated intelligence" for "crime prevention and investigation – including increased police presence and visibility, better coordination amongst agencies, and a data center with predictive analytics" as well as "intelligence sharing".

IBM bases its innovations on its new "Watson" supercomputer system famous for surpassing humans in the quiz show Jeopardy. Their Smart Vision Suite includes "moving object detection, tracking, object classification, color classification, and face tracking" as well as "large scale learning of vehicles and pedestrians". They have a ten-year partnership with South Africa's Department of Science and Technology.

SA in the 21st Century: A Digital Police State

South Africa's smart policing movement has escaped public conversation. Media coverage has been mostly taken up by tech outlets that focus on individual technologies, and apparently see nothing wrong or even endorse this turn of events.

In March, hard-hitting investigative journalists at amaBhungane reported that the Free State issued and awarded a "One Stop ICT Fusion Centre" tender in violation of proper procurement procedures. The fusion centre will apparently provide "an integrated ICT

system for the entire provincial government", including "security camera surveillance and traffic management" in a centralized control room. Indian corporation Tech Mahindra is "the solutions partner".

There is another story here, aside from the tender: what is Tech Mahindra up to? According to a Tech Mahindra brochure, as a part of their "Smart City Solutions", they provide "Smart Security Surveillance", which includes license plate and facial recognition, behavior analysis, video analytics, and real-time monitoring.

Mahindra Defence Systems and US-based Cisco Systems have teamed up in Lucknow, India, to deploy 10,000 cameras. In April 2015, the Uttar Pradesh government's "state police demonstrated drones that can be used to shower pepper powder on an unruly mob". Five of these "crowd control" drones were to be launched that month; they have a range of up to 600 meters. The surveillance "will be very useful in managing traffic violations" as well.

Mahindra is based in India. However 21st century models and technologies of repression are distinctly Western.

This is the current path for South Africa, already begun.

Perhaps it is worth recalling a bit of history. In 2016, a former (now-deceased) CIA operative, Donald Rickard, happily admitted he provided intelligence which led to Nelson Mandela's 1962 arrest. Years later, Steve Biko was placed under a banning order by the state, which silenced his speech and restricted his movement. Police detained and tortured him, leading to his tragic death. Apartheid cops murdered untold numbers through riot control, the "prevention of unrest", and the policing of "public disorder".

SA universities are spending millions on surveillance to quell #FeesMustFall protests. In 2016, CCTVs at Rhodes University mushroomed to provide what seems like blanket coverage, even extending inside buildings. Management refuses to disclose details. Earlier this year, Wits University added new CCTVs and announced considerations for drone surveillance and biometrics on campus. And in March, eNCA's Checkpoint reported that the University of Johannesburg appointed a private security company, Bold Heart Group, that spies on students.

Outside of student spaces, service delivery protests abound. From Vuwani to Cape Town, people are active in the streets. In response to Zuma's latest cabinet re-

shuffle, tens, if not hundreds of thousands of people amassed in public to exercise their constitutionally protected right to protest.

On April 20, amaBhungane launched a challenge to the constitutionality of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (Rica). The challenge focuses on bulk communications interceptions. There could be no better time to also challenge the legality and ethics of smart policing.

It is essential to note that both major political parties – the ANC and the DA – are assembling the smart surveillance state. It remains to be seen what smaller parties like the EFF and UDM have to say – and what the public will say itself.

Two decades after apartheid, half the population lives on $2 (R26) or less per day, while the majority are getting poorer. Serious plans for large scale wealth redistribution remain off the table. In the shadows, the state – and some wealthy citizens – are teaming up with corporations to unleash Western policing for population control.

Michael Kwet is a doctoral candidate in Sociology at the University Currently Known as Rhodes (UCKAR). He studies the digital revolution in South Africa, with a focus on basic education.
