17th Annual Ruth First Memorial Lecture

Big 'Tsek: Surveillance and public space in Johannesburg

Murray Hunter[1]

The beginning

It’s early 2019. I'm with a TV crew. We're face-down on a tiled patio floor, and we're being robbed.

As the two men loomed over us, rooting through our valuables, I realised it was a very inconvenient time to be held up at gun point.

We had just finished filming a segment about a controversial public-space surveillance initiative, involving a company called Vumacam. Minutes earlier, I'd been on tape to decry the company's rollout of cameras in Joburg's suburbs as an undemocratic takeover of public space, part of a long culture of surveillance technology profiting from our deepest fears for our safety. You can see how getting robbed might be a rhetorical setback.

And then, the men were gone, just as suddenly as they'd appeared. The crew lost all their equipment, laptops and phones – and the footage we'd just shot. All I lost was some cheap PR points, and perhaps a small piece of my dignity.

Vumacam, the private security firm, had made a public launch in January 2019, just a few weeks early. The company was rolling out a vast network of smart cameras across the fibre lines of Johannesburg suburbs. By the time of their PR blitz, nearly a thousand cameras were already up and running, with a plan to roll out up to 15,000 in Johannesburg – R500 million worth of infrastructure[2] – and expand to other cities soon after.

Big plans take big money. Vumacam was founded by Ricky Croock, a private security entrepreneur who already piloted a model for camera-over-fibre security with a previous company. Vumacam exists as a partnership between the internet fibre provider Vumatel, and a Croock-aligned investment fund called Imfezeko Holdings. (Their ownership split is 51% to 49%, according to competition authorities). Vumatel, in turn, is a subsidiary of an entity called Community Investment Venture Holdings (CIVH), which is 55% owned by Remgro, the investment giant linked to billionaire Johan Rupert. (In November 2021, Vodacom and Remgro announced plans for the mobile operator to buy a co-equal stake in Vumatel and CIVH’s other fibre assets, for R6-billion, and add its own fibre lines into the mix.)

[1] I’m grateful for the support of Ruth First Fellowship Committee, Bob and Sueanne Huston, Bongani Kona, Dominic Cull, Eric Williams, Gavin Borrageiro, Heidi Swart, Jane Duncan, Kenicho Serino, Matthew Kalil, Michael Kwet, Sophia Phirripides, Wilna Combrink, Ziyanda Stuurman, and colleagues at ALT Advisory.

[2] MyBroadband, ‘Vumacam – Vumatel’s CCTV system to keep South Africa safe’, 14 February 2019. Available here: https://mybroadband.co.za/news/security/295960-vumacam-vumatels-cctv-system-to-keep-south-africa-safe.html

Vumacam's initiative represented a new, possibly unprecedented model for private surveillance technology. Its technology is interesting enough: the camera system piggybacks on fibre networks (some of them owned by its parent company, Vumatel) and uses automatic license-plate recognition to log each vehicle that passes beneath its cameras. The software checks these against a list of vehicles of interest (mostly vehicles reported as stolen or believed to be linked to previous crimes). Vumacam's system also uses a monitoring algorithm to look for signs of unusual activity by pedestrians or vehicles in view of its cameras. If the system detects anything it thinks is suspicious, it pings a human operator for further action.

That's the tech. But the model and its scale are what really set Vumacam apart. Privately owned camera networks are already a familiar presence in many South African suburbs and public spaces. But these have generally been small, feudal networks. Each batch of cameras has been its own closed loop operated by one security company for one set of clients in a single neighbourhood or business centre. Vumacam's offering is a network of many cameras, spanning many neighbourhoods, for many different clients.

It's a lease-as-you-go surveillance network. Any security company with its own set of private clients could pay to get access to certain parts of the camera network – you pay per month per camera, wherever you have active clients. If every little camera network previously existed as its own little fiefdom, Vumacam's proposal was to build something closer to an empire.

* * *

By the time Vumacam made its public launch, I was serving out my notice period at the Right2Know Campaign, a civil society organisation that had become a significant voice on surveillance issues. R2K had initially convened nearly a decade earlier as a broad civil society response to the 'Secrecy Bill', the proposed national security law which would have shored up, and expanded, the state's powers to control the flow of information.

For all its chaos and contradictions, it was an exciting time for activism: a broad, pragmatic, noisy coalition of activists and formations from the middle class, working class and unemployed poor that was campaigning for the free flow of information not just as an elite concern, but as being central to enabling poor and marginalised groups to organise.[3]

The Bill, we felt, was part of a broader effort by South Africa's intelligence structures to claim more of a role in politics and public life. Over time, more of us started taking interest in what else the spy agencies were up to as part of that effort – such as spying on people's communications. As it turns out, that was happening quite a lot.[4] But the intrusions weren't

[3] S Mottiar and T Lodge, ''Living inside the movement': The Right2Know campaign, South Africa'. *Transformation* 102(1):95-120, January 2020.

[4] M Hunter, and T Smith, 'Spooked: Surveillance of Journalists in South Africa'. Right2Know Campaign, 2018. Available at https://r2k.org.za/spooked
Right2Know Campaign, 'Stop the Surveillance: Activist Guide to RICA & State Surveillance in SA', 2017. Available at: https://r2k.org.za/rica-guide

only technological. There were signs that state intelligence operatives were in the habit of viewing their critics, and other troublemakers, as threats – and responding accordingly. As it turns out, this was also happening quite a lot. (It has since come to light that the Agency had infiltrated a range of unions, political groups, NGOs and civic formations, including ours.[5])

In responding to these developments, the Right2Know Campaign became, not quite accidentally, an organisation seeking to provide activist responses to surveillance abuses. The research, activism, journalism and litigation from that period fed towards the Constitutional Court's ruling last year, which struck down parts of South Africa's interceptions law, RICA.[6]

On reflection, this work was mostly concerned about the state and *its* surveillance powers – a necessary response, perhaps, to the turmoils of the post-apartheid state, where the security structures have been a terrain of struggle for competing factions of all sorts: the outgoing guards, the incoming guards, and of course not a few people who turned the structures into a vehicle for their own criminal interests.[7]

But barring a few exceptions, like the Stellenbosch firm VASTech who was caught supplying spyware to the Gaddafi regime[8], surveillance entrepreneurs have worked in the shadows, and have largely been spared the same kind of scrutiny. Where private companies *have* faced public pressure on surveillance issues, it has often in their capacity as contractors and vassals for government surveillance – such as pressure on South Africa's mobile network operators to disclose more about their role in wiretapping,[9] or questions to European spyware vendors about their contracts to South African state bodies.[10] And of course, a number of the more scandalous surveillance entrepreneurs have been state employees who rent out their government surveillance powers to private clients.[11]

* * *

In any case, by January 2019 I had resigned my post – burnt out, and bruised by the harsh internal politics that are common in big, social organisations.[12]

[5] High-Level Review Panel Report on the State Security Agency. Presidency of the Republic of South Africa, December 2018. http://www.thepresidency.gov.za/download/file/fid/1518.

[6] AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others [2021] ZACC 3

[7] J Duncan, *Stopping the Spies: Constructing and resisting the surveillance state in South Africa,* 2018, p 57-87

[8] The Intercept, 'South Africa spy company used by Gadaffi touts its NSA-like capabilities,' 31 October 2016. Available at: https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities/

[9] TechCentral, 'Court battle to get Rica data from mobile operators', 7 November 2018. Available at: https://techcentral.co.za/court-battle-to-get-rica-data-from-mobile-operators/201200/

[10] Duncan, p 129

[11] See for example M Hunter, 'Cops and call records: Policing and metadata privacy in South Africa', Media Policy and Democracy Project, 2020, https://mediaanddemocracy.com/, p 35

[12] See P Mlungwana, 'Reflections on Leadership', *Fragments of Activism,* 2019, p 133; D McKinley, 'Lessons of Struggle: The Rise and Fall of the Anti-Privatisation Forum', The South African Civil Society Information Service, 8 February 2012. Available at: https://sacsis.org.za/site/article/1197

Yet, with just a few weeks left in my role, Vumacam's public launch lit a rage in me. Perhaps it was an attempt at legacy-building. But I fired off emails. Unleashed tweets. I went on the radio to harangue their staff. When we realised they were operating without a private security license, we complained to the regulator and the company was sanctioned.

Then, a producer for a local news show called. There was a Vumacam pole right outside her house, she said. Could we do an interview right there on the pavement? The answer was yes. So we did it, and of course, were robbed a few minutes after finishing filming.

Before the robbery, it seemed pretty clear that the producers had been unimpressed with Vumacam's answers about who had been consulted in the rollout of their cameras, and what thinking they had done about the privacy implications of their whole enterprise. But when the story went to air, I can only imagine that having a robbery at the centre of the story added a degree of sympathy to the company's point of view.

And so, after a bumpy launch, the company was able mainly to proceed apace. Although the organisation fell into funding troubles, a few comrades at Right2Know tried to keep the heat up, joined by a Lonehill-based businessman named Gavin Borrageiro who emerged as a local anti-surveillance activist over an unrelated CCTV scheme in his own neighbourhood.

Every so often, the company has faced new and embarrassing articles about the less savoury aspects of their operations, notably from the surveillance scholar Michael Kwet, and the journalist Heidi Swart. For my part, I must admit I'd retreated to the margins of the whole affair, but every now and then, I'd send a mean tweet.

Vumacam invested in PR touting its privacy credentials, upgraded their legal documents, and bought advertorials in newspapers. And the cameras kept rolling out.

Vumacam vs the City of Johannesburg

In 2020, in the midst of the pandemic, a very curious battle between Vumacam and the local authorities spilled out into the high court.

Vumacam was suing the Johannesburg Road Agency and the City of Johannesburg, saying that the authorities had taken an off-the-books decision to prevent the company from putting up its camera poles. According to municipal law, if you want to erect a pole or bury a cable next to a public road, you need the council's permission: a bit of paper called a wayleave.

Vumacam told the court that, in the early months of their operations, the company could expect to the authorities to approve each pole installation within 48 hours. But sometime in April 2019 – in other words, in the weeks following the initial controversy around Vumacam's scheme – the approval process started to slow down.

The company's founder and CEO, Ricky Croock, told the court that the Roads Agency started coming back on every application, asking for additional documents and adding new conditions to their applications. A public participation process. Authorisation from the police, the private security regulator, and ward councillors. And then, after briefly suspending all operations for the first six weeks of lockdown, the Agency notified Vumacam that applications for CCTV installations would remain suspended until further notice.

With no mandate, and scant legal power it should be said, the bureaucrats in charge of public roads were pushing back on the surveillance scheme.

I reached out to the Joburg Roads Agency and its then acting head, Victor Rambau, to ask about this and didn't receive replies. But in the court case, Mr Rambau gave a pretty frank explanation for their discomfort. This was not, he explained, just about permission to put up poles: "The approval which Vumacam seeks is in fact to install surveillance cameras to spy on the public and thereafter sell the spy footage and related data to interested parties for a fee."

"The JRA and the City," Mr Rambau told the court, "do not have legislative powers to authorise such an infringement of privacy rights."

States are complicated creatures. Local government entities are not usually known for taking bold moral stands. And the City of Johannesburg has ambitions of growing its own camera network, as part of a vast 'smart city' project.[13]

And not all arms of government were so uncomfortable with the Vumacam initiative. Vumacam's court papers included a glowing letter from a Brigadier of the SAPS's provincial command, which had originally been written to lobby the city electricity providers to resolve an issue around the company's use of neighbourhood grids.

Vumacam, the Brigadier wrote, is "a critical component part in assisting with the fight against crime". The Brigadier stated that Vumacam is one of the hundreds of private security firms participating in the Eyes and Ears initiative, a collaboration between business and police to feed information from private security guards into the police's war room. "We anticipate that the Vumacam solution will then be deployed to other major cities across Gauteng and then nationally if successful in Gauteng," he wrote.

What the City's true motivations were, we can't say.

But the court ruled in Vumacam's favour, although it was careful not to weigh in on the legality or otherwise of city-wide video surveillance. (The Right2Know and Gavin Borrageiro made independent submissions to the court, as *amici curaie,* to argue against its constitutionality. That question was ultimately left for unresolved.) Quite simply, Vumacam's legal team convinced the court that the case had nothing to do with the nature of Vumacam's business or its technology. What was at the top of the poles was irrelevant: all that mattered was whether the city's bylaws allowed Vumacam to put up poles, and whether the roads agency was allowed to stop them.

[13] M Kwet, 'The City Surveillance State: Inside Johannesburg's Safe City Initiative', Policy Briefing 231, South African Institute for International Relations, March 2021

Considering the JRA's arguments that it felt unable to permit Vumacam to roll out its camera network without public participation or legal regulation, the judge wrote: "This may be well-meaning, but it is not lawful."[14] The judge ordered the JRA to process Vumacam's wayleaves within a week.[15]

Shift to Detroit

In July 2021, while civil unrest and opportunistic looting brought parts of South Africa to the edge of shutdown, I was mid-town Detroit in the United States, sitting down in a coffee bar with Eric Williams, a civil liberties lawyer with the Detroit Justice Center.

Williams had been among the central figures in an activist campaign in Detroit against Project Green Light, a city-wide police surveillance network that has become a global case study for civic resistance to surveillance technology.

Decades of industrial decline and white flight to neighbouring towns have made Detroit one of the poorest cities in the US.[16] It's also 80% Black.

In 2016, as part of a grand economic bounce-back, Detroit's city leaders launched Project Green Light, an ambitious partnership with local businesses to build a camera-based public safety programme – or, as its critics would call it, a privately-funded police surveillance network.

As part of Project Green Light, local businesses and organisations can pay to erect police-monitored smart cameras on their premises. For anywhere between R15,000 and R90,000, a business can pay one of the city's approved private contractors to install the cameras, plus a yearly fee of around R24,000 for cloud storage.[17] No money changes hands between the businesses and the city: the contractors build the network, the businesses pay for it, and the police monitor it.

Every location with Green Light cameras also installs, at their own cost, a flashing green light – a branded beacon to signal its participation in the programme, and its status as a place of safety. The video goes to a police control centre, where officers cycle through live feeds and can pull up the feed from a particular location in the event of a 911 call. There are now over 700 locations with cameras up. Most of these are retail businesses – petrol stations, bottle stores, and the like – but more than a third of the Green Light locations are categorised as "service organisations" such as churches or non-profits, or residents' associations.

[14] Vumacam Judgment

[15] I reached out to the JRA for comment, and did not get a response. I reached out to Mr Rambau, who now works at another agency, and did not get a response.

[16] Poorest Cities in America, https://worldpopulationreview.com/us-city-rankings/poorest-cities-in-america

[17] Detroit Community Technology Project, A Critical Summary of Detroit's Project Green Light and its Greater Context, 2019, p9

If you've heard of Project Green Light, it might be because of what happened in 2019, when it emerged that the police had built facial recognition capabilities into their flagship public safety project. The city had signed a R15-million contract for facial recognition software from a company called DataWorks Plus, which allows police to compare images from the camera feed to a database of about 40 million photos – some from law enforcement database, but mostly using collections of drivers' license photos.[18] This wasn't part of the original public pitch.

Eric Williams, the attorney, told me, "I do not have an inherent bias against the police." Five of his closest relatives work in law enforcement. "But this shit is *shady.*"

The technology used by DataWorks Plus was found by a federal study to falsely identify Black and Asian faces up to 100 times more often than Caucasian faces.[19] As I mentioned, Detroit is one of the Blackest cities in the United States.

That year, a series of police oversight hearings became the staging site for public mobilisation against the programme. The Detroit Board of Police Commissioners, a civilian oversight committee, had all supported Project Green Light. But now, activists lined up at the microphone to condemn the programme as a symptom of police overreach and the surveillance of communities if colour. At one hearing, a member of the oversight committee who opposed the surveillance programme refused to yield the floor; in front of news cameras, his colleagues had him arrested and removed from the meeting in handcuffs.[20] Pressure on the programme grew in 2020, after two separate cases in Detroit where police acted on false matches from the facial recognition software to arrest black men – in fact, one adult man and one teenager – who couldn't possibly have committed the crimes under investigation.[21]

To some extent, the pressure seems to have worked.

Although the programme remains intact – and the City extended its contract with DataWorks Plus – the police developed an extensive policy governing the use of facial recognition.

The activism around Project Green Light also made it a literal textbook case for the links between surveillance technology and racial injustice. And last year the Detroit City Council passed a new bylaw, adapted from a 'model' bill produced by the American Civil Liberties

[18] Ibid, p4

[19] New York Times, 'Wrongfully Accused by an Algorithm', 24 June 2020, Available at https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[20] The Detroit News, 'Police commissioner sues over arrest at board meeting', 13 August 2020. Available at https://www.detroitnews.com/story/news/local/detroit-city/2020/08/13/police-commissioner-sues-over-arrest-during-board-meeting/3368946001/

[21] Washington Post. 'Wrongfully arrested man sues Detroit police over false facial recognition match' 13 April 2021. Available at: https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

Union (ACLU), which requires more transparency and community input in how the city uses surveillance technology.[22]

But these are slender gains. For starters, Project Green Light continues to roll out. And the celebrated bylaw had been stripped of some of the muscle in the ACLU model bill on which it was based. Most notably, the Detroit bylaw removed a provision for punishment for any official who misuses the technology. It also nixed a section that required any pre-existing surveillance programmes to be reviewed and brought in line with the new policy.[23] In Eric Williams' words, "It goes a long way toward ensuring transparency, but it does nothing about accountability."

In all, the battle over Detroit's surveillance network offers important lessons for communities faced with similar programmes. For example, that a focus on particular aspects of the technology (such as facial recognition) may help draw attention to the problems and risks of the technology but should not come at the cost of questioning the very logic of the system itself. (While concerns about facial recognition were a big part of the controversy around Project Green Light, the programme's critics have been clear that the greater problem is a surveillance network that monitors majority-Black neighbourhoods and draws millions in infrastructure spending that could be used for nearly anything else.) Another lesson is that legal reforms are important, but may offer only a partial solution. And yet another is that resistance *still matters* – and the sooner, the better. Because once the cameras go up, they don't come down.

Vumacam's algorithms

I should say at this stage that Vumacam did not respond to written questions or agree to an earlier request for an interview. But I'm certain they would feel these views are deeply unfair.

One of Vumacam's key defences against critics is that it does not use facial recognition – although it has left the door open to doing so later. (A PR rep told journalist Heidi Swart, "while we are not going to engage in facial recognition until regulatory compliance is assured and the technology is reliable and safe enough to engage, we certainly always have our eye on the ball in terms of innovation used responsibly as a means to fight crime."[24])

Vumacam's main form of tracking is its automatic license-plate recognition, which allows it to log the movements of every vehicle from one intersection to the next wherever their network

[22] Detroit Free Press, 'Detroit to boost surveillance transparency but skeptics remain', 29 May 2021. Available at: https://www.freep.com/story/news/2021/05/29/detroiters-feedback-facial-recognition-surveillance/7486598002/

[23] Proposed Community Input Over Government Surveillance Ordinance, 12 April 2021. Available at https://www.bridgedetroit.com/wp-content/uploads/2021/05/LAW-CIOGS-with-transmittal-letter-4-14-21-amended-at-4-12-21-PHS.pdf

[24] Heidi Swart, 'Vumacam's 'hundreds of thousands of cameras' will be watching you'. *Daily Maverick* 25 September 2021. Available at: https://www.dailymaverick.co.za/article/2021-09-25-vumacams-hundreds-of-thousands-of-cameras-will-be-watching-you/

is live. (It currently claims to read nearly 7000 license plates every minute.[25]) The company is keen to emphasise that this logging is automatic – that in the vast majority of cases no human being takes note of any data point being entered to the system – but this is part of the basic nature of modern, digital surveillance. For surveillance to be total or near total, it's almost always going to be by a machine, not a human.

Another controversial power of the Vumacam capability is its behavioural analytics – the feature which flags unusual activity by pedestrians or vehicles. This is powered by a piece of software called iSentry, which Vumacam describes as a "completely non-biased" algorithm. A passage that you will either find attributed to Ricky Croocks in media articles, or printed verbatim in the company's PR material, explains: "...[the software] is not pre-programmed to identify race. Unlike many other behavioural analytics software, iSentry is one of only a few that do not have any preprogramming of what is deemed to be unusual behaviour thus removing any forms of programmed-in bias. It utilises unsupervised Artificial Intelligence to monitor pixels, so if it detects unusual formations of pixels, that are different to what it observes 24/7 it will send an alert to the security company control room where the company can monitor the situation to determine if it requires intervention."[26]

This means you have nothing to fear, unless you are an unusual formation of pixels.[27]

But there is a troubling trend in what formations of pixels this system finds unusual. In previous research, the writer Michael Kwet unearthed an iSentry "shift report" posted by Vumacam's predecessor, the Croock-owned company Fibrehoods, which used the same software. The single shift report flagged 28 "suspicious" people in the streets. None of the 28 were up to any wrongdoing, but all were Black: an electrician, construction workers, a person sitting on the side of the road, people walking in a group.[28]

The blame goes beyond Vumacam's bit of software. The contemporary South African reality is that some of us are deemed to be unusual formations of pixels, and some of us are not. But whether they know it or not, at best technology like this serves to mimic and replicate these patterns of injustice.

I found a similar case in a Vumacam business presentation from last year, which showcased its services to the Sandton Community Improvement District (CID), in partnership with a security monitoring firm called AI surveillance and a patrol company called Servest. At 7.16am on 12 May 2020, a Vumacam-powered shift report notes the following incident alert from Sandton

[25] Vumacam, LPR hits per minute at 21 October 2021. Available at: https://vumacam.co.za

[26] Vumacam, 'The Facts Regarding the Integrated Smart Camera Network', 3 December 2021. Available at: https://www.vumacam.co.za/the-facts-regarding-the-integrated-smart-camera-network/

[27] As a side note, it reflects an odd misunderstanding to say an algorithm is non-biased because it is not "pre-pregrammed to identify race." When it comes to discrimination, machines are much like humans: their bias is usually implicit. An algorithm need not be designed to identify a characteristic such as race, gender, economic class, sexual identity, etc, in order to discriminate along those characteristics.

[28] M Kwet, 'Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa,' *Motherboard*, 22 November 2019. Available at: https://www.vice.com/en/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa

CBD: “an alert triggered a group of unknown males walking alongside the road... on-site security officers confirm the unknown males are vagrants and have been removed from the site. Controller maintained a close watch.” At 9.45 that same morning, at a different intersection, a new alert: “An alert triggered an unknown male standing in the middle of the road. Controller contacted Servest control room who confirmed the unknown male is a beggar that works at various intersections. JMPD have failed to remove the beggar from the site. Controller maintained a close watch, everything is in order.”[29]

Two incidents, from a single suburb, on a single morning.

“Trust in our vision”

With over 5,300 cameras, Vumacam’s network is growing, and its ambitions are growing with it.

In 2020, Croock told an interviewer that the company had moved past its initial vision of a 15,000 camera rollout in Johannesburg: it was now building its system to manage 100,000 cameras, with plans to integrate existing camera networks in shopping centres and residential estates. “We’re just saying, ‘We’ll take over those cameras, we'll put it into our platform, we'll marry it to the public space, and it's all centralised.’ Now the numbers start becoming really exciting, in terms of in our dealing with hundreds of thousands of cameras – but again, dealt with responsibly, it’s compliant, it’s structured, you can report on it correctly.”[30]

The scope of Vumacam’s offering has also grown. At some stage it expanded its client base beyond the private security industry, taking on insurance companies, for instance, who can use access to the footage to verify insurance claims.[31]

In an interview last year, Ricky Croock suggested the company was developing the capacity for cameras to have social-distancing awareness or mask detection[32], although a PR representative recently told journalist Heidi Swart that this was just “a theoretical example (based on a trial build)” and that Vumacam was not rolling out such analytics.[33]

But the conclusion is clear: Vumacam is open to moving the goal posts.

In the face of criticism, Vumacam is sure to emphasise its compliance. But it’s run into compliance issues before. I’ve already mentioned that, soon after they launched, the security

[29] Vumacam, untitled presentation, March 2021. Available at: https://web.archive.org/web/20211009014829/https://www.gpma.co.za/wp-content/uploads/2021/03/2021_03-Vumacam.pdf

[30] TechCentral, Interview: Vumacam CEO Ricky Croock, 23 June 2020: https://techcentral.co.za/interview-vumacam-ceo-ricky-croock/176322/

[31] MyBroadband, ‘Vumacam footage being used in insurance claims investigations’, 12 December 2020, available at: https://mybroadband.co.za/news/security/373269-vumacam-footage-being-used-in-insurance-claims-investigations.html

[32] TechCentral, 23 June 2020

[33] H Swart, ‘Vumacam’s ‘hundreds of thousands of cameras’ will be watching you’, Daily Maverick, 25 September 2021, available at https://www.dailymaverick.co.za/article/2021-09-25-vumacams-hundreds-of-thousands-of-cameras-will-be-watching-you/

industry regulatory, PSIRA, slapped the company with charges for operating without a security license.[34] (Part of the marketing blitz about their disruption to the sector was a repeated emphasis that "we're not a security company, we're a technology company" – the law and the regulator disagreed.) Yet it's not clear that they were fully compliant for the technology aspect of their business either: while researching this piece I noticed that their license to operate a communications network was only issued in May 2019, the year after their cameras started going live. Vumacam and ICASA declined to answer questions about this, but operating an unlicensed communications network – if this is what was happening – is against the law. In theory, it can result in criminal charges.[35]

Vumacam has also emphasised its fastidious compliance to South Africa's data protection law, known as POPIA, and the EU's even more stringent GDPR. But recent reporting by Heidi Swart showed the company had made misleading claims about the GDPR credentials of its video management software – and Vumacam quietly scrubbed the claim from its website.[36]

* * *

Underscoring all of this, of course, is South Africa's notorious crime.

Vumacam may position itself as a technology company, but it's basically part of South Africa's massive private security industry, which is made up of more than 11,000 companies and over half a million registered employees.[37] (This would make it one of South Africa's biggest employers. Before the Covid economic crisis, the regulator reported there were another 1.9 million *unemployed* security guards.)

That South Africa has a serious problem with crime, and especially violent crime, is obvious.

What's less clear is whether the private security industry is part of a solution. Only one in ten South Africans are clients of the private security industry[38], but the industry has four or five times more employees than the South African police. Of course, many of those are employed to 'guard' public-private spaces – everything from shopping malls and airports to Home Affairs offices and the local magistrate's court, but that's precisely the point.[39]

This disparity is a symptom and a cause of our social malaise: it's not just that only the privileged minority can pay for private security, it's the very fact that they're the privileged minority that gives them suburbs, estates and office parks that *need* private security. But the privatisation of 'public' safety also means in a crime-stricken society, the vast majority of

[34] The Citizen, 'Who watches Big Brother? Joburg's private surveillance cameras come under fire', 1 March 2020. Available at: https://www.citizen.co.za/premium/2248702/who-watches-big-brother-joburgs-private-surveillance-cameras-come-under-fire/

[35] Electronic Communications Act 36 of 2005, s72

[36] Swart, 25 September 2021

[37] Private Security Industry Regulatory Authority, Annual Report 2019/20. Available at https://www.psira.co.za/

[38] StatsSA, Victims of Crime Survey, 2019/20; 2018/19.

[39] D McKinley, *South Africa's Corporatised Liberation*, 2017, p 118.

money being spent on protecting people and space goes to private services, for select areas, for select people.[40]

Certainly, the South African state has done little enough to keep the trust of its people on the question of public safety and much else. (A recent Afrobarometer poll found trust in the police at its lowest level in the 20-year history of the survey.[41])

But companies like Vumacam have benefitted from a deep and generalised mistrust of government, in favour of the private sector. In an interview with Croock, a tech journalist remarked: "I personally feel more comfortable that it's a private company rolling out this network and not the government or the City of Johannesburg *because you have a profit motive*, whereas there may be other motives involved in a state actor rolling out such a network."

In some of its earliest PR material, the company actually made distrust of the police part of their sales pitch, writing in a blogpost:

> "...*many believe that they cannot rely on the SA Police Service.* Not only has the Police Ministry admitted there are not enough members to ensure visible policing, which is a deterrent on its own, Africa Check, which analyses data, has *accused the cops of not being forthcoming on information on how many police officers themselves are criminals.*"[42]

What is it about private power that makes it so much more palatable, to some, than public power?

I put this question to the policing researcher Ziyanda Stuurman.

"[The security industry] creates this vision of itself that's outside of the state and even says, 'We function better than the state, but more importantly, will function better than the state *for you,'*" she told me. "That plays into that individual desire for safety in a way that is incredibly profitable for them, but also assuages a lot of middle class and elite fears about crime."

It's curious that we would be asked to put our faith in an unelected private body operating across vast stretches of public space, with no public mandate, and governed only by a patchwork of public laws.

"Who are they accountable to?" Ziyanda exclaimed. "They're certainly not accountable to *me*. Those employees are accountable to their managers, those managers are accountable to their bosses, and those bosses are accountable to the shareholders of Vumacam, not to the average South African person, and definitely not to the public," she told me.

[40] The political analyst Sizwe Mpofu-Walsh has gone so far as to declare, in a recent book, that "Apartheid did not die; it was privatised."

[41] Afrobarometer, 'South Africans' trust in police drops to new low, Afrobarometer survey finds', October 2021. Available at: https://afrobarometer.org/press/south-africans-trust-police-drops-new-low-afrobarometer-survey-finds

[42] Vumacam, 'CCTV: Security or just scary', 30 November 2018. Available at: https://www.vumacam.co.za/cctv-security-or-just-scary/

Vumacam and democracy

I need to be clear that this is not the problem of a particular company or technology, but of the frailty of our democratic life. Vumacam's model is, in the most literal sense, a tech company privatising the public space. It's as apt an analogy as one could ever want for why democratic activists in South Africa need to reckon with the unchecked power of tech companies whose influence spans the globe and who answer to no single authority.

Yet the Vumacam story also tells us something about the limits of what we call the public sphere. The specific business model has raised concerns about privacy, spatial justice, inclusivity and public participation. But these were never values found in abundance on the average street corner in South Africa. Vumacam in some ways is merely a technological innovation on a set of analogue injustices.

But whether you support the business model or not, the company seems largely able to do what it thinks is best.

They can get the endorsement of a ward councillor, or a ratepayers' association, and call it public consultation, but this is a tenuous link to the polity.

They face a fragmented civic space, crumbling media, and public institutions that are creaking under the weight of their own mandates.

And above all, a business model like this is enabled by the failures of our democratic state to serve its people. The question of whether people want the cameras or not is a bit of a distraction. I'm certain that very many do. In a society where the democratic state has so utterly failed to keep its people safe, many people would – and do – go to extraordinary lengths to make themselves feel safer. The violence, inequality and depravation of our public life invite anti-democratic solutions – which, the theory goes, fuels more violence and perpetuates inequality.

Writing about the 'fortified enclaves' of Sao Paulo – and those of Johannesburg, Los Angeles, Budapest, and beyond – the anthropologist Teresa Caldeira argues that, no matter how understandable the urge for fearful communities to securitise public spaces, the effects are fundamentally anti-democratic and toxic to public life. "Cities of walls," she writes, "do not strengthen citizenship but rather contribute to its corrosion."[43]

In responding to the specific threats these technologies present, we may want better data protection, new oversight and scrutiny of algorithms, or perhaps regulation over the infrastructure and business models themselves. But we need more than this as well.

[43] Teresa P. R. Caldeira, *City of Walls: Crime, Segregation, and Citizenship in São Paulo*, 2000, p 334

We need to build strong, resilient social coalitions against the co-option of public space and public life. We need to build public spheres capable of defending themselves, and *worth defending*.

* * *

The coming skirmishes with Big Tech

I've been thinking of the Vumacam initiative a lot recently, because it spells trouble for the battles ahead with other, much bigger industries.

For a brief, bright moment last year it appeared that South Africa's institutions and its people might be lining up to challenge the authority of the company then called Facebook.

In early 2021, Facebook faced global backlash when it announced changes to the WhatsApp privacy policy for all non-EU users; it lead to a surge in downloads of competing messaging apps in South Africa and many other parts of the world. The actual policy changes were relatively minor, but seemed to spark a delayed outrage among users at the extent of personal data flows that were already happening between WhatsApp and other Facebook companies – and of course at the reality that Facebook intends to do what it wants with the platforms it thinks of as an empire, and the users it thinks of as its subjects. The company backpedalled, and poured millions into damage-control ad campaigns. South Africa's Information Regulator went on a warpath – albeit a wonkish one – by issuing an opinion that WhatsApp couldn't lawfully share any South African users' data with other FB companies,[44] and announcing that it would explore litigation against the company.[45]

Around the same time, South Africa's Parliament had summoned Facebook to a hearing. Formally the meeting was billed as a roundtable on content moderation with industry players, but then-MP Phumzile van Damme – who had first called for the meeting – expressed interest in broaching a wider range of issues: Facebook's plans to deal with electoral disinformation in South Africa, data protection, and even discussions around Facebook paying South African media houses for carrying their content.[46] In any case, Facebook agreed to participate, which would have been its first appearance before an African legislature, but a few days before the hearings, the company pulled out.[47] Facebook had stood up lawmakers in far more powerful countries, and will certainly do so again.

Months later, van Damme – who had by then resigned from her party, the Democratic Alliance – revealed that DA leaders had tried to pressure her to soften her tone on Facebook. The party

[44] Reuters, 'South Africa's information regulator says WhatsApp cannot share users' contact information', 3 March 2021. Available at https://www.reuters.com/business/media-telecom/south-africas-information-regulator-says-whatsapp-cannot-share-users-contact-2021-03-03/

[45] Reuters, 'South African regulator seeking legal advice on WhatsApp's new privacy policy', 13 May 2021. Available at: https://www.reuters.com/world/africa/south-african-regulator-seeking-legal-advice-whatsapps-new-privacy-policy-2021-05-13/

[46] https://www.da.org.za/2021/05/da-looks-forward-to-historic-meeting-in-parliament-with-facebook

[47] https://www.news24.com/fin24/companies/ict/facebook-refuses-to-appear-before-sa-parliament-on-its-own-20210525

had also refused to authorise a statement criticising Facebook for withdrawing. Text messages from the party's chief whip Natasha Mazzone showed both a flimsy understanding of how the company works, and a concerning lack of appetite to take a firm position against the company. "We do not want to escalate into a fight with FaceBook [sic]," Mazzone wrote. "They are our biggest social media apparatus and it's a fight we will not win."[48]

If questions of Big Tech and the public sphere need to be resolved between Big Tech and the public, it's hard to emphasise just how outmatched we all are. Most of us live in countries that are so puny that we're not even on their balance sheet.

In Facebook's latest annual report, South Africa, along with the other 53 countries of Africa, and those of Latin America and the Middle East, are grouped together as "Rest of World". Together these countries accounted for 600 million daily users, and $7,7 billion in revenue in 2020. (This seems a lot – and it is – but Facebook earned three times that in Europe, and fives times as much in North America.)[49]

In financial reports from Google's parent company, Alphabet, all of Africa disappears into the regional group of 'EMEA' (Europe, Middle East and Africa) – which together net 30% of the company's $182 billion in revenue last year.[50] Microsoft brought in $143 billion, reporting a simple two-region breakdown: "United States" and "Other countries".[51]

Like the guy says in *Jaws*: We're going to need a bigger boat.

On hope

It's been theorised as 'surveillance capitalism' – where the Googles and Facebooks of the world have created a vast monopoly on social and economic power by turning every person's most mundane digital interaction to profit.[52] Another is 'digital colonialism', where the exploitation is not just from corporation to user, but from north to south: foreign powers engaged in a new scramble to lay claim to bits of territory ("marketshare") and subjects ("users") as sources for wealth and control.[53]

There seem to be few questions of justice, freedom and morality that don't at some point come down to a piece of technology, and who owns it, and what they do with it. More and more of our public and private lives are playing out across digital property, usually owned by someone else, who usually work to a set of rules that we can only vaguely understand, and rarely control. These technologies, and more importantly the people who own them, are capable of

[48] https://www.news24.com/news24/southafrica/news/van-damme-and-steenhuisen-at-loggerheads-over-her-resignation-as-an-mp-20210825

[49] *Facebook Annual Report 2020,* January 2021. Available at: https://investor.fb.com/financials/default.aspx

[50] *Alphabet Annual Report 2020*, April 2021. Available at: https://abc.xyz/investor/

[51] *Microsoft Annual Report 2020,* October 2020. Available at: https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/2020_Annual_Report.docx?version=8a3ca1db-2de7-c0e7-d7c5-176c412a395e

[52] The term is popularised by S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2018

[53] Digital colonialism: US empire and the new imperialism in the Global South, Race & Class, Vol. 60(4) 3–26, 2019

great and terrible things. They can unite or divide; empower or repress; inform or deceive; connect or exclude – and when we look to the giants of Silicon Valley, or Shenzhen, very often it appears that many of them are doing all of these things all at once, and profiting handsomely for it.

The age of surveillance capitalism often leaves little room for hope. There is plenty of optimism, from tech CEOs promising to change the world, and from naive proponents of techno-solutionism.

Yet for most people, to have mindful experience of the technological products associated with surveillance capitalism is to feel something worse than despair. It's *dread*: a paralysing sense of hopelessness, helplessness, and inevitability. In this, surveillance capitalism is too much like another great, existential threat of our age: the climate crisis.

Yet, our collective sense of their inevitability is one thing that makes them inevitable. The agents of surveillance capitalism don't just benefit from this sense of dread; they rely on it for their own survival.

This dread masks a range of choices that each person can make individually, and that all of us can make collectively. A word for this is *agency*.

It includes, very often, the choice to use different technology, where possible or practical.
It also includes the choice for collective action, at a local level – whether it's to show up at a residents' meeting to push for different outcomes or show up at a city council to push for new laws. In the US, 21 cities have passed a version of the ACLU surveillance oversight law recently adopted in Detroit.[54] In the EU, policymakers have proposed similar initiatives. The opportunity exists to create local or national oversight on these technologies in South Africa, or anywhere else.

There are bigger political opportunities as well. In the US, where the majority of true tech giants are headquartered, there are very serious conversations about using anti-monopoly laws to break the giants of Silicon Valley into their component parts.[55] This would hardly solve the problem, but at least changes the balance of forces to give individual users – and communities across the world – a fighting chance to rein these companies in or boycott them meaningfully.

Shoshana Zuboff describes surveillance capitalism's assault on our sense of outrage as the loss of astonishment. "We grow numb to these incursions and the ways in which they deform our lives. We succumb to the drumbeat of inevitability, but nothing here is inevitable. Astonishment is lost but can be found again."[56]

[54] ACLU, Community Control Over Police Surveillance, n.d. Available at: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance

[55] Zephyr Teachout, *Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money,* 2020.

[56] Zuboff, 194.

They are, if we choose to act, and to act *together*, very evitable.

[ends]