IN THE HIGH COURT OF THE REPUBLIC OF SOUTH AFRICA

GAUTENG LOCAL DIVISION, JOHANNESBURG

Case Number: **14867/2020**

In the application for admission as *amici curiae* of:

THE RIGHT2KNOW CAMPAIGN	First Applicant for Admission as an *amicus curiae*
and	
GAVIN DENNIS BORRAGEIRO	Second Applicant for Admission as an *amicus curiae*

In the matter between:

VUMACAM (PTY) LTD	Applicant
and	
JOHANNESBURG ROADS AGENCY	First Respondent
CITY OF JOHANNESBURG METROPOLITAN MUNICIPALITY	Second Respondent

---

HEADS OF ARGUMENT ON BEHALF OF THE *AMICI CURIAE*

TABLE OF CONTENTS

INTRODUCTION

1. This matter concerns the roll-out of bulk and indiscriminate CCTV video surveillance, which directly implicates the right to privacy[1] of "thousands of residents of Johannesburg".[2] For this reason alone, this matter clearly raises a constitutional issue. In addition, this matter seeks to review and set aside administrative decisions taken by the Respondents relying on the Promotion of Administrative Justice Act[3] ("**PAJA**"), which further raises a constitutional issue of just administrative action in terms of section 33 of the Constitution.[4] As constitutional issues are clearly raised, this Court's jurisdiction to make any order which is "just and equitable" is engaged,[5] as is the right of the Applicants for Admission as *amici curiae* ("**Applicants for Admission**") to apply to intervene in this matter.[6]

2. As a matter of public interest with constitutional ramifications, the Applicants for Admission seek leave to intervene as interested parties to enrich this constitutional debate.[7] In complying with Rule 16A of the Uniform Rules of Court ("**Rules**"), albeit

---

[1] Section 14 of the Constitution provides that "[e]veryone has the right to privacy, which includes the right not to have—
(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed."

[2] Applicants HoA, para 44, page 17.

[3] 3 of 2000.

[4] *MEC for Health, Eastern Cape and Another v Kirland Investments (Pty) Ltd* [2014] ZACC 6; 2014 (5) BCLR 547 (CC); 2014 (3) SA 481 (CC) ("***Kirland***") at para 27; *Camps Bay Ratepayers' Association and Another v Harrison and Another* [2010] ZACC 19; 2011 (4) SA 42 (CC); 2011 (2) BCLR 121 (CC) ("***Camps Bay***"); *Fuel Retailers Association of Southern Africa v Director-General: Environmental Management, Department of Agriculture, Conservation and Environment, Mpumalanga Province, and Others* [2007] ZACC 13; 2007 (6) SA 4 (CC); 2007 (10) BCLR 1059 (CC); and *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Others* [2004] ZACC 15; 2004 (4) SA 490 (CC); 2004 (7) BCLR 687 (CC).

[5] Section 172(1)(b) of the Constitution provides that "[w]hen dealing with a constitutional matter within its power, a court may make an order that is just and equitable".

[6] Rule 16A(1)(a) of the Uniform Rules of Court ("**Rules**").

[7] *De Lange v Presiding Bishop of the Methodist Church of Southern Africa for the time being and Another* [2015] ZACC 35; 2016 (1) BCLR 1 (CC); 2016 (2) SA 1 (CC) ("***De Lange***") at 64.

on undue urgency, the submissions raised by the Applicants for Admission are relevant to this matter, will assist the Court, and differ from the submissions of the other parties.[8]

3. In sum, the Applicants for Admission seek to present submissions in the following terms:

3.1. The Respondents have not followed a proper procedure in this matter. As set out in by the answering affidavit, the Respondents acknowledge that "they do not have the legislative powers to authorize the installation of cameras the use of which would infringe the right to privacy of individuals", which motivated the decision to suspend the issuing of the approvals that are now in dispute.[9] However, this acknowledgement equally impacts the unlawfulness of the previous approvals of wayleaves, in addition to any prospective approvals. The Constitutional Court in *Kirland* has confirmed that state respondents must apply to set aside unlawfully awarded approvals by way of formal counter-applications.[10] This has not been done in this case. Resultantly, the Applicants for Admission submit that there is a duty on the Respondents to seek to set aside previous wayleave applicants should the grant of those wayleave applications be considered to be unlawful. On the Applicant's version, this point is "novel"[11] and it is relevant to this Court's determination of what may constitute a just and equitable remedy in this matter. This basis alone supports the contention that the Applicants for Admission should be admitted as *amici curiae*.

[8] Rule 16A(6) of the Rules.
[7] Master Bundle, 009-15, para 3.8
[8] See *Kirland* above n 4.
[9] Master Bundle, 049-39, para 32.

3.2. <u>There is no enabling legal framework authorising bulk and indiscriminate CCTV video surveillance</u>. The Applicants for Admission submit that the reasoning of the Gauteng Division of the High Court, Pretoria in *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*,[12] pertaining to the need for lawful authority to trespass on privacy rights in relation to communications surveillance,[13] is apposite to video surveillance. Specifically, and in a similar vein to the present matter, the High Court declared that the bulk surveillance activities undertaken by the National Communications Centre were unlawful and invalid as there was no legal framework to permit such surveillance from taking place.[14] As a result of the absence of such an enabling legal framework, it is not be just and equitable for this Court to grant the relief sought by the Applicant in relation to the present wayleave applications, at this stage.

3.3. <u>An appropriate balance between privacy and security needs to be considered</u>. In this regard, the Applicants for Admission draw the Court's attention to various international and foreign law instruments which consider privacy, security and video surveillance which are relevant to this matter, particularly in relation to how the balance may be struck and what constitutes a reasonable expectation of privacy in public spaces. The Applicant argues that an individual who is recorded by CCTV video surveillance on public roads and in public areas "does not have an

[10] *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Corrections and Others* [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) 2020 (1) SACR 139 (GP) ("***amaBhungane***").
[11] Id at para 165.
[14] Id.

expectation of privacy".[15] This is plainly not the case and arguments contesting this averment are made by the Applicants for Admission.

4. The Applicant opposes the application for admission as *amici curiae ("**amici* **application**")**, with costs, contending that the Applicants for Admission do not have the requisite interest in this matter and that the submissions that they seek to advance are "irrelevant".[16] This is simply incorrect. The opposite is true: the Applicants for Admission have a direct interest in this matter and the submissions which they seek to advance are not "irrelevant" — but may be inconvenient to the Applicant. The inconvenient truth for the Applicant is that this is not a simple, "crisp issue"[17] as it alleges throughout its papers. It is a complex, constitutional issue which should be fully ventilated by the parties, including the Applicants for Admission.

5. The Respondents have neither consented nor opposed the admission of the Applicants for Admission in this *amici* application.

RULE 16A AND URGENCY

6. As indicated in the *amici* application, Rule 16A serves to facilitate the admission of *amici curiae* by providing courts with guidelines on how this should happen.[18] It is the "entry point for non-parties into public interest matters with constitutional ramifications".[19] Simply, Rule 16A(1)(a) requires any person "raising a constitutional issue in an

[15] Master Bundle, 049-45, para 54.
[16] Master Bundle, 049-38, para 29.
[17] Master Bundle, 049-31, para 5.
[18] *De Lange* above n 7 at 60.
[19] Id.

application or action" to give notice, which is to be made public and placed on a notice board. (Own emphasis.) The importance of the notice cannot be gainsaid: it notifies interested parties of public interest matters and invites them to seek consent to enter proceedings and play a role in the development of South Africa's constitutional jurisprudence.[20]

7. Following publication of the notice, interested parties may seek written consent to intervene in proceedings, provided that the submissions that they seek to advance are relevant, may assist the Court in its determination of the matter, and are different from the submissions of the other parties.[21] To the extent that consent is not received, interested parties may apply to a court for admission.[22] Importantly, a court may dispense of the requirements of Rule 16A, including the prescribed timeframes, if it is in the interests of justice to do so.[23]

8. The Applicants for Admission have complied with the substantive requirements for admission. However, as a result of the urgency of this matter, the timeframes stipulated in Rule 16A have not been complied with. The Applicants for Admission seek the Court to condone non-compliance with these timeframes as it is in the interests of justice for this Court to do.[24]

9. Despite the failure by the Applicant to file a notice and only being formally notified of this matter as a result of the publication of a notice by the Respondents on 17 July 2020.

---

[20] Master Bundle, 049-18, para 35.
[21] Rule 16A(6) of the Rules.
[22] Rule 16A(5) of the Rules.
[23] Rule 16A(9) of the Rules. See, also, *De Lange* above n 7 at 60.
[24] Id.

The Applicants for Admission have acted swiftly in order to properly engage in this matter. Despite the prejudice suffered as a result of the failure of the Applicant to file a notice, the Applicants for Admission have taken all reasonable steps to ensure compliance with Rule 16A — including briefly describing the interest of the *amici curiae* in the matter and setting out the submissions which the Applicants for Admission seek to advance.[25] It is submitted that any non-compliance with Rule 16A should be condoned.[26]

10. The urgency of this application is directly aligned to the conduct of the Applicant and the need for this application to be heard alongside the Main Application.[27] This is clearly a constitutional matter and it is arguable that the failure by the Applicant to file a notice has shut the door on other potential *amici* who may have wished to enrich this constitutional debate.[28] The Applicant's conduct should not also shut the door on the Applicants for Admission.

11. In its Responding Affidavit, the Applicant does not make out a case as to why it has failed to file a notice and its reliance on Rule 16A(9) and the "interests of justice" threshold is inappropriate.[29] Rule 16A(1)(A) is clear that "any person raising a constitutional issue" must give notice. To argue that this onus is discharged by the Respondents duly filing their notice is incorrect in law.[30]

---

[25] Rules 16A(6) of the Rules.
[26] Master Bundle, 049-19, at para 39.
[27] Master Bundle, 049-18, at para 36.
[28] *De Lange* above n 7 at 64.
[29] Master Bundle, 010-33, para 76.
[30] Master Bundle, 049-55, para 81.

12. It is, in fact, not in the interests of justice for this matter to proceed without a reasonable opportunity for *amici curiae* to apply for admission given the constitutional issues that are raised, even if such an opportunity is on reduced timeframes.[31] Alternatively, this Court may postpone this matter *sine die* until a notice is filed by the Applicant.[32] Either way, the Applicants for Admission have complied with Rule 16A and should be admitted as *amici curiae* in the interim.

THE ROLE OF *AMICI CURIAE* AND THEIR INTEREST

13. It is clear that this matter raises constitutional issues and thus invokes the domain of an *amicus curiae*.[33] It is also clear that the First Applicant is a public interest organisation and, alongside the Second Applicant, they seek to act in the public interest and have a direct interest in this matter. This is particularly so in relation to concerns around the right to privacy occasioned by CCTV video surveillance. However, the interest of the Applicants for Admission also relates to just administrative action, the lawful exercise of public power, and transparency in processes such as the award of wayleaves which relate to CCTV video surveillance,[34] inclusive of decisions on the "poles" that are used to support — and enable the use of — the CCTV video surveillance cameras.

14. It also bears reference that a complaint submitted by the Second Applicant for admission as an *amicus curiae* to the Ombudsman of the City of Johannesburg constitutes evidence before this Court in this matter.[35] This, and the interest of the Applicants for Admission

[31] Section 172(1)(b) of the Constitution.
[32] *De Lange* above n 7 at n 50. This approach was adopted by the court *a quo* in *Phillips v South African Reserve Bank and Others* [2012] ZASCA 38; 2013 (6) SA 450 (SCA); 2012 (7) BCLR 732 (SCA).
[33] Rule 16A(1)(a). See, also, n 4 above.
[34] Master Bundle, 049-12, para 14.
[35] Master Bundle, 009-113 onwards; 028-3 onwards.

in just administrative action regarding CCTV video surveillance, is uncontested by the Applicant. It is clear that the Applicants for Admission have an interest in this matter both in relation to the right to privacy and just administrative action.

15. In terms of the role of *amici curiae*, the Constitutional Court in *In Re: Certain Amicus Curiae Applications*[36] provides:

> "The role of an amicus is to draw the attention of the court to relevant matters of law and fact to which attention would not otherwise be drawn. In return for the privilege of participating in the proceedings without having to qualify as a party, an amicus has a special duty to the court. That duty is to provide cogent and helpful submissions that assist the court. The amicus must not repeat arguments already made but must raise new contentions; and generally, these new contentions must be raised on the data already before the court. Ordinarily it is inappropriate for an amicus to try to introduce new contentions based on fresh evidence."[37] (Own emphasis.)

16. The threshold identified by the Constitutional Court is four-fold: (1) the submissions by *amici* must draw a courts attention to relevant matters of law and fact to which attention would not otherwise be drawn; (2) the submissions must be cogent and helpful and assist the court; (3) the submissions must not repeat submissions already made; and (4) generally the submissions should be based on evidence already before the court. The submissions which the Applicants for Admission seek to advance meet this threshold. The threshold is not that the parties to the matter or the court must necessarily agree with submissions advanced by the *amici curiae*. Additionally, the threshold advanced by the

[36] *In Re: Certain Amicus Curiae Applications*; *Minister of Health and Others v Treatment Action Campaign and Others* [2002] ZACC 13.
[37] Id at para 5.

Applicant that it is the role of amicus to make a case for one or either of the parties or introduce new evidence is certainly not the threshold.[38]

17. The Respondents make the averment that CCTV video surveillance violates the right to privacy and the right to freedom of movement. The Applicant goes to great lengths to challenge this argument, both in its replying affidavit[39] in the Main Application and in its answering affidavit[40] in the *amici* application. The Applicants for Admission seek to draw this Court's attention to relevant matters pertaining to the right to privacy and just administrative action, which have not been brought to this Court's attention, and which will assist this Court in its determination of this matter. To this end, the Applicants for Admission have complied with Rule 16A and the threshold for admission, and should be admitted accordingly.

RELEVANT CONTEXT

18. Before turning to the specific arguments that the Applicants for Admission seek to advance, it is necessary to briefly describe the relevant context underpinning these arguments. At the crux of this matter is the widescale and indiscriminate infringement of the right to privacy through the CCTV video surveillance network that has been established by the Applicant. This is a key element of the Respondents' decision to refuse to grant the wayleaves, and underpins the submissions set out below.

[38] Master Bundle, 049-41, at para 42.
[39] Master Bundle, 010-21-29, at para 48-64.
[40] Master Bundle, 049-43-50, at para 48-59.

19. There are three key points to be highlighted in this regard. First, the interference of the right to privacy occurs from the moment of collection of information about a person, and continues through all phases of the processing of that personal information, including the use, sharing, storage and destruction of the personal information. This is consonant with the approach taken throughout the Protection of Personal Information Act[41] ("**POPIA**"), including in respect of the definition of "processing" contained in section 1 thereof. In the context of the Applicant's CCTV surveillance network, this interference takes place in a number of ways, including by collecting images, footage, location information, vehicle registration details and more. The CCTV surveillance network not only interferes with the right to privacy insofar as it collects images and footage of people, but also in respect of the daily activities in people's lives, such as who they visit and who visits them, when they travel to and from work, how frequently they leave their homes, and the activities in which they engage in their surrounding areas.

20. Second, the interference with the right to privacy arises irrespective of whether the affected person has knowledge thereof. As has been noted by the United Nations Special Rapporteur on Freedom of Expression:

> "Targets of surveillance suffer interference with their rights to privacy and freedom of opinion and expression whether the effort to monitor is successful or not. The target need have no knowledge of the attempted or successful intrusion for the interference with their right to privacy to be complete. Indeed, Governments generally seek tools that intrude without the knowledge of the target. However, it

[41] 4 of 2013.

> is critical to see such interference as part of an overall effort to impose consequences on the target."[42]

Furthermore, it is irrelevant in terms of POPIA whether the processing of personal information is done by automated or non-automated means;[43] even processing by automated means still constitutes an interference with the right to privacy.

21. Third, the role of private surveillance companies has been a persistent cause for concern; in this regard, the United Nations Special Rapporteur has noted that "digital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close to impunity."[44] As companies in the private surveillance industry typically operate under a cloak of secrecy, the public lacks meaningful information about the way in which they may — if at all —consider the human rights impacts of their products.[45]

22. It is by now well-established under international law that unlawful or arbitrary surveillance are "highly intrusive acts" that interfere with fundamental human rights, including the right to privacy.[46] This is a matter of such serious concern that the United Nations Special Rapporteur on Freedom of Expression has recommended to the Human Rights Council that states should impose "an immediate moratorium on the

---

[42] United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression ("**United Nations Special Rapporteur on Freedom of Expression**"), 'Report to the Human Rights Council: Surveillance and human rights', 28 May 2019, A/HRC/41/35, para 21.
[43] See, for instance, sections 1, 3 and 70 of POPIA.
[44] Id at para 6.
[45] Id at para 29.
[46] Id at para 1, with reference to United Nations General Assembly Resolutions 68/167 and 71/199.

export, sale, transfer, use or servicing or privately developed surveillance tools until a human rights-compliant safeguards regime is in place".[47]

23. The Applicants for Admission submit that it was therefore appropriate for the Respondents to have refused to grant the wayleaves to the Applicant in the present matter, as the interference with the right to privacy caused by the Applicant's CCTV surveillance network is of serious concern to the realisation of the right to privacy in South Africa, and particularly for the rights of each and every person who is — or will be — captured by the Applicant's CCTV video surveillance network.

I. THE DUTY ON THE RESPONDENTS TO REVIEW PREVIOUS UNLAWFUL CONDUCT

24. The Respondents argue in their answering affidavit that in terms of the present wayleave applications made by the Applicant they "do not have legislative powers to authorize such an infringement of privacy rights".[48] The Respondents go on further to argue that:

24.1. "[T]here is no policy and legislative framework or by-law framework for the City and JRA to consider and approve aerial and CCTV wayleave applications."[49]

24.2. "The by-laws and code of practice upon which Vumacam seeks to rely for this relief, does not empower JRA and the City to authorize the installation of

[47] Id at para 66(a).
[48] Master Bundle, 009-15, para 3.6.
[49] Master Bundle, 009-30, para 6.2.1.

> equipment the use of which is going to violate the right to privacy of a long list of unknown people."[50]

25. The Respondents further take the position that:

> "Even if Vumacam were to comply with all of the requirements agreed upon, it would still be unlawful for the JRA and the City to approve its applications due to the fact that such approval would authorize the installation and use of surveillance cameras which are going to result in the invasion of the right to privacy and the freedom of movement of private individuals."[51]

26. What the Respondents fail to do is deal with the 64 previous wayleave applications which were granted by the Respondents to the Applicant between October 2018 and April 2020.[52] It is apparent that if the Respondents accept — as they clearly do — that the grant of any prospective wayleaves will be unlawful, it follows that the grant of past wayleaves must be unlawful too. However, instead of acknowledging this as should properly have been done, the Respondents contradict themselves by saying that the award of the previous wayleaves "is a clear indication that the JRA does not seek to frustrate Vumacam and has always acted in good faith to assist Vumacam where possible".[53]

[50] Master Bundle, 009-31, para 6.5.3.
[51] Master Bundle, 009-32, para 6.5.6.
[52] Master Bundle, 001-18, para 41.1.
[53] Master Bundle, 009-55-56, para 13.16.

The *Kirland* decision

27. In *Kirland*,[54] the Constitutional Court held that:

> "PAJA requires that the government respondents should have applied to set aside the approval, by way of formal counter-application. They must do the same even if PAJA does not apply. To demand this of government is not to stymie it by forcing upon it a senseless formality. It is to insist on due process, from which there is no reason to exempt government. On the contrary, there is a higher duty on the state to respect the law, to fulfil procedural requirements and to tread respectfully when dealing with rights. Government is not an indigent or bewildered litigant, adrift on a sea of litigious uncertainty, to whom the courts must extend a procedure-circumventing lifeline. It is the Constitution's primary agent. It must do right, and it must do it properly."[55]

28. The Respondents, in this instance, are state entities and no different to the respondents referred to *Kirland*. On the one hand, they allege that rights violations may occur as a result of the successful grant of the present wayleave application. However, on the other, there is no evidence of the Respondents having taken any steps to seek to review and set aside the 64 previous wayleave applications, which were successfully awarded by the Respondents to the Applicant. The end result is that the rights violations complained of by the Respondents and the lack of an enabling legal framework persist, without any action whatsoever being taken by the Respondents to review their previous unlawful conduct. According to the Constitutional Court, the Respondents must do right, and they

[54] See above n 4.
[55] *Kirland* above n 4 at 82.

must do it properly.[56] That has not happened in this case, to the detriment of the fundamental rights of the broader public.

29. First in *Khumalo*[57] and then in *Gijima*,[58] the Constitutional Court has held that the principle of legality is the means through which an organ of state may seek to review its own decision.[59] In *Khumalo*, the Court confirmed that such a review should proceed without undue delay stating that:

> "Section 237 acknowledges the significance of timeous compliance with constitutional prescripts. It elevates expeditious and diligent compliance with constitutional duties to an obligation in itself. The principle is thus a requirement of legality.
>
> This requirement is based on sound judicial policy that includes an understanding of the strong public interest in both certainty and finality. People may base their actions on the assumption of the lawfulness of a particular decision and the undoing of the decision threatens a myriad of consequent actions."[60]

30. To the extent that the Respondents fail to stop the ongoing unlawful conduct and rights violations of their own volition, the Applicants for Admission submit that it would be both appropriate, as well as just and equitable, for this Court to pronounce on this issue, guided by the jurisprudence of the Constitutional Court set out above.

---

[56] Id.
[57] *Khumalo and Another v Member of the Executive Council for Education: KwaZulu Natal* [2013] ZACC 49; 2014 (3) BCLR 333 (CC); (2014) 35 ILJ 613 (CC); 2014 (5) SA 579 (CC) ("***Khumalo***").
[58] *State Information Technology Agency SOC Limited v Gijima Holdings (Pty) Limited* [2017] ZACC 40; 2018 (2) BCLR 240 (CC); 2018 (2) SA 23 (CC) ("***Gijima***").
[59] Id at paras 40-1.
[60] *Khumalo* above n 57 at paras 46-7.

II. THERE IS NO LAW AUTHORISING BULK AND INDISCRIMINATE CCTV VIDEO SURVEILLANCE

CCTV video surveillance and the right to privacy

31. In its CCTV Surveillance Policy ("**Surveillance Policy**"), the Applicant refers to the right to privacy on no less than seven occasions.[61] In doing so, it expressly provides that "Vumacam strives to ensure each individual's constitutional right to privacy" and "balance the privacy rights of individuals against other rights, particularly the rights of members of the general public to safety and security."[62] While the Applicants for Admission dispute the veracity of these statements, it is nevertheless clear that even the Applicant acknowledges its CCTV video surveillance network — akin to Bentham's Panopticon[63] — invokes the right to privacy.

32. In the present matter, the Applicant suggests that all that is to be considered by this Court is the administrative approval "to place a poll in the ground"[64] and that the "wayleaves authorise the construction of the poles for whatever purpose — not specifically for the purposes of using cameras."[65] This is too simply stated. On the Applicant's own version, the wayleaves are needed to expand the Applicant's video surveillance network.[66] The Applicant specifies no other purpose for the so-called "poles". The Respondents aver,

---

[61] Master Bundle, 009-68-75.
[62] Master Bundle, 009-69, at para 3.1.
[63] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stan. L. Rev. 1373, 1424.
[64] Master Bundle, 049-40, para 36.
[65] Master Bundle, 049-37, paras 23-4.
[66] Master Bundle, 001-31, para 67.7.

on multiple occasions, that the installation of the "equipment" "is going to violate the right to privacy".[67]

33. The wayleaves, and the cameras which are placed on the poles that they authorise, directly implicate the right to privacy of every person whose data is collected through the wide and indiscriminate network of the thousands of cameras of the Applicant. In this regard, the Applicant notes that the "CCTV surveillance network employs fixed cameras, designed and deployed to record images of individuals, as well as vehicle and vehicle registration plates, on public roads and in public spaces."[68] On the one hand, the Applicant directly states that it "does not infringe on privacy rights";[69] on the other, it goes on to acknowledge that there may be some infringement of the right to privacy, but suggests that the right to privacy is attenuated in public spaces.[70] The applicant further contends that it only plays a limited role in surveillance, and that it relies on artificial intelligence ("**AI**") to alert "someone" to assess surveillance footage of a member of the public.[71]

34. CCTV video surveillance clearly implicates — and may violate — the right to privacy and associated rights. The fact that CCTV video surveillance implicates the right to privacy and associated rights is an important context within which the Applicant's relief should be considered. This is so because the relief sought implicates the right to privacy and, as a result, an enabling legal framework should be in place before any further

[67] Master Bundle, 009-31, para 6.5.3.
[68] Master Bundle, 049-45, para 54.1.
[69] Master Bundle, 049-44, Para 50.
[70] Master Bundle, 049-46, para 55.
[71] Master Bundle, 049-43, para 49.

"poles", with operational CCTV video surveillance cameras affixed, are put in the ground.

35. It is important to note that the United Nations Human Rights Committee, in considering South Africa's Initial State Report in March 2016, held that:

> "The State party should take all necessary measures to ensure that its surveillance activities conform to its obligations under the [ICCPR], including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality. The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization and consider revoking or limiting the requirement for mandatory retention of data by third parties. It should also ensure that interception of communications by law enforcement and security services is carried out only on the basis of the law and under judicial supervision. The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies."[72] (Own emphasis.)

36. The position noted by the United Nations remains largely unchanged and it is within this context that this matter should be decided.

[72] Human Rights Committee, Concluding Observations on the Initial Report of South Africa, CCPR/C/ZAF/CO/1, 27 April 2016 at para 43.

Associated constitutional rights

37. It is also of relevance to this Court to note that video surveillance may have the effect of implicating a broad array of rights, which may extend beyond traditional notions of the right to privacy. These include, among others:

38. Freedom of association or associational privacy: Video surveillance implicates freedom of association[73] or "associational privacy". In this regard, the US Supreme Court has held that the "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[74] This, in turn, implicates freedom of expression.[75]

39. Freedom of movement or locational privacy: Video surveillance equally implicates freedom of movement.[76] This has been recognised by the Article 29 Working Party in their 2004 Opinion on the processing of personal data by means of video surveillance whereby it is stated that:

> "the right to free movement of individuals…is safeguarded by Article 2 of Additional Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms. This freedom of movement may only be subject to such restrictions as are necessary in a democratic society and proportionate to the achievement of specific purposes. Data subjects have

[73] Section 18 of the Constitution.
[74] *National Association for the Advancement of Colored People v. Alabama*, 357 U.S. 449 (1958).
[75] Section 16 of the Constitution.
[76] Section 21 of the Constitution.

> the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct as well as without being the subject of detailed monitoring such as to allow tracking their movement and/or triggering "alarms" based on software that automatically "interprets" an individual's supposedly suspicious conduct without any human intervention - on account of the disproportionate application of video surveillance by several entities in a number of public and/or publicly accessible premises."[77]

40. Best interests of the child: The Constitution mandates that a child's best interests are of paramount importance in all matters concerning the child.[78] Given the innate vulnerability of children, the Constitutional Court has recognised that children merit special protections that guard and enforce their rights and liberties.[79] With specific reference to the right to privacy, the Constitutional Court has held that the analysis of the right is even more pressing when dealing with children, including on the basis that the protection of the privacy of young persons fosters respect for dignity, personal integrity and autonomy.[80] In the present matter, the Applicant's CCTV surveillance network pays no heed to the privacy rights of children, and indiscriminately collects personal information about the children who may be caught the remit.

---

[77] Article 29 Data Protection Working Party, Opinion 4/2004 on the processing of personal data by means of video surveillance', 11750/02/EN, WP 89, 11 February 2004, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf

[78] Section 28(2) of the Constitution.

[79] *Teddy Bear Clinic for Abused Children v Minister of Justice and Constitutional Development* [2013] ZACC 35; 2014 (2) SA 168 (CC); 2013 (12) BCLR 1429 (CC) at para 1. In this regard, the Constitutional Court has explained that the principle of the best interests of the child acknowledges the importance for children to be free to form opinions, participate in their communities, and learn as they grow about how to conduct themselves. See *S v M* [2007] ZACC 18; 2008 (3) SA 232 (CC); 2007 (12) BCLR 1312 (CC) at para 19.

[80] *Centre for Child Law v Media 24 Limited* [2019] ZACC 46 at para 49.

41. A further point to consider is the impact of the Applicant's conduct on the right to equality and non-discrimination,[81] as well as the right to dignity.[82] In addition to the interplay with the right to privacy, this also gives rise to concern in the way in which the Applicant deploys its AI to "identify suspicious behaviour".[83] As explained by the United Nations Special Rapporteur on Racial Discrimination, "[a]s 'classification technologies that differentiate, rank and categorize', artificial intelligence systems are at their core 'systems of discrimination'".[84] Data sets, as a product of human design, can be biased due to skews, gaps and faulty assumptions, which have the potential to lead to discrimination against certain segments of the population based on race, ethnicity or gender.[85] Even where discrimination is not intended, indirect discrimination can result from using innocuous and genuinely relevant criteria that also operate as proxies for race and ethnicity.[86]

42. The Applicant provides no detail on how it identifies or categorises "suspicious behaviour". Practically, this can lead to various forms of discrimination, in violation of the rights to equality and dignity. While companies deploying AI may purport a commitment to human rights standards, the United Nations Special Rapporteur on Racial Discrimination notes that: "There is a genuine risk that corporations will reference human rights liberally for the public relations benefits of being seen to be ethical, even in the absence of meaningful interventions to operationalize human rights principles. Although references to human rights, and even to equality and non-discrimination, proliferate in

[81] Section 9 of the Constitution.
[82] Section 10 of the Constitution.
[83] Master Bundle, 010-22, para 50.3.
[84] United Nations Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance ("**United Nations Special Rapporteur on Racial Discrimination**"), 'Report to the Human Rights Council: Racial discrimination and emerging digital technologies: A human rights analysis', 18 June 2020, A/HRC/44/57, para 7.
[85] Id.
[86] Id at para 8.

corporate governance documents, these references alone do not ensure accountability."[87] The Special Rapporteur cautions further that: "From a human rights perspective, relying on companies to regulate themselves is a mistake, and an abdication of state responsibility."[88]

43. The Applicants for Admission therefore submit that the Respondents were rightly concerned about the grant of the further wayleaves to the Applicant, and — particularly in the absence of appropriate safeguards for the right to privacy and other associated rights — urges the Court to similarly refrain from permitting the Applicant to continue the roll-out of its CCTV video surveillance network.

The *amaBhungane* decision and private power

44. It is trite that the exercise of all public power is constrained by the principle of legality.[89] The Constitutional Court in *AAA Investments* and *Allpay II* has also recognised that private actors are increasingly being used to perform state functions,[90] and can exercise public power.[91] It is arguable that this is the case here. The Applicant's CCTV video surveillance function — or what is referred to as the "Vumcam solution" by the South

[87] Id at para 61.
[88] Id at para 62.
[89] See *AAA Investments (Proprietary) Limited v Micro Finance Regulatory Council and Another* [2006] ZACC 9; 2006 (11) BCLR 1255 (CC); 2007 (1) SA 343 (CC) at para 39 ("***AAA Investments***").
[90] Id at para 22.
[91] *Allpay Consolidated Investment Holdings (Pty) Ltd and Others v Chief Executive Officer of the South African Social Security Agency and Others* (No 2) [2014] ZACC 12; 2014 (6) BCLR 641 (CC); 2014 (4) SA 179 (CC) at para 54 ("***Allpay II***"). In *Allpay II* at paras 52-53, the Constitutional Court stated that: "When Cash Paymaster concluded the contract for the rendering of public services, it too became accountable to the people of South Africa in relation to the public power it acquired and the public function it performs. This does not mean that its entire commercial operation suddenly becomes open to public scrutiny. But the commercial part dependent on, or derived from, the performance of public functions is subject to public scrutiny, both in its operational and financial aspects."

African Police Service[92] ("**SAPS**") — constitutes, at least in part, an attempt to compliment and even perform the constitutional function of the SAPS[93] and thus constitutes the exercise of public power. If this is not the case, the Constitutional Court in *Juma Masjid*[94] has confirmed that private parties, such as the Applicant, have a negative obligation "not to interfere with or diminish the enjoyment of a right".[95] This obligation devolves from section 8(2) of the Constitution.[96] The same obligation rests with all organs of state, including the Respondents in this matter.[97]

45. With further reference to the principle of legality, a right in the Bill of Rights may only be limited by a law of general application.[98] It has been explained that the principle of legality requires that states specify clearly and concretely in the law the actual limitations to the exercise of rights in order to enable the public to know in advance what is permissible and what the consequences are of disobedience.[99] In the present matter, however, there is simply no law authorising the bulk and indiscriminate surveillance currently being undertaken by the Applicant, which it seeks to expand through the grant of the additional wayleaves.

---

[92] Master Bundle, 001-91.
[93] See section 205(3) of the Constitution which provides that "[t]he objects of the police service are to prevent, combat and investigate crime, to maintain public order, to protect and secure the inhabitants of the Republic and their property, and to uphold and enforce the law. See further section 239 of the Constitution which defines an "organ of state" as "any other functionary or institution exercising a power or performing a function in terms of the Constitution".
[94] *Governing Body of the Juma Musjid Primary School & Others v Essay N.O. and Others* [2011] ZACC 13; 2011 (8) BCLR 761 at para 58 ("***Juma Musjid***").
[95] Id at para 58.
[96] Section 8(2) of the Constitution provides that: "[a] provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right."
[97] Section 8(1) of the Constitution.
[98] Section 36(1) of the Constitution.
[99] *Chimakure v Attorney-General of Zimbabwe*, Constitutional Court of Zimbabwe, Constitutional Application No SC 247/09 (2014) at paras 24-6.

46. In *amaBhungane*,[100] the Gauteng Division was asked to consider, among other things, the lawfulness of bulk communication surveillance.[101] In doing so, the Court reaffirmed that all public power must be authorised by law.[102] Similar to this matter, the need for public power to be authorised by law is uncontested. In terms of bulk communication surveillance, the Court held that absent an enabling law, bulk communications surveillance was unlawful and invalid. In doing so, the Court held:

> "Accordingly, in my view, no lawful authority has been demonstrated to trespass onto the privacy rights or the freedom of expression rights of anyone, including South Africans, whose communications criss-cross the world by means of bulk interception. A declaratory order to that effect is appropriate."[103] (Own emphasis.)

47. *amaBhungane*, which is presently before the Constitutional Court seeking confirmation, is relevant to this matter. As with bulk communications surveillance, bulk and indiscriminate video surveillance is wholly unregulated and equally intrudes on privacy and associated rights. In the absence of an enabling legal framework which expressly authorises video surveillance, such activities should under no circumstances be permitted to take.

48. As an side, the Applicant seeks to suggest that it complies with POPIA. Whether or not the Respondent complies with POPIA is irrelevant to the question of whether the Respondents can lawfully grant the wayleaves. Neither the Applicant nor the Respondents is empowered in law, including in terms of POPIA, to conduct mass

[100] See above n 10.
[101] Id at paras 143-66.
[102] Id at para 147.
[103] Id at para 165.

surveillance. This includes the power to grant wayleaves which enable video surveillance. In any event, given that the substantive provisions of POPIA only become enforceable from 1 July 2021, there can be no argument that POPIA can be relied on either at present or in the past to have authorised the Applicant's CCTV surveillance network.

49. The Applicant alleges that "[t]here is no need for positive law specially authorising Vumacam to operate a CCTV network"[104] and that "there is no requirement that the activities of a private party be empowered by law."[105] If this Court accepts that Vumacam performs a public function and thus exercises public power, it is plain that an enabling legal framework, which does exist, is necessary and the relief sought by the Applicant cannot be awarded, at this stage.

The Applicants for Admission submit that, given the lack of an empowering legal framework, as well as the obligation on the Applicant and the Respondent to respect the right to privacy and other rights in the Bill of Rights, the Court may be cautious to award the relief sought by the Applicant in the present matter.[106]

III. STRIKING THE APPROPRIATE BALANCE BETWEEN PRIVACY AND SECURITY IN PUBLIC SPACES

50. The right to privacy and the interests of security are not necessarily opposed. To the contrary, security interests can indeed be pursued, subject to the requirements that they

[104] Master Bundle, 049-52, para 65.
[105] Master Bundle, 049-51, para 64.2.
[106] See, for example, Venice Commission Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection, 430/2007, 8 June 2007 ("**Venice Commission Opinion**").

are provided for in law, and are necessary and proportionate in a democratic society. Furthermore, to the extent that security measures are implemented that implicate the right to privacy and other associated rights, such measures must contain appropriate safeguards to protect against the unjustifiable infringement of rights.

51. In the Surveillance Policy, the Applicant expressly acknowledges the need to balance privacy and security.[107] However, in the Main Application, the Applicant is unwilling to acknowledge this balance and focuses only on security, going as far as to say that an individual who is recorded by CCTV video surveillance on public roads and in public areas "does not have an expectation of privacy."[108] This is incorrect; the right may be "attenuated",[109] but it does not cease to exist.

52. South African courts have interpreted the right to privacy broadly. For example, the Constitutional Court has defined the right to privacy as "the right of a person to live his or her life as he or she pleases."[110] Indeed, as "a person moves into communal relations and activity, such as business and social interaction, the scope of personal space shrinks accordingly."[111] However, personal space includes the way in which we "live our daily lives,"[112] and "when people are in their offices, in their cars or on mobile telephones they still retain a right to be left alone by the state unless certain conditions are satisfied."[113] Importantly, the Constitutional Court in *Bernstein* held that the right to privacy will be

---

[107] See above n 62.
[108] Master Bundle, 049-45, para 54.
[109] Master Bundle, 049-46, para 55.
[110] *NM and Others v Smith and Others* [2007] ZACC 6; 2007 (5) SA 250 (CC); 2007 (7) BCLR 751 (CC) at para 33.
[111] *Bernstein and Others v Bester NO and Others* [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (CC) at para 67 ("***Bernstein***").
[112] *NM* above n 110 at para 130.
[113] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* [2000] ZACC 12; 2001 (1) SA 545 (CC) at para 16.

protected where a person has a subjective expectation of privacy that society considers to be objectively reasonable.[114]

53. In this regard, the European Court of Human Rights has held that "the notion of 'private life' may include professional activities or activities taking place in a public context … There is a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'".[115] In a joint concurring opinion in the same judgment, it was noted that "[a]n important aspect of the right to respect for private life is the 'right to live privately, away from unwanted attention'".[116] Notably, it was explained that the right to privacy "also guarantees the development, without outside interference, of the personality of each individual in his or her relations with other human beings."[117]

54. In *PG and Another v United Kingdom*, the European Court, in considering the right to privacy as contained in article 8 of the European Convention on Human Rights, explained the position as follows: [118]

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not

[114] *Bernstein* above n 111 at 75.
[115] *Antovic and Another v Montenegro*, European Court of Human Rights: Second Section, Application No. 70838/13 at para 42.
[116] Id at para 3 of the Joint Concurring Opinion.
[117] Id at para 4 of the Joint Concurring Opinion.
[118] European Court of Human Rights: Third Section, Application No. 44787/98 at para 57.

> necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method".

55. In relation to the Applicant's CCTV video surveillance network, persons are subjected to persistent and continuing surveillance in all public spaces as a result of the surveillance network, without any enabling legal framework, effective oversight or appropriate safeguards. This is starkly different from other, less intrusive, forms of crime prevention measures that do not risk the mass collection, retention, storage, sale and distribution of information about every person that is observed. More so, the "excessive psychological conditioning" which may be occasioned by such a network may have the effect of violating other rights, such as the right to freedom of movement and the right to freedom of association.[119] This network is exactly what the Applicant seeks to establish, and to continuously expand.[120]

56. While the Applicant seeks to argue that it has safeguarded the right to privacy by voluntarily complying with POPIA, this raises a litany of concerns:

---

[119] See above n 77.
[120] Master Bundle, 001-29, para 66.2.

56.1. Given that the substantive provisions of POPIA are only enforceable from 1 July 2021, it is currently not possible for an affected person to seek recourse for any privacy violations in terms of that legislation.

56.2. The Applicant is scant on detail regarding how personal information will be processed, stored and shared.

56.3. While the Applicant indicates that it the real-time surveillance services to "pre-vetted and pre-approved companies providing security services",[121] this determination is made at the sole discretion of the Applicant, with little to no oversight of how the information will be used by such third parties, and underpinned by the Applicant's own commercial motivation in the dissemination of this information.

56.4. While "[d]ata from Vumacam's system may only be accessed with Vumacam's express prior written consent", the affected persons whose personal information is being collected, stored and shared – the majority of whom will be innocent persons caught in the surveillance net – are not similarly afforded the opportunity to consent to their personal information being accessed, and are not provided with any prospect of opting out.

56.5. Affected persons are not notified if their personal information has been accessed, used or shared, rendering them unable to challenge such actions.

[121] Master Bundle, 010-22, para 50.1.

57. For these reasons, and in addition to the lack of an enabling framework, this Court should refrain from granting the relief sought by the Applicant.

CONCLUSION

58. For the reasons set out above, it is submitted that the Applicant for Admission should be admitted as *amici curiae* in the Main Application, and that the submissions made by the Applicants for Admission should be considered by the Court in reaching its determination and making a just and equitable order.

59. As set out above, the Applicant has opposed the *amici* application, and the Respondents have provided no response. The Applicants for Admission submit that, in the event that they are admitted by the Court, they are entitled to costs. To the extent that the Applicants for Admission are unsuccessful in the *amici* application, no costs order should flow given that the Applicants for Admission have sought through this application to vindicate the constitutional rights referred to above.[122]

MICHAEL POWER
AVANI SINGH
Attorneys with Right of Appearance
Rosebank, Johannesburg, 25 July 2020

[122] See *Biowatch Trust v Registrar Genetic Resources and Others* [2009] ZACC 14; 2009 (6) SA 232 (CC); 2009 (10) BCLR 1014 (CC) at 17-8 ("***Biowatch***") and *Lawyers for Human Rights v Minister in the Presidency and Others* [2016] ZACC 45; 2017 (1) SA 645 (CC); 2017 (4) BCLR 445 (CC).

TABLE OF AUTHORITIES

South African cases

In Re: Certain Amicus Curiae Applications; Minister of Health and Others v Treatment Action Campaign and Others [2002] ZACC 13

Lawyers for Human Rights v Minister in the Presidency and Others [2016] ZACC 45; 2017 (1) SA 645 (CC); 2017 (4) BCLR 445 (CC)

MEC for Health, Eastern Cape and Another v Kirland Investments (Pty) Ltd [2014] ZACC 6; 2014 (5) BCLR 547 (CC); 2014 (3) SA 481 (CC)

NM and Others v Smith and Others [2007] ZACC 6; 2007 (5) SA 250 (CC); 2007 (7) BCLR 751 (CC)

Phillips v South African Reserve Bank and Others [2012] ZASCA 38; 2013 (6) SA 450 (SCA); 2012 (7) BCLR 732 (SCA)

S v M [2007] ZACC 18; 2008 (3) SA 232 (CC); 2007 (12) BCLR 1312 (CC)

State Information Technology Agency SOC Limited v Gijima Holdings (Pty) Limited [2017] ZACC 40; 2018 (2) BCLR 240 (CC); 2018 (2) SA 23 (CC)

Teddy Bear Clinic for Abused Children v Minister of Justice and Constitutional Development [2013] ZACC 35; 2014 (2) SA 168 (CC); 2013 (12) BCLR 1429 (CC)

Foreign cases

Antovic and Another v Montenegro, European Court of Human Rights: Second Section, Application No. 70838/13

Chimakure v Attorney-General of Zimbabwe, Constitutional Court of Zimbabwe, Constitutional Application No SC 247/09 (2014)

National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).

PG and Another v United Kingdom, European Court of Human Rights: Third Section, Application No. 44787/98

Additional resources

Article 29 Data Protection Working Party, Opinion 4/2004 on the processing of personal data by means of video surveillance', 11750/02/EN, WP 89, 11 February 2004

Human Rights Committee, Concluding Observations on the Initial Report of South Africa, CCPR/C/ZAF/CO/1, 27 April 2016

International Association of Chiefs of Police, Privacy Impact Assessment Report for the Utilization of License Plate Readers, September 2009.

Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stan. L. Rev. 1373, 1424

United Nations Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, 'Report to the Human Rights Council: Racial discrimination and emerging digital technologies: A human rights analysis', 18 June 2020, A/HRC/44/57, para 7.

United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Report to the Human Rights Council: Surveillance and human rights', 28 May 2019, A/HRC/41/35.

Venice Commission Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection, 430/2007, 8 June 2007.