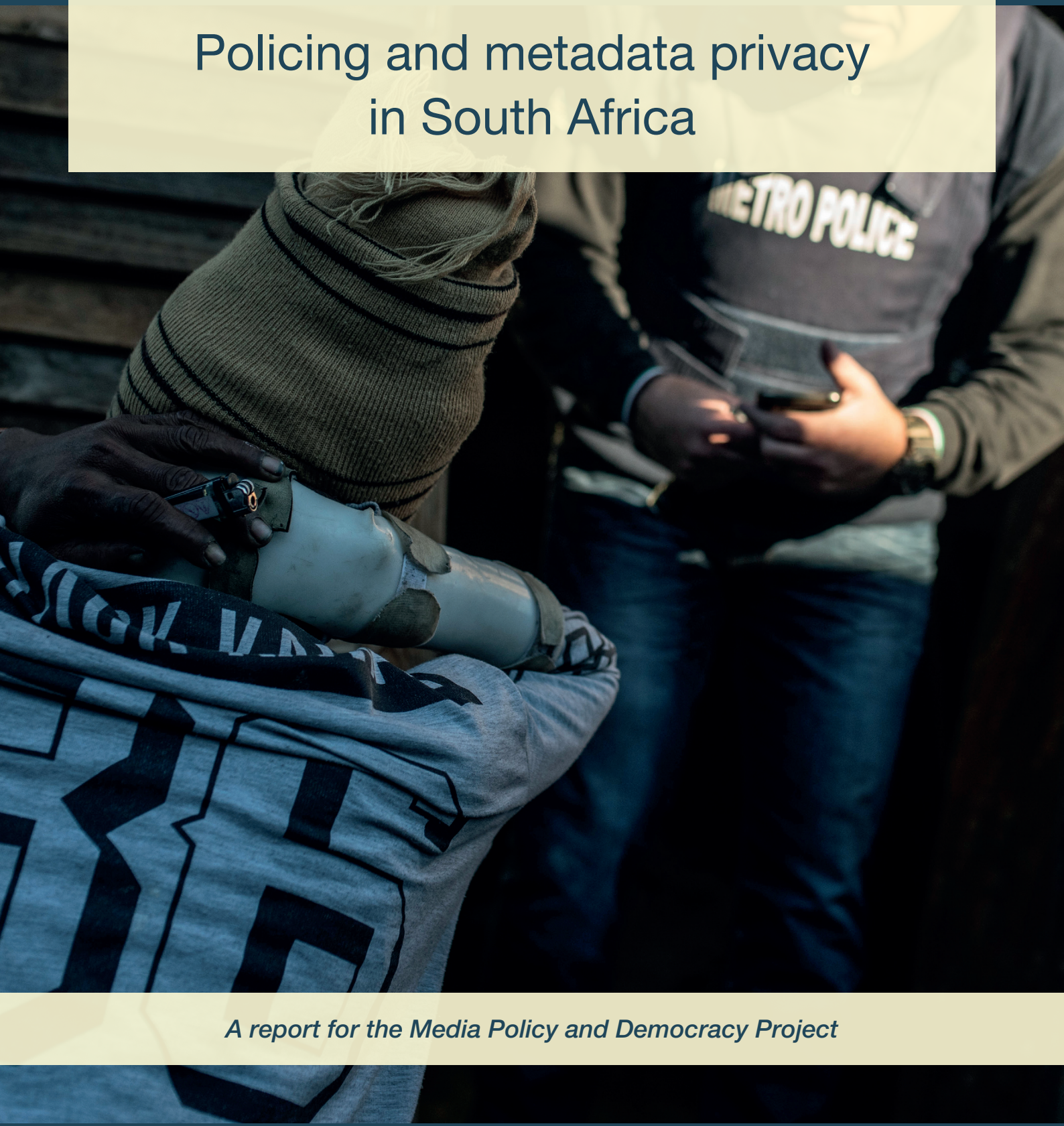
Cops and call records

Policing and metadata privacy in South Africa



A report for the Media Policy and Democracy Project

Murray Hunter

Cops and call records:

Perspectives on privacy, policing and metadata in South Africa

A report for the Media Policy and Democracy Project

Privacy laws often disregard the sensitivity of communication metadata – information about who a person communicates with, and how, where and when they do it. Yet this information often reveals as much or about that person, than the contents of the communication itself.

Certainly South Africa's laws have disregarded metadata privacy. While the weaknesses in the main surveillance law, RICA, face growing criticism, most police investigations of people's communications use a separate avenue: the 'Section 205' procedure, which allow the police to seize a person's phone records or other communications metadata, with few safeguards or limits.

This research draws on interviews with current and former law enforcement officials, to assess how police use these 'Section 205' metadata requests, and to sketch out possible reform options that would increase privacy protections for communication metadata.

While security officials have publicly painted reform proposals as being fatal to policing, these interviews show a surprising diversity of views within law enforcement structures, and map out some of the terrain for possible reforms.

Murray Hunter

murray@c1rcleup.org

March 2020

The author wishes to acknowledge the assistance of Michael Bishop, Caryn Dolley, Jane Duncan, Andrew Faull, Simone Haysom, Irvin Kinnes, Gareth Newham, Karabo Rajuili, Peter Schmitz, Heidi Swart, and all current and former law enforcement officials who participated in interviews.

Cover image by Shaun Swingler | shaunswingler.com

Contents

Introduction 2

Purpose of this research 5

The privacy case for metadata 8

The legal framework for surveillance 10

The RICA procedures 10

The transparency critique of RICA 11

The metadata critique of RICA 12

The Section 205 procedures 13

How the process works 15

Police perspectives on metadata use 18

Corroborating evidence or refuting alibis 19

Mapping criminal networks 20

Tracing suspects 20

The use of 'tower' records 21

Different structures, different picture 22

Formal and informal checks on the system 23

Police perspectives on reforms 25

Limiting its use 26

User Notification 27

Raising the bar for Section 205 requests 29

Reducing or ending the mandatory storage of metadata 30

Reporting requirements and oversight measures 32

Prospects for metadata reform 33

The policing case for surveillance reform 35

Citations 38

1 Introduction

It is common cause that South Africans worry about crime: surveys suggest that it comes second only to unemployment among South Africans' greatest social concerns.[1] There is less consideration, however, for how South Africans feel about privacy.[2] Yet a global survey in 2018 found that South Africans are significantly more likely to have growing privacy concerns than the citizens of many other countries: 68% of South Africans polled said they were more concerned about their online privacy than they had been the year before. Of 24 countries polled, only respondents in Egypt and India had higher levels of growing concern. In the same poll, 64% cited their own government as a contributing source of their concern.[3]

The laws and practices governing the interception of communication in South Africa have come under growing criticism. Much of this has focused on the law known as RICA,[4] the main law that governs when and how the state can intercept a person's communications.

In late 2019, the Gauteng High Court struck down key parts of RICA as being an affront to the constitutional right to privacy.[5] The facts in the *amaBhungane* case stemmed from the discovery by journalist Sam Sole that state agents had monitored his phone line for at least six months, listening in on his calls and messages with confidential sources, colleagues and

1 'The Quality of Democracy and Governance in South Africa', Afrobarometer Round 7.
2 See Duncan, *Stopping the Spies*, 89.
3 CIGI-Ipsos, '2018 CIGI-Ipsos Global Survey on Internet Security and Trust'.
4 RICA is a necessary abbreviation for the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.
5 *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) (16 September 2019).

loved ones – and the extent to which this infringed on media freedom and privacy. The case was heard in the High Court against a growing body of research, journalism and activism responding to evidence of surveillance abuses by factional elites in the South African state – as well as a damning Presidential policy review on dysfunction and criminality in the State Security Agency.[6] The case also echoed ongoing international debates seeking to realign laws and norms to protect privacy and human rights in the face of growing technological, political and legal threats. As this paper was submitted for publication, the *amaBhungane* matter was due for final consideration in the Constitutional Court: unless the justices decide to overturn the High Court's earlier ruling, it would set in motion a significant reform of the RICA law.

However, the vast bulk of state interceptions of communications data will not be affected by the outcome in the *amaBhungane* case*,* because they flow from a separate legal avenue than RICA: Section 205 of the Criminal Procedure Act, which enables a police investigator to seize a person's phone records through an order from the lower courts.

This is because South Africa's law, like many of its global equivalents, treats some kinds of communications data as being more sensitive than others. RICA creates a distinction between communication *content* and communication *metadata* (or what RICA calls 'communication-related information'). In the stereotypical definition, 'content' would be what is *said* in a call or message, and metadata would be any information *about* the communication – an index of who communicated with whom, when, where, over what devices, and so on.[7] As the state's responding papers in the *amaBhungane* case showed, there is an underpinning assumption that communications metadata is less sensitive or private than the content of the communications itself – and thus, subject to fewer safeguards. As argued below, this assumption does not withstand much scrutiny.

While RICA has been hammered for its lack of privacy protections, Section 205 fares much worse. As detailed below, 'RICA' procedures generally provide for live interceptions of the contents of calls and messages, which are mostly limited to investigations of serious crimes, and which need the approval of a senior judge; 'Section 205' procedures grant investigators access to years of a person's communication records, for even low-level offences, with the approval of the most junior magistrate.

7 A leaked policy document of the United Kingdom's Government Communications Headquarters, or GCHQ, gives some insight into how state agencies may classify different categories of communications data. By GCHQ policy, examples of 'content' include the contents of a call, email or message, any attachments or the file names of attachments, any key strokes, and contents of address books. Examples of 'metadata' include the identity of senders or receivers of messages, locational information, device information, time and duration of communication, and details of websites visited. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHd8b5.dir/doc.pdf

The quality of the safeguards matters. One pattern that has emerged from documented spying abuses in South Africa shows that investigators and intelligence operatives have used weaknesses in the oversight procedures to secure bogus warrants to spy on their adversaries: a judge may sign off on an interception warrant for an investigation of racketeering or a burglary syndicate, not realising that the supplied phone numbers belong to a journalist, or a public official, or even another police member.[8] Two cases have come to light where the Section 205 procedures have been abused in this manner:

In the Western Cape, a former Captain in the SAPS Crime Intelligence Division named Paul Scheepers faces criminal charges for, among other things, allegedly using Section 205 procedures to fraudulently seize the phone records of nearly 40 people, including senior police officials, lawyers, a government regulator and some private citizens. According to court records, in each instance the Section 205 application purported to be for an investigation of a regular offence, including house robbery and intimidation case.[9] Scheepers was moonlighting as a private investigator at the time.

In Gauteng, journalist Athandiwe Saba learned that a police officer had fraudulently acquired her cell phone records using a Section 205 order, apparently on behalf of a private investigator working for a public official she had investigated.[10] A copy of the magistrate's order shows that the police officer compelled Saba's mobile network operator to hand over a log of all incoming and outgoing calls and text messages, as well as location data, over six months. The order also shows that the police official claimed that Saba's numbers belonged to a suspect in a housebreaking investigation.[11]

Such brazen abuses illustrate why safeguards matter.[12] However, the safeguards matter even when the targets are not high-profile public-interest actors – including in legitimate investigations where the targets are legitimately suspected of wrongdoing. South Africa's Constitution and its undertakings in international law require that an infringement of a person's rights, including the right to privacy, can only be justified if tested against principles of necessity, proportionality and protection of human rights.[13]

8 See, for example, Duncan, 'Communications Surveillance in South Africa: The Case of the Sunday Times Newspaper'.
9 *S v Scheepers*.
10 Hunter and Smith, 'Spooked', 15–16.
11 Pinetown Magistrate Court, M201/08/2016.
12 For the purposes of contemplating safeguards, it should be added that both the Scheepers and Saba cases were discovered through happenstance: the Saba case came to light when her phone records were discovered in an unrelated investigation of the public official who paid to have her spied on, and Scheepers' use of Section 205 procedures was reportedly discovered during an internal probe of his 'moonlighting' as a private investigator.
13 Constitution of the Republic of South Africa, sec. 36.

Purpose of this research

The 2013 disclosures by whistleblower Edward Snowden sounded a global warning on the urgency for new legal, political and technological protections of privacy in an era of unprecedented surveillance potential. Among other efforts, an international group of civil society bodies and experts developed the 13 'Necessary and Proportionate' principles, a set of which were introduced to the United Nations Human Rights Committee to offer a framework for modern communications surveillance laws and practices to align with human rights protections.[14]

This research explores the perspectives of police investigators and prosecutors to assess how Section 205 metadata requests are used in policing, and to draw on their insights to assess the prospects for reform. Several factors inform the importance of these questions. Firstly, the volume of Section 205 requests for metadata show that it is by far the biggest documented surveillance 'tool' used by the state – and deserving of more scrutiny in the context of growing concerns about communications surveillance in South Africa. While government and judicial bodies do not appear to track the use of Section 205 procedures, statistics released by South Africa's mobile network operators show that authorities invoke 'Section 205' much more frequently than they do RICA – with as many as 1,000 subpoenas being issued to network providers every week:

	2015	2016	2017	2018
Vodacom	19 614	18 594	19 580	22 690
MTN	25 808	23 762	29 749	Not provided
Cell C	5 786	6 455	5 733	Not provided
Telkom	1 189	1 450	1 611	Not provided

Table 1: Total number of Section 205 subpoenas received by each network provider.
Source: Responses to PAIA requests by author, 2018

14 International Principles on the Application of Human Rights to Communications Surveillance.

		2015	2016	2017	2018
Section 7	(verbal request for content)	0	1	1	0
Section 8	(verbal request for location)	405	403	349	720
Section 11	(RICA only)[15]	43	49	22	30
Section 16	(real-time intercept of content)	189	178	205	230
Section 17	(real-time intercept of metadata)	150	148	166	190
Section 18	(real-time intercept of content and metadata, and access to archived metadata)	149	147	166	190
Section 19	(access to archived metadata)	148	149	166	190
Section 21	(entry warrant)	0	0	0	0

Table 2: Number of RICA interception directions received by Vodacom, by category. Note that some of the subtotals here may represent 'double-counting'.
Source: Response to PAIA request by author, 2018 (The other service providers refused similar requests.)

Secondly, the privacy victory in the *amaBhungane* case may well *raise* the privacy risks associated with Section 205 of the Criminal Procedure Act: if Section 205 procedures are left intact, any new transparency and oversight safeguards in RICA procedures may simply drive more investigators to use the less cumbersome procedures in Section 205. Raising the protections against one intrusive measure may simply invite more investigators to seek out intrusive measures with fewer protections. Thirdly, in the event that lawmakers do seek to reform the Section 205 procedures – which the Department of Justice and Correctional Services has undertaken to do, albeit only in the face of critique[16] – a better understanding of how law enforcement actors use Section 205 metadata requests is vital to sketching out the options for reform.

Perhaps unsurprisingly, even where they admit to shortcomings in the current surveillance regimen, policymakers and law-enforcement actors have voiced genuine concerns that privacy-oriented reforms could have a negative effect on policing. While this follows the time-worn path of practically every privacy debate in the world, the sheer volume of Section 205 subpoenas being sent to network providers does suggest that any reforms to limit use of this tool will indeed have an impact on policing – although whether positive or negative is up

15 This category was provided by Vodacom but it is not clear what type of request it refers to.
16 Author's correspondence with Department of Justice and Constitutional Development.

for debate. A reform process would have a better chance of success where there is some level of buy-in from law-enforcement actors, and where the reform measures are designed to provide appropriate protections against abuse, without creating unreasonable burdens or delays that frustrate legitimate policing or encourage investigators to seek out new loopholes.

This research draws on interviews with *seven* current and former investigators and *two* senior prosecutors, to test some of the common (and competing) assumptions of privacy advocates and police leadership against the perspectives of those who make regular use of Section 205 requests for metadata. By assessing the views of law-enforcement actors, it aims to sketch out possible avenues to protect metadata privacy from within the ranks of law-enforcement agencies.

The respondents who agreed to interviews for this research[17] come from a range of structures and ranks within law enforcement, offering a blend of perspectives and experiences:

- A former senior police investigator, with the rank of Major General, from the Directorate for Priority Crime Investigation (DPCI), commonly known as the 'Hawks', specialising in investigations of organised crime and racketeering.
- A former senior digital forensics investigator with more than a decade of experience at the Special Investigating Unit (SIU).
- Four station-level detectives with decades of combined experience in investigating serious and violent crime, including murder, 'trio crimes' (home robberies, business robberies and hijacking), and fraud.
- A former SAPS station manager, with the rank of Lieutenant Colonel.
- Two State Advocates with the National Prosecuting Authority, with several decades' combined experience in prosecutions of murder, serious commercial crime and corruption-related offences – as well as oversight of Section 205 requests.

While this research focuses on one avenue for the state to access communication metadata, the question of metadata protection is likely to become ever more relevant. Although previous research and journalism has detailed various advanced interception technologies being used, sought or procured by SAPS and the intelligence agencies, this research suggests that the majority of 'conventional' police use of communications data is still focused on cellular and telephonic data. Interviews and document research also give a strong sense that the

17 Several requests were made to a SAPS provincial Research Unit for the institution to authorise members to participate in this research, with no response.

police's use of communications data is often constrained as much by (lack of) capacity as by law or organisation culture. However, if the state's technical capabilities grow, these same questions will apply to more types of communications data, and more often – including more digital messaging data, internet browsing data, social media data, and data acquired through remote hacking.

The privacy case for metadata

While RICA, like many of its international equivalents, treats metadata as being less sensitive than content, this logic seems increasingly out of step with technological and practical realities. In a 2014 report, the UN High Commissioner for Human Rights argued that:

> *The aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.*[18]

As the ACLU put it:

> *Metadata can reveal who we are, who we know, what we do and care about and plan to do next – essentially the same spectrum of sensitive information that could also be contained in the contents of a communication.*[19]

In some instances, communication metadata is inherently sensitive, revealing intimate details of a person's life.[20] With no further analysis, for example, locational information from a person's cell phone data would reveal where they sleep at night and who they visit during the day; whether they stop in at a temple or a clinic or a political meeting and for how long. Their call records would reveal much about their associations and activities: who they communicate with and for how long, and how regularly they speak with a labour lawyer or a debt counsellor or make late-night calls to someone who is not their spouse.

Yet even when metadata may seem less sensitive when viewed as individual data points, the modern era of 'Big Data' capabilities is defined by technologies which draw together seemingly innocuous data points to infer the most intimate truths about a person's activities,

18 UN High Commissioner on Human Rights, 'The Right to Privacy in the Digital Age', para. 19.
19 ACLU of California, 'Metadata: Piecing Together a Privacy Solution', 5.
20 ACLU of California, 'Metadata', 5.

beliefs and personal characteristics.[21] Indeed, one of the features that gives communications metadata such intrusive potential is that it is much more readily and cheaply stored and analysed in bulk than the content of any communication. The European Court of Human Rights summed this up on a case concerning metadata retention in the EU:

> *In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with ...*[22]

The irrationality of giving different tiers of privacy protection to 'content' and 'metadata' is further complicated by the reality that in many instances, no clear technical distinction can be made. Certain types of communication data are both 'metadata' and 'content' at the same time: the subject line of an email, or the address of a website in someone's browsing history, for example.[23]

In short, metadata privacy matters.

21 ACLU of California, 'Metadata', 7.
22 *Big Brother Watch and Others v The United Kingdom* [2018] ECHR 722 paragraph 356.
23 ACLU of California.

2 The legal framework for surveillance

In broad terms, the primary law governing the interception of communication in South Africa is the RICA Act, although several other laws enable the authorities to seize a person's communication records through subpoena.[24] Although RICA has already suffered a good deal of criticism elsewhere,[25] it is necessary to unpack the workings of both RICA and Section 205 interceptions, and some of the key critiques against each of them.

The RICA procedures

In broad terms, RICA provides that the state may only intercept a person's communications or communication data for high-level policing and security functions, and only with the approval of a specially appointed judge (colloquially, the 'RICA judge'). The list of serious offences for which interception may be sought includes violent offences (any which could result in someone's death), those stemming from organised crime and racketeering, and crimes against the state such as treason or terrorism. For the intelligence agencies specifically, RICA also allows for interception on vaguer intelligence-gathering grounds, as such as threats to national security, or 'compelling national economic interests of the Republic'.[26] Only relatively

24 Aside from Section 205 of the Criminal Procedure Act, the Public Protector has used subpoena powers under Section 7(4) of the Public Protector Act to seize phone records, and investigators in the Special Investigating Unit have similarly used Section 5(2) of the Special Investigating Units and Special Tribunals Act.
25 See, for example, Duncan, *Stopping the Spies*; and Mare and Duncan, 'An Analysis of the Communications Surveillance Legislative Framework in South Africa'.
26 RICA, Act 70 of 2002, sec. 16(5).

senior officials from the police and intelligence agencies may apply to the RICA judge to intercept communications and communication data.[27]

RICA puts significant obligations on the communications industry to assist the state in intercepting people's communications. In addition to logging the identity of all users through SIM registration and other account authentication, mobile or internet service providers must store all user metadata for at least three years.

In some instances, the Act does allow law-enforcement agencies to demand immediate access to someone's locational data without pre-approval of the judge, to prevent serious bodily harm or a life-threatening emergency.[28] These requests can be made orally, but the Act requires post-facto justification and notification to the RICA judge.

While it is evident that RICA contains various protections for the right of privacy and safeguards against abuse of power, its weaknesses have faced significant criticism in academia, activism and the courts. For the sake of brevity, this discussion will focus on just a few such weaknesses.

The transparency critique of RICA

One of the most significant findings in the High Court's initial ruling in the *amaBhungane* case is that targets of 'RICA' interceptions should generally be notified after the fact[29] – a policy proposal often called 'user notification'. If this ruling is upheld by the Constitutional Court in 2020, it would strike down a secrecy provision in RICA which expressly prohibits any of the parties involved in an interception from 'tipping off' a target of the interception, in perpetuity.[30] Should the High Court's order prevail, in future investigations the authorities would ordinarily have to notify a person that their communication had been intercepted, 90 days after the interception period ends. Under this system, the authorities would still be able to apply to the RICA judgment for such notification to be postponed to preserve an ongoing investigation.

The *amaBhungane* lawyers persuaded the High Court judge of a long-held grievance about RICA's secrecy clause – that lack of user notification in the law had enabled a culture of surveillance abuses by making it near impossible to detect such abuses. Various authorities have decried the 'user notification' proposal as being potentially crippling to all future law-

27 According to the police's submissions in *amaBhungane*, within the police all applications for RICA interceptions must first be approved by the national head of Crime Intelligence and the relevant provincial police commissioner. Within State Security, the Act requires applications for RICA interception to be approved by an official with the seniority of 'General Manager'.
28 RICA, Act 70 of 2002, secs 7 and 8.
29 Judgment in the *amaBhungane* case.
30 RICA, Act 70 of 2002, sec. 42.

enforcement investigations – apparently ignoring that such notification would only occur after an investigation has concluded or lapsed, and that such a provision would bring RICA in line with many international equivalents, even in notoriously spy-happy jurisdictions like the United States. Perhaps ironically, while RICA's regime of secrecy has prevented 'innocent' people from detecting surveillance operations against them, the only person who would be likely to find out that their communications had been intercepted would be someone who was spied on as part of a legitimate investigation, and then faced criminal charges, *and* discovered that evidence from their communications is introduced as evidence at trial.[31]

Aside from the (pending) user notification proposal, the only transparency requirement built into RICA procedures is a requirement for the RICA judge to submit a brief annual report to Parliament's closed-door Joint Standing Committee on Intelligence; the report generally includes a summary of the number of interceptions authorised.[32] However, the inconsistent quality of these reports mean that even when they are eventually made public, they are of little use for public oversight.[33]

The metadata critique of RICA[34]

Criticisms of RICA's provisions on metadata fall into two major themes. The first is *storage*: critics have argued that storing all users' communication records for three years is excessive (*amaBhungane* lawyers argued in their High Court case for a limit of one year[35]), while the Right2Know Campaign argued that mandatory storage is unacceptably invasive altogether.[36] In the *amaBhungane* case, the High Court ultimately dismissed a proposal to reduce the duration of metadata storage on the grounds that not enough evidence had been put forward to justify it – a matter we will revisit later.

The second theme is *access*: RICA has been criticised for treating metadata as inherently less sensitive than content. While this is a noted flaw in many interceptions laws globally, RICA also takes a different (and equally unhelpful) approach, treating *historical* information as inherently less sensitive than 'real-time' information. In terms of RICA, only the designated judge can authorise the interception of a person's communications or metadata in 'real-

31 Interview with former Hawks investigator.
32 The RICA judge's reporting mandate stems from RICA, sec. 60 and the Intelligence Services Oversight Act 40 of 1994, sec. 3(i)iii.
33 See Duncan, *Stopping the Spies*, chap. 4.
34 It should be noted that RICA's metadata provisions are intended to apply both to telecommunications providers and internet service providers, but as yet the state has handed down only the necessary regulations to compel the telecommunications industry to comply (Duncan, p.106). As the extent and period of metadata retention by internet-service providers is unclear and not subject to any government regulations, this paper limits its focus to telecommunications metadata.
35 Applicants' founding affidavit, in *amaBhungane*, paragraph 80.
36 Amici Curiae submission, in *amaBhungane*, paragraph 41.

time', meaning that investigators can 'listen' in on a communication as it happens.[37] In the case of metadata, the threshold is somewhat lower for the requester, in that he or she is not obliged to show the judge that other less invasive investigative measures have failed – but the request does still need to be put to the RICA judge. However, to access a person's *historical* communication records, section 19 of RICA allows that permission can be sought from *any* judge or magistrate, even at the lowest courts. These orders authorise the handover of 'archived' communication records – meaning that they are older than 90 days. (To avoid confusion, this provision in Section 19 of RICA is separate to – and possibly made redundant by – the provision to access a person's communication records through Section 205 of the Criminal Procedure Act.)

The Section 205 procedures

Irrespective of the interception procedures in RICA, the Criminal Procedure Act provides for the authorities to seize a person's communications records from network providers, using an order or subpoena from the lower courts. Section 205 of that Act provides:

> *A judge of a High Court, a regional court magistrate or a magistrate may [subject to section 15 of RICA] ... upon the request of a Director of Public Prosecutions or a public prosecutor authorised thereto in writing by the Director of Public Prosecutions, require the attendance ... of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed [emphasis added].*[38]

The Criminal Procedure Act lays out a vast set of rules for the day-to-day workings of the criminal justice system, from investigations and arrests to prosecution. In its initial version, signed into law in 1977, Section 205 served to compel a reluctant witness to testify or submit documents in court. As amended in the post-RICA era, it authorises a magistrate to order a communications service provider to hand over a user's metadata – in a manner of speaking, it forces the network provider to act as a 'state's witness' against a user on their network.[39] This parallel process is enabled through section 15 of RICA, which provides that other laws may also provide for access to metadata.[40]

37 'Real-time' is defined as any communication or metadata occurring contemporaneously or within the last 90 days.
38 Criminal Procedure Act, Act 51 of 1977, sec. 205.
39 The use of Section 205 subpoenas is not restricted to communications data: investigators can invoke Section 205 to seek bank records, CCTV footage, and all manner of other information held by a third party.
40 RICA, Act 70 of 2002, sec. 15.

In short, the critiques of RICA's safeguards notwithstanding, Section 205 serves as a parallel route to access people's communications metadata which bypasses nearly every safeguard or oversight measure built into the RICA Act.

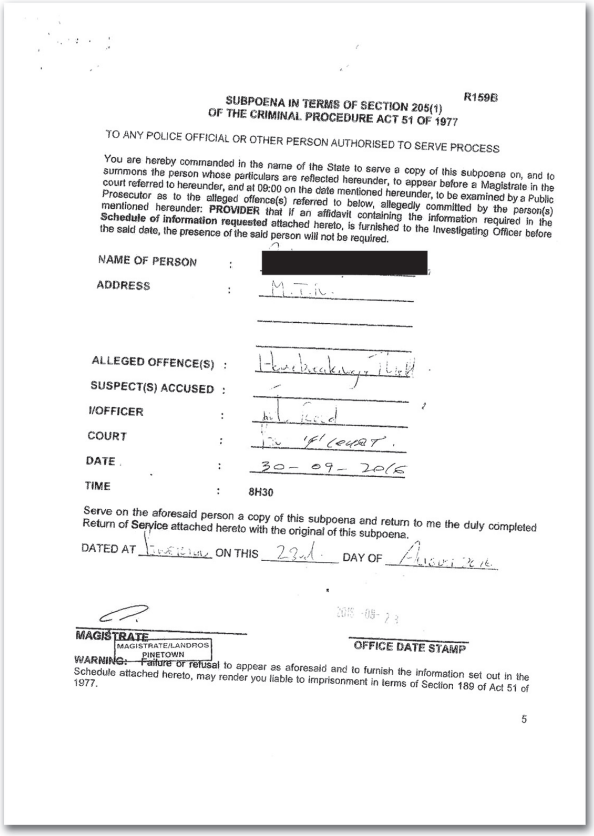
While RICA procedures are slightly less stringent for requests for 'archived' metadata than for 'real-time' interceptions of content or metadata, there are nonetheless several safeguards in place: a RICA request for 'archived' metadata may only be sought to investigate serious offences and threats to national security, and only by relatively senior officials, and only if they can provide a range of information and justifications to the relevant judge – who is, generally speaking, a specially appointed judge with a unique mandate to oversee decisions where privacy and security concerns appear to collide.

By contrast, Section 205 of the Criminal Procedure Act allows that a police official of any seniority can request access to a person's communications data, as long as the request is authorised by one of a wide category of prosecutors and even the most junior magistrates. It may be granted for any offence, with scarcely any information required by the requesting official. On paper, the bar could barely be set lower. While RICA intercepts are subject to an annual report by the RICA judge, the judges and magistrates issuing 'Section 205' orders are not required to undertake any reporting. In fact, one prosecutor argued that Section 205 requests actually give wider access to communications data than could be sought through RICA's provisions for 'archived' information; while a RICA request for 'archived' metadata would yield only data which is 90 days older or more, an order issued in terms of Section 205 could theoretically apply to a user's metadata that is created and stored on that same day.[41]

One would be hard-pressed to tease out the logic behind this arrangement. Indeed, papers filed on behalf of the SAPS in the *amaBhungane* case, which sought to persuade the court that existing privacy protections were more than sufficient, instead revealed an unwitting complacency about metadata privacy. Major General King Bhoyi Ncgobo, the (now axed) head of Crime Intelligence, argued in a court submission that notwithstanding various safeguards and oversight measures for interceptions of communication, the SAPS tried wherever possible to rely on the 'less intrusive tool' of call-related information – for example, through 'Section 205' metadata orders, which allowed for such data to be sought in 'the normal course of investigating *general crime*' (that is, not *serious crime* as contemplated in the RICA Act) [emphasis added].[42] Sadly, having made the admission that communication

41 Interview with State Advocate B.
42 Police answering affidavit, in *amaBhungane*, No. 2598/17, paragraph 43.2.

metadata is treated as less sensitive, and is indeed used to investigate non-serious crimes in the absence of all the oversight mechanisms on which the state's defence of RICA was based, the affidavit did not spell out any reasoning for this.



R159B

SUBPOENA IN TERMS OF SECTION 205(1) OF THE CRIMINAL PROCEDURE ACT 51 OF 1977

TO ANY POLICE OFFICIAL OR OTHER PERSON AUTHORISED TO SERVE PROCESS

You are hereby commanded in the name of the State to serve a copy of this subpoena on, and to summons the person whose particulars are reflected hereunder, to appear before a Magistrate in the court referred to hereunder, and at 09:00 on the date mentioned hereunder, to be examined by a Public Prosecutor as to the alleged offence(s) referred to below, allegedly committed by the person(s) mentioned hereunder: **PROVIDER** that if an affidavit containing the information required in the **Schedule of information requested** attached hereto, is furnished to the Investigating Officer before the said date, the presence of the said person will not be required.

NAME OF PERSON : [redacted]

ADDRESS : M.T.N.

ALLEGED OFFENCE(S) : Housebreaking, theft

SUSPECT(S) ACCUSED :

I/OFFICER : Mr Ismail

COURT : The Regional Court.

DATE : 30-09-2015

TIME : 8H30

Serve on the aforesaid person a copy of this subpoena and return to me the duly completed Return of Service attached hereto with the original of this subpoena.

DATED AT Pretoria ON THIS 23rd DAY OF August 2015

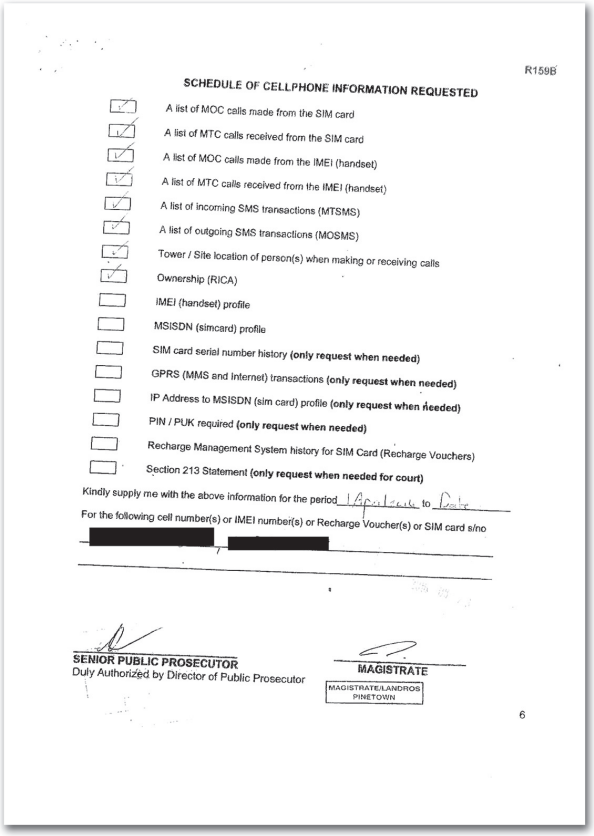
MAGISTRATE

MAGISTRATE/LANDROS PINETOWN

OFFICE DATE STAMP

WARNING: Failure or refusal to appear as aforesaid and to furnish the information set out in the Schedule attached hereto, may render you liable to imprisonment in terms of Section 189 of Act 51 of 1977.

5



R159B

SCHEDULE OF CELLPHONE INFORMATION REQUESTED

- [x] A list of MOC calls made from the SIM card
- [x] A list of MTC calls received from the SIM card
- [x] A list of MOC calls made from the IMEI (handset)
- [x] A list of MTC calls received from the IMEI (handset)
- [x] A list of incoming SMS transactions (MTSMS)
- [x] A list of outgoing SMS transactions (MOSMS)
- [x] Tower / Site location of person(s) when making or receiving calls
- [x] Ownership (RICA)
- [ ] IMEI (handset) profile
- [ ] MSISDN (simcard) profile
- [ ] SIM card serial number history **(only request when needed)**
- [ ] GPRS (MMS and Internet) transactions **(only request when needed)**
- [ ] IP Address to MSISDN (sim card) profile **(only request when needed)**
- [ ] PIN / PUK required **(only request when needed)**
- [ ] Recharge Management System history for SIM Card (Recharge Vouchers)
- [ ] Section 213 Statement **(only request when needed for court)**

Kindly supply me with the above information for the period 1 April 2015 to Date

For the following cell number(s) or IMEI number(s) or Recharge Voucher(s) or SIM card s/no [redacted]

SENIOR PUBLIC PROSECUTOR
Duly Authorized by Director of Public Prosecutor

MAGISTRATE

MAGISTRATE/LANDROS PINETOWN

6

Illustration 1: Excerpt from the S205 subpoena issued for journalist Athandiwe Saba's phone records. The listed offences are 'housebreaking, theft'. The order is for six months of call and message transactions and tower/location data.

How the process works

Based on several interviews and court submissions, the following picture emerges for a Section 205 metadata request. First, an investigating officer identifies a suspect, phone number or device number (or, as we shall see, a cell tower) that he or she considers relevant to an investigation. The officer fills out an application for a Section 205 subpoena, detailing any information sought and the date range – in some instances the subpoena may simply be for the account owner's details, but very often it will be for the call records themselves. This application takes the form of a sworn affidavit that includes details of the case and any relevant evidence. The investigating officer must first get the application counter-signed by a prosecutor before taking it to a magistrate, who must give the final authorisation. The investigating officer then generally transmits the magistrate's order to a regional or provincial

branch of SAPS's Technical Support Unit (TSU),[43] a structure within the Crime Intelligence Division which provides a variety of digital forensics services within SAPS. The TSU liaises with a designated staff member at the relevant network provider – for example, MTN. The MTN representative searches for any relevant records from their system, downloads them to a CSV file,[44] and sends it back to the police liaison. According to one piece of court testimony by a technical expert for MTN, this database query takes just a few minutes.[45]

Once the records are in the hands of the police, they can be analysed for investigative leads (such as a suspect's possible identity, whereabouts, or modus operandi) or evidence (information which corroborates an existing theory of guilt, such as evidence that two suspects who deny knowing each other are in fact in regular contact, or which refutes an existing theory, such as locational data that shores up a suspect's alibi).[46] The most commonly cited tool for SAPS to analyse communications data is a piece of IBM-made software called i2 Analyst's Notebook, which allows the user to create visual maps of people's associations and linkages based on a spreadsheet of call records, bank statements, or similar data. Analyst's Notebook, for which about 1,500 police members had reportedly received training in 2017,[47] has been cited in a number of criminal trials where an expert police witness presents cell phone evidence to the court.

However, the police's capacity to analyse phone records appears to be fragmented and unevenly distributed. According to interviews for this paper and patterns that emerge in court cases, in some instances the SAPS technical support unit[48] or other specialised units will provide an analysis for the investigator;[49] in other instances individual investigators develop pockets of self-taught expertise, either using Analyst's Notebook or producing a painstaking manual analysis.[50] A vivid picture of this patchwork effect emerges in a 2015 master's dissertation by a detective on the potential to use cell phone data to combat cable theft syndicates: of 19 detective colleagues she interviewed, each of whom specialised in this area of investigation, only one had been trained in the Analyst's Notebook software. Eight said that investigators should conduct their own analysis of phone records, while seven detectives said they got assistance from specialised units or more experienced investigators. The remaining

43 References to the 'TSU', or sometimes 'Technical Support Services', appear in various recruitment notices, media reports, Parliamentary hearings and interviews with SAPS members, but this research was unable to find any publicly available SAPS document or organogram listing either structure.
44 Comma-separated value file – a common file format for large datasets, which can be opened as a spreadsheet.
45 *S v Brown and Others* (CC 18/2017) [2019] ZAECPEHC 11; [2019] 2 All SA 552 (ECP) (5 February 2019).
46 Interview with former Hawks investigator
47 Heidi Swart, 'Big Brother Is Watching Your Phone Call Records'.
48 Interview with Detective Warrant Officer
49 Testimony in a trial of three accused abalone poachers suggests that the Hawks directorate has 'in-house' expertise for phone records analysis. See:. *S v Brown and Others*
50 See, for example, interview with Hawks forensics analyst Thereza Botha in Burgess, *Heist! South Africa's Cash-in-Transit Epidemic Uncovered*, chap. 22.

three appeared not to use call records analysis.[51] The relatively scant literature on the use of phone records in South African policing shows that, at least in the early 2000s, third-party service providers have delivered metadata analysis to police investigations and prosecutions – notably the Council of Scientific and Industrial Research, a government-funded research agency.[52] However, at least in the case of the CSIR, these collaborations appear to have been linked to specific projects, rather than part of an ongoing service relationship.[53]

51 van Niekerk, 'The Analysis of a Cell Phone Record as a Source of Intelligence in the Investigation of Copper Cable Theft', 69.
52 Schmitz, Riley, and Dryden, 'Mapping Time and Space as a Forensic Tool', 54.
53 Email correspondence with Prof. Peter Schmitz, Department of Geography, UNISA.

3 Police perspectives on metadata use

In the *amaBhungane* case, police argued that access to communications data was an essential response to the realities of modern crime, where criminal syndicates can communicate, strategise and even commission crimes remotely, often without generating any physical or written evidence of their interactions.[54] The police papers argued this was particularly important where criminal syndicates successfully shield themselves from other avenues of police investigation, such as witnesses, forensic evidence, and informants and undercover agents,[55] and in building a case against the 'mastermind' of a syndicate who directs others to do crime via lieutenants and henchmen.[56] The state's paradoxical view is that communications metadata reveals so little that it requires few privacy protections, yet reveals so much that investigators cannot do without it.

Several interviews reflect that, while the legal framework (and its custodians) tend to *underestimate* the sensitivity of metadata, the debates around RICA may also have *overestimated* the usefulness of intercepting content. One investigator complained that, aside from the slow application process RICA entails, intercepts themselves are a very labour-intensive tool for investigations: a 90-day interception order can generate tens if not hundreds of interceptions every day which investigators must listen through, transcribe, and

54 Police answering affidavit, in *amaBhungane*, paragraph 52.
55 Police answering affidavit, paragraph 50.
56 Police answering affidavit, paragraph 55.

analyse for evidence and intelligence. In some cases, a target may communicate in several languages, which may require investigators to have a translator on hand.[57]

Thus, while in *amaBhungane* the police called metadata a 'less intrusive' investigative tool, in reality it may often be a *more useful* investigative tool – capable of drawing out the necessary insights about a person with less effort and expense. This would explain one reason that police seek out users' metadata using Section 205 exponentially more often than they seek to intercept users' communication using RICA.

Certainly, every investigator and prosecutor interviewed for this research was at pains to show that that communications metadata by itself is profoundly useful for different aspects of their work.

Corroborating evidence or refuting alibis

One of the most commonly cited uses for cell phone evidence is the use of locational data to shore up circumstantial evidence, especially in murder cases where there is no living witness to the crime. The earliest reported use of such data in the South African criminal justice system dates back to the prosecution of Cape Town gangsters for a series of murders and hijackings in 1998.[58]

Since then, locational data from the phone records of both victim and accused often play a definitive role in high-level investigations and prosecutions. One state advocate, in describing how phone locational data can often be crucial to a case, pointed to a gang-related murder in which, after killing the victim, the murderer used the victim's car to transport and dispose of the body. Though the police had a suspect, the evidence tying him to the crime was circumstantial at first, until they were able to match location data from the vehicle's tracker to location data from the suspect's phone records. Presented with the correlation, which refuted his alibi, the suspect confessed to the murder.[59]

57 Interview with former Hawks investigator.
58 Schmitz and others, 'Breaking Alibis Through Cell Phone Mapping'.
59 Interview with State Advocate A.

Mapping criminal networks

Communication data can also be used to map out a criminal network. In one of South Africa's biggest criminal trials, cell phone records gave crucial evidence in the state's case against the 'KZN 26', a group of men accused of a series of violent cash-in-transit heists. When the main group of suspects were arrested, police found large wads of cash in their vehicles, along with several firearms, unopened safe boxes from a cash-in-transit van, and an angle grinder similar to that which had been used to cut open one of the cash-in-transit vans. However, as noted by the court, the evidence against the accused was largely circumstantial.[60] All 26 of the accused denied any complicity in any of the crimes of which they were accused, and several of them declined to testify at all. Their cell phone records, seized under Section 205, ended up forming the backbone of the state's case: the state analysed 72,000 phone calls between the 26 men in the single month leading up to the robberies, in order to establish a pattern of coordination between each of them, as well as to establish evidence of their locations and movements during key phases of the heists.[61]

Tracing suspects

One station-level detective recalled investigating a home robbery-murder in the Western Cape where the victim's phone was found to be missing. On the assumption that the perpetrators had stolen the victim's phone, he applied for access to the victim's call records using the Section 205 procedure. These records showed that someone was still making and receiving calls from the number and device. The investigating officer used tower locations to trace the user to Fort Beaufort in the Eastern Cape, and made contact with several people who had communicated with the current user of the number in order to establish the suspect's identity – eventually, leading to their arrest and prosecution for the murder. In the investigating officer's version, the ability to track the victim's phone was the only lead in solving the case.[62]

60 *S v Shange and Others* (CC169/07) [2012] ZAKZPHC 69 (29 June 2012).
61 *S v Shange and Others* (CC169/07) [2012] ZAKZPHC 69 (29 June 2012).
62 Interview with former Detective Warrant Officer.

The use of ‘tower’ records

The former SIU investigator described in detail how investigators can use Section 205 requests to seize large batches of data from cellular towers – creating a dragnet of all communication within an area, not only of a particular suspect.[63] This practice, which appears to have been overlooked in previous research and journalism, can be used where investigators know the approximate time and location of an offence, but have not identified a suspect or a phone number: by seizing all records of all cell phone activity recorded by the nearest cell tower, investigators can identify a pool of possible suspects, albeit one that contains the sensitive records of thousands of unwitting bystanders. An investigation of a series of crimes – for example, a string of cash-in-transit heists – could cross-reference data from cell towers in the vicinity of each robbery and look for any phone numbers that appeared in each database.[64] In doing so, however, an investigator would be entrusted with the communication data of potentially tens of thousands of people.

The former SIU investigator stated that a request for tower data can be more targeted. For example, a police investigator can give specific parameters to the network operator to narrow the request, such as a window of time in which the offence occurred, or a request for records relating to specific phone number that is already of interest. This can yield a limited record, or even an expert witness affidavit that summarises any findings relevant to the investigation. However, he reported that in instances where the service provider lacks analytical capacity, even a targeted request can result in a ‘raw data dump’ of many thousands of records.

In fact, such records would include locational data about each of those users that could not be obtained if a law-enforcement agency made a targeted request for their metadata directly. The RICA regulations stipulating what communication data network operators need to store for law enforcement purposes only require that base station information be logged when a communication is made or received[65] – however, in order to be available to make and receive calls, there is a constant exchange of radio signals between cellular devices and the base station. As a result, data from a base station includes locational information about a user even if they do not send or receive any communication – this data is not stored in the 3-year archives of metadata which each network operator maintains, but can be accessed in the short term via a Section 205 request to a base station.

63 Interview with former SIU investigator.
64 Interview with former SIU investigator.
65 RICA directives, Notice 1325 of 2005, Government Gazette, 28 November 2005.

Different structures, different picture

Interviews with investigators at different levels of the SAPS suggest stark differences and inconsistencies in the police's understanding of and capacity to use communications metadata.

Interviewees from specialised units and the NPA describe the Section 205 process as relatively quick and painless – even a next-day 'service'. However, station-level detectives described the process as maddeningly slow.

When describing the usefulness of call data to his investigations, one detective sergeant almost immediately turned to the delays as a tempering factor: 'The problem is time. The Hawks and special units get it [the requested data] the next day. We at the station level must wait months'.[66] To illustrate his point, he called two colleagues from the corridor to share their frustration with slow replies to Section 205 metadata requests. Both agreed: while the process of getting the request authorised by a prosecutor or magistrate usually took less than a day, they could expect to wait as long as four or five months to receive the data.

None could say whether blame for the delays rested with their counterparts in the police's Technical Support Unit, or with the service providers.

A station-level detective in a high-crime township of Cape Town also reported waiting for four months or more after submitting Section 205 metadata requests. In describing how these delays affected his use of communications data in investigations, he offered some interesting insights. On one hand, he described the slow turnaround time for requests as an incentive to *limit* his use of metadata in certain investigations:

> *For schedule 1 offences such as a murder it would be standard, but for something like theft... only if I really have to, because of the time [delays]. I would rather use witnesses and physical evidence to move forward on a case as quickly as possible.*[67]

On the other hand, he later described how the slow turnaround of Section 205 requests created an incentive to make such requests as *expansive* as possible. This is because, if the investigator learns, several months into an investigation, that an initial Section 205 request did not yield useful information, they may be forced to draft follow-up Section 205 requests,

66 Interview with Detective Sergeant.
67 Interview with former Detective Warrant Officer.

losing even more time in an investigation. To mitigate this risk, the detective described a tendency to make any Section 205 application as broad as possible, to include information that might only become pertinent to the investigation at some later stage – in other words, the slow turnaround of Section 205 requests was perceived to increase the 'risk' of limiting the scope of such requests.[68]

Formal and informal checks on the system

The critiques of Section 205's lack of safeguards notwithstanding, interviews with law enforcement stakeholders uncovered some safeguards worth noting – although these stemmed from organisational or individual choices rather than the law itself.

While a Director of Public Prosecutors can empower any prosecutor with the authority to endorse Section 205 requests, in the experience of one State Advocate, this authority is only granted to senior prosecutors and higher.[69] In another example, while Section 205 metadata requests may be granted for investigations of any offence, one detective said that certain prosecutors are less likely to approve Section 205 requests if they feel the offence is too minor.[70] Detectives interviewed here said that magistrates generally did approve a Section 205 request once it had been endorsed by the prosecutor – though not always; two detectives described prosecutors as being more likely to scrutinise the request carefully. For example, one detective reported that some prosecutors will refuse to sign off on a Section 205 request for call records if the date range is too broad: in these instances, the investigating officer must either justify the parameters of the request or narrow them.[71] On the other hand, the fraudulent Section 205 subpoena in the Athandiwe Saba case (see page 15) shows that a subpoena can also be issued for non-violent offences such as 'housebreaking, theft', and for the relatively broad date range of six months: a police detective, a prosecutor, a magistrate and at least one representative from MTN were each party to that request, and no objections appear to have been raised.

The same detective pointed out that no procedures exist for the destruction of any sensitive communication data when an investigation lapses. Gesturing in his office to a large stack of papers containing messages and data extracted from the phone of a man killed in a roadside shooting – which he and the victim's family had scoured unsuccessfully for a possible motive

68 Interview with former Detective Warrant Officer.
69 In the hierarchy of the criminal justice system, senior prosecutor is ranked above junior prosecutor, prosecutor and control prosecutor.
70 Interview with Detective Sergeant.
71 Interview with Detective Sergeant.

or suspect – he indicated that it would be on his conscience to ensure that such 'private, family stuff' was properly disposed of. This individual sense of duty is admirable, but the lack of systemic safeguards is another warning sign: one of the grounds on which the High Court found RICA to be unconstitutional was its lack of privacy procedures for the safekeeping, handling and eventual destruction of any communication data seized by the police through RICA procedures.

4 Police perspectives on reforms

As explored below, the interviews for this research yielded a surprising plurality of views on the use of communications data in policing, although understandably still largely framed in the logics of policing and law-enforcement. In general, the interviewees favoured 'light touch' reform options – which could build a few safeguards against fishing expeditions and other misuse of Section 205, without resulting in delays or administrative hurdles, or restricting investigators' access to the procedures. One interviewee summed up the argument for a 'light touch' approach by saying:

> *What you don't want is to make it so difficult that good policemen who want to get the job done in country with high levels of crime are now being stifled with more paperwork.*[72]

Most interviewees appeared to have either intuitive or first-hand appreciations of the risks of abuse of Section 205 procedures: in two cases, former investigators believed they themselves had been targets of illegal spying by rogue officials, and several others were aware that the procedures could be or had been abused by private actors.

72 Interview with former Hawks investigator.

Limiting its use

One proposal to limit the scope for abusive or non-proportionate use of communications metadata is to confine Section 205 requests to serious offences. Without exception, the law-enforcement respondents balked at this suggestion, arguing that call records were too valuable a tool to exclude from investigations of any kind. Aside from perspectives on privacy, this tended to be informed by a worldview that police work is all but fatally disadvantaged. As a former Hawks investigator said, 'We live in a crime-ridden society, and everything, everything is [already] against the investigator'.[73] A station-level detective complained that, 'the law protects always the suspect, never the complainant'.[74] Leaving aside the merits of these views, they reflect a common theme in police culture and suggest that any proposal that might limit an investigator's options will be met with resistance.

Several investigators framed their argument for 'all available tools' in terms of their responsibility towards victims of crime, arguing for example that the theft of R1,000 may not be considered a 'serious' crime in terms of policing priorities but represents a crisis for a victim living in poverty. While acknowledging that metadata's potency as an investigative tool does raise privacy implications, one investigator framed his responsibility towards the victim: 'If any evidence can help investigate any offence, it would be unprofessional of me as an investigator to exclude any potential evidence'.[75]

While these arguments are made in earnest, it should be pointed out that they are also largely hypothetical: while Section 205 requests *may* be invoked in any offence, several investigators indicated that a range of informal limits are in place.

Although the delays in Section 205 requests result from lack of administrative capacity rather than oversight, station-level detectives cited these delays as a reason to use the requests only for more serious offences. As detailed already, at least in some instances prosecutors will reject a Section 205 request if they deem the offence to be too trivial. Finally, it is a given that police officials do in fact prioritise their work every day – this is a fundamental feature of the constrained capacity of South African policing, whether those priorities are imposed through directives from leadership or the result of informal decisions and practices by individual members.

73 Interview with former Hawks investigator.
74 Colleague's remark during interview with Detective Sergeant.
75 Interview with former SIU investigator.

These factors suggest that, generally speaking, a range of informal and practical limits on use of metadata do exist – but are not written into law.

Several respondents offered a more thought-provoking case for not limiting the use of Section 205: that the call records of a person arrested for a low-level offence such as petty theft may yield connections to high-level offences, such as a criminal syndicate. However, in interviews this scenario was posed largely as a hypothetical.

User Notification

The 'user notification' principle is one place where interviewees differed completely from the official views of law enforcement agencies. As noted earlier, the leadership of SAPS has fought bitterly against proposals for user notification in the ongoing RICA case. Appealing the High Court judgment, the Minister of Police argued to the Constitutional Court that 'the very purpose of the RICA [combatting crime] *can only be achieved* if there is a *total* ban on notification'.[76]

Strikingly, none of the investigators interviewed for this study held that view. Seven current and former investigators, ranging from station level to the Hawks and SIU, each allowed that some form of *post-facto* notification of Section 205 metadata requests could be introduced without disrupting investigations, and several specifically proposed user notification as a way to deter to abuse of the system, so that anyone whose records are seized unlawfully can take corrective action.[77] The former Hawks investigator who argued against limiting the use of Section 205 argued that it would be better to offset risks of abuse by implementing a form of user notification: 'I would rather have the consequences to be more dire should you access [metadata] unlawfully, than making the policeman's work more difficult'.[78]

These respondents differed in their views on *when* such notification should take place and under what circumstances it should be postponed. Where an investigation relates to an ongoing pattern of criminality, such as racketeering, one can easily see the argument for postponing notification while an investigation is ongoing. In matters where there is a single historical offence under investigation – a domestic murder where the spouse is under suspicion

76 Minister of Police notice of appeal, in *amaBhungane*, section 1.7. Emphasis added.
77 One respondent – a former station commander who oversaw detectives specialising in a range of serious offences – even seemed to believe, incorrectly, that notification was already a feature of the system.
78 Interview with former Hawks investigator.

– investigators generally said that user notification would not disrupt an investigation, perhaps even while it was ongoing.

One possible solution posed by the former SIU investigator would be to have a schedule of different notification windows for different types of investigations and offences. He also suggested that investigators seeking a Section 205 metadata order could be required to request in their application whether notification should be deferred, and if so to provide a motivation for this at the time of the request.[79]

If 'user notification' were applied to Section 205 metadata requests, settling on the exact timeframe for notification could be a thornier issue. International comparisons differ widely: Japan and South Korea's surveillance laws generally require notification within 30 days, the USA and Canada within 90 days, and Slovenia within two years. Germany, Belgium and many others simply provide for notification as soon as can be done without endangering an investigation or doing other harm. Each provides conditions in which notification may be deferred, or ruled out entirely.[80] In *amaBhungane*, the High Court accepted a proposal by the applicants that notification of RICA interceptions should occur 90 days after the fact, pending a full amendment of the RICA law.

In order for such a system to be transposed to Section 205 requests, it is plain that several things would have to change. For example, where station-level detectives can expect to wait four months or more to receive the data they requested under Section 205, it follows that a three-month notification window is too narrow: to arrive at a reform proposal that has any hope of winning support from investigators, either the turnaround time for Section 205 must be shortened, or the notification window lengthened, or both.

An appropriate notification period might be best designed according to average lengths of investigations, although it is not clear if reliable figures of this kind exist.[81] The former SIU investigator felt, for example, that a 90-day notification window would be unworkably narrow for complex multiyear investigations, such as those required in racketeering cases – potentially trapping investigators in a process of perpetual applications to defer notification while they continue their investigations.

79 Interview with former SIU investigator.
80 Unpublished memorandum by Privacy International.
81 It might be noted that if SAPS had not rejected the concept of user notification outright it may have offered insights into how best to implement such a policy.

One station-level detective who showed more scepticism towards notification proposals argued that it would be impossible to arrive at a 'default' notification period, and that notification should only occur when an investigation is closed, or when the person of interest has been excluded as a suspect. He hinted that user notification could be a source of anxiety for station-level police who work in close proximity to criminals elements who would not take kindly to discovering that their phone records had been seized.[82]

Another question needing more consideration is how notification would be achieved. In some jurisdictions, and in the High Court's order in RICA, this responsibility would fall to the police or intelligence agencies. In other countries, it falls to a prosecutor or judge involved in authorising the intrusion. Given that the whole point of notification is to limit the scope for abuse of interceptions procedures, it stands to reason that notification should not fall to those who requested the interception as the risk of non-compliance is high. Most respondents did not have specific proposals for how to implement notification, but one prosecutor proposed that notification could fall to the service providers, to lessen the administrative burden on law enforcement agencies.[83]

Only one interviewee felt that user notification would be detrimental to law enforcement: a State Advocate who remained sceptical of any prospects for reforms to the Section 205 procedures.[84] In his view, while user notification could help identify and act on abuses of the procedures, it would also place new pressures and burdens on law-enforcement agencies by opening each process to review. (As it stands, any Section 205 order that produces evidence in a criminal trial is already open to such review by a defendant's legal team.) Any benefits, to his mind, would be outweighed by the risk of vexatious legal challenges by criminals with deep pockets, which could drain prosecutors' time and resources.

Raising the bar for Section 205 requests

Generally, interviewees said that it would be impractical to remove the Section 205 process from the lower courts entirely – arguing, for example, that placing the authority in the High Courts could delay authorisation by months. However, several respondents offered other proposals to boost oversight and limit the scope for misuse of Section 205 metadata requests. These include:

82 Colleague's remark during interview with Detective Sergeant.
83 Interview with State Advocate A.
84 Interview with State Advocate B.

- **Limiting the authority to grant Section 205 orders to more senior magistrates:** One station-level detective suggested that the responsibility could at least be restricted to more senior branches of the lower courts, such as regional magistrates rather than district magistrates.[85] He further suggested that Section 205 applications could be considered by specially designated magistrates, with particular insight on the legal, technological and rights issues at hand. Essentially, this novel proposal would replicate the 'RICA judge' model in the lower courts.[86]
- **Making the 'test' higher:** Rather than restricting which courts may authorise Section 205 metadata requests, or for which offences, one respondent argued that Section 205 should simply be amended to require the court to consider higher standards from applicants – for example, that the request must meet a higher legal test than 'likelihood' of relevance to an investigation, such as 'probable cause' that the requested information would reveal criminal activity,[87] and that less invasive investigative methods have failed. An amended Section 205 could also require the judge to weigh up the privacy implications of the request.[88]

Reducing or ending the mandatory storage of metadata

One of the most ambitious proposals for privacy advocates – in South Africa and abroad – is to end the mandatory storage of communications metadata. Legal regimes that force network providers and internet service providers to store their users' metadata for possible state interception have faced growing critique in international law. In 2018 report, the UN High Commissioner for Human Rights summed up concerns with such laws, writing:

They limit people's ability to communicate anonymously, create the risk of abuses and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches. Such laws exceed the limits of what can be considered necessary and proportionate.[89]

Leaving aside whether the mandatory storage of metadata in South African law can be squared up against international law, the interviews suggest that there is little prospect for privacy

85 Interview with Detective Warrant Officer.
86 State Advocate B said that it is already generally the case that only certain magistrates in a court authorise '205' orders, although it is not clear whether this is by policy or an ad hoc arrangement. Certainly it is not clear that magistrates are required to weigh up privacy implications of the order.
87 The current test in Section 205 is simply that the requested information is 'likely' to give 'relevant information' about an offence.
88 Interview with former SIU investigator.
89 UN High Commissioner on Human Rights, 'The Right to Privacy in the Digital Age', para. 18.

advocates to win support for the proposal to end mandatory retention of metadata entirely. In this scenario, communication service providers would no longer be legally obliged to store their users' metadata; rather, law-enforcement agencies would have the option of seeking a court order to store the metadata of a person currently under suspicion of wrongdoing. The interviews here largely concur with the state's assertions in the *amaBhungane* case that the police's main use of metadata is to investigate specific historical offences, and that ending the mandatory storage of metadata would eliminate a very useful tool from many investigations.

Given the slim chances for that proposal to find support in a policy debate, there may be more in the question of reducing the period of storage – although even that proposal suffered a setback when in *amaBhungane* the court ultimately dismissed the applicants' argument to shorten RICA's three-year storage requirements, saying that there had not been enough evidence to make that case.

There is little empirical evidence to settle this question – and it might be argued that the onus rests on the state to provide evidence to justify the privacy infringement – but a few details are worth mentioning. The first is a survey of the metadata retention periods of 36 Western democracies compiled by the Australian government during a policy review of their own interception laws.[90] Of all 36 countries surveyed, South Africa had the *longest* metadata storage periods (three years). Twenty-three of the countries (63% of those surveyed) had retention periods between 6 and 12 months.

The second is a curious admission by the Department of Justice's representative in the *amaBhungane* case that requests for communications metadata in South Africa generally span less than 19 months.[91] In interviews for this study, the oldest date range for which any investigators remembered seeking communication data was 12 months.

One detective who, like his peers, did not support proposals to shorten the data-retention periods, still made one point that further complicates the state's argument: that career criminals tend to change phones and numbers vary regularly. He conceded that this would make long retention periods irrelevant to many investigations.[92] He argued, however, that older metadata could still be needed to investigate a suspect who is less savvy than a career criminal – for example, a business figure who commissions the murder of their spouse.

90 'Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014'.
91 Department of Justice answering affidavit, in ***amaBhungane,*** section 133.2.
92 Interview with Detective Sergeant.

In other words, it appears that South Africa stores communication data for longer than any of its peers, nearly twice as long as the state's own estimates of what authorities generally need, and which a savvy criminal can easily evade. Yet police members seem likely to fight any proposal to shorten this period of data retention: perhaps another example of fighting to keep 'all tools', irrespective of how often they are needed.

While the decision not to strike down metadata retention in the *amaBhungane* hearing may have poured cold water on any bid to shorten metadata storage periods, the court was careful *not* to rule on the substance – indicating that this is a question of policy, to be settled outside of a court. Let it be so.

Reporting requirements and oversight measures

A number of interviewees made proposals for reporting requirements for the use of Section 205 metadata requests, as a way of limiting the scope for abuse – these ranged from record-keeping and annual reporting by magistrates on Section 205 authorisations,[93] to a centralised digital record-keeping system of requests which would help the authorities flag abuses of the system.[94] Such proposals may be unrealistic in light of the lower courts' ongoing struggles with digitisation and modernisation – one State Advocate lamented the lack of computers and internet connections in some magistrate's districts[95] – which may point back to the earlier proposal to restrict Section 205 authorisations to more senior magistrates.

Nonetheless, the lack of any internal or public monitoring and reporting on the use of Section 205 procedures presents a huge obstacle to improving democratic oversight.

93 Interview with former Hawks investigator.
94 Interview with former SIU investigator.
95 Interview with State Advocate A.

5 Prospects for metadata reform

It would not be overly cynical to assume that the police as an institution will push back against any proposal to curb their use of communication metadata. Certainly, the arguments before the High Court in *amaBhungane* suggested as much, as lawyers for the various state agencies argued that even the modest reforms proposed in that case would 'defeat [the] very purpose' of national security efforts,[96] 'neutralise the capacity of the services to act promptly in averting or actively preventing threats to national security,'[97] and 'compromise the investigation of serious crimes'.[98] The High Court ruled decidedly against those arguments and, at time of writing, both the Minister of Police and State Security Agency had appeals before the Constitutional Court which echoed similar sentiments. One might expect these paper records to be a template for any future debate on the use of Section 205 procedures to protect metadata privacy.

Yet, the interviews conducted for this research suggest otherwise: current and former investigators showed a surprising diversity of views and openness towards possible reforms. It would be naive to conflate that the views of individual members with the positions of the SAPS as an institution, or to exaggerate those members' appetite to significantly restrict access to communications metadata in police work. Indeed, some interviewees indicated that the main limits on their use of metadata were practical, not legal or ethical – stemming from lack of technical capacity in police structures. From the point of view of law-enforcement actors,

96 State Security Agency answering affidavit, in *amaBhungane*, paragraph 47.4.
97 State Security Agency answering affidavit, paragraph 97.
98 Police answering affidavit, in *amaBhungane*, paragraph 74.

this represents an untapped opportunity to use the investigative potential of communications metadata *more*, not less. Nonetheless, the majority of respondents suggested a range of constructive reform measures that could, in their estimation, build greater privacy protections for communications metadata without requiring major concessions from the police. Taken altogether, these protective measures may still be found to fall short, but they indicate that a range of pathways to reform exist, even from within police institutions.

The material from these interviews may help map out the likely terrain for different reform measures. For example, on user notification, the interviewees generally differed greatly from the police's official position: some enthusiastically supported it as a possible measure to curb abuse, others indicated it would be an unwieldy but necessary measure, and only one interviewee (a State Advocate) objected in principle. On 'bulking up' the application process, similarly all interviewees (except for the same State Advocate) supported or proposed some measure to make judicial oversight of Section 205 requests more rigorous – at least in the magistrates' courts. In other areas, interviewees' comments suggest a more difficult path for privacy reforms: notably, on whether Section 205 metadata requests should be restricted to only serious offences, as the case is for RICA requests, and on any proposal to reduce or end the mandatory storage of metadata, the interviews suggest that on some matters the police and privacy advocates are unlikely to find common ground.

The interviews also showed instances where law enforcement officials' perceptions of risks did not stem from material facts: for example, all interviewees felt that reducing the three-year period for metadata storage would be untenable for law-enforcement, but none had ever had a practical need for metadata older than a year. In other instances, investigators' perceptions on privacy differed significantly from constitutional norms: the seizing of bulk metadata from cell towers may constitute 'dragnet' surveillance, inviting serious concerns about its constitutionality, but was generally perceived by interviewees as an invaluable and inoffensive investigative tool. Only one, the former SIU investigator, noted the potential privacy risks.

Yet, several interviewees touched on one of the most fundamental reasons why law enforcement institutions may wish to build safeguards around measures such as the Section 205 procedures: not simply to protect the 'targets' of surveillance, but to protect the integrity of the institutions themselves.

The policing case for surveillance reform

In both the High Panel Review on State Security and the unfolding Zondo Commission, unchecked surveillance powers emerge as a key feature in the inter-agency factionalism and internal corruption that has plagued South Africa's state agencies. Two interviewees who had been involved in investigating corruption in the police and other state institutions say they themselves became targets for interception by corrupt police officials. As one noted, 'They utilise interceptions to strategise [against other investigators], not for evidence in a criminal investigation'[99] – thus helping corrupt factions stay one step ahead of investigations against themselves, seeking out material for blackmail and leverage for adversaries, and so on. Certainly, there is good reason to believe that state spies do turn their powers against their own. For example, the alleged victims of Paul Scheepers, the former Crime Intelligence official who is charged with illegally acquiring phone records using Section 205, include a police Brigadier and a Lieutenant Colonel.[100] In 2018, Lieutenant Colonel Charl Kinnear of the Western Cape Anti-Gang Unit wrote a complaint to his superiors that, among other things, his communications were being monitored by corrupt officials in Crime Intelligence.[101] Even the former National Commissioner of Police, Bheki Cele, discovered that his phone records were monitored by police operators, in an illegal bugging operation that also ensnared two *Sunday Times* journalists.[102]

As much as unchecked surveillance powers can be a tool for corrupt officials, they also may well be a catalyst for corruption: police officers with access to unsupervised surveillance capacity are a valuable asset for criminal networks and rogue private security firms: both of the 'documented' Section 205 spying scandals involve police who appear to have used the Section 205 metadata procedures illegally in the private investigations industry. In the Scheepers case, he is accused of illegally accessing phone records for his own private investigations firm, while in the case of journalist Athandiwe Saba, her phone records were seized through a fraudulent Section 205 request by a police officer in Pinetown before being passed on to a private investigator.[103]

While the state's arguments in *amaBhungane* reflect a concern, sometimes echoed in these interviews, that restricting access to communications data will make police less effective and imperil efforts to combat crime, there is a strong case that the *lack* of restrictions has

99 Interview with former Hawks investigator.
100 *S v Scheepers.*
101 Lt. Col. Charl Kinnear, Complaint, 29 December 2018.
102 Hunter and Smith, 'Spooked', 13.
103 Hunter and Smith, 16; Pinetown Magistrate Court, M201/08/2016.

had that effect, by helping to foster corruption and dysfunction within law-enforcement institutions. It should come as no surprise that political interference and factionalism have corroded the criminal justice system. In a joint submission to the 'State Capture' commission, the Institute for Security Studies and Corruption Watch pointed out that the 'Zuma' era of political manipulation of policing agencies and the NPA coincides with a near-23% increase in categories of aggregated robbery, most associated with organised crime: car hijacking, business and home robberies, and cash-in-transit heists. These statistics, along with a 40% rise in aggravated robbery overall, point to a serious decline in the police's capacity.[104] It would be impossible to measure how, if at all, surveillance abuses factored in the broader corrosion of law-enforcement institutions, but it would be reasonable to conclude that any effect has been less than positive.

Of course, not all cops or prosecutors who engage in unlawful spying are doing so for personal or criminal gain: some may see themselves as 'bending the rules' in an otherwise legitimate investigation. Several interviewees confirmed that police investigators (perhaps even themselves) do occasionally source communication data unlawfully, to aid an investigation – and use lawful procedures after the fact if the data is likely to be needed as evidence in court. One avenue is the 'emergency' procedures in RICA (Sections 7 and 8) which allow for an investigator without a warrant to compel service providers to hand over locational data, or even the communication itself, in life-or-limb situations: several investigators stated that these procedures can be invoked to track down a suspect who may otherwise destroy their phone and SIM card, even if no life-or-limb risks exist. One interviewee said he could use personal contacts in specialist units such as the TSU or other crime intelligence structures to acquire certain communication data while waiting for service providers to respond to a Section 205 subpoena, although he did not know what methods were involved. He described the motivation to use 'back doors' as part of his duty of care as a police member: 'To save a life, I will break the law'.[105]

No matter how nobly intended, these kinds of transgressions may still present a risk to policing institutions. It is commonly imagined that good cops need to 'bend the rules' in the worthy pursuit of fighting crime, but studies on police corruption note that even minor transgressions may put police members on a 'slippery slope' towards corruption.[106] It may well be that, just like other forms of corruption, a culture of spying abuses can be contagious.

104 Institute for Security Studies and Corruption Watch, 'State Capture and the Political Manipulation of Criminal Justice Agencies', Joint Submission to the Judicial Commission of Inquiry into Allegations of State Capture, 49–50.
105 Interview with Detective Warrant Officer.
106 Grobler, *Crossing the Line: When Cops Become Criminals*, 177.

While police respondents mostly take the view that the spying scandals in South Africa are the work of a few 'bad apples', researchers on police corruption have already noted that 'corrupt behaviour, for which an individual or a few individuals are initially blamed, turns out to be part of an organised and more extensive system weakness, reinforced by the tolerance of non-participating officials or commanders'.[107] Just as rotten barrels make rotten apples, law-enforcement institutions that fail to protect against the abuse of spying powers are likely to be riddled with people who abuse their spying powers.

Any attempt to tackle these challenges should be tempered with the knowledge that bad actors will always seek out a loophole: a point made by several officials interviewed in this research. The former Hawks investigator, who was in general in favour of building safeguards around interception procedures, was still cautious about the limits of safeguards:

> *If a person wants to get a journalist's phone records ... I don't care if you put five judges on the panel, they're going to get it anyway.*[108]

While most interviewees tempered their proposals with some dose of cynicism, only one – the sceptical State Advocate – argued that this rendered any reform proposals moot. An interview in his office ended up in a circular debate:

Yes, he allowed, the procedures in Section 205 have been abused, but only because investigators made false claims in their applications. The procedures are therefore adequate when investigators are honest in their applications. Surely, he was asked, safeguards are inadequate if they only prevent wrongdoing when nobody is seeking to do wrong. He responded that the problem is not the procedures: as long as everyone is honest in their application, the procedures are adequate.[109]

We can only hope that the conversation moves past that point.

107 Newham and Faull, 'Protector or Predator? Tackling Police Corruption in South Africa', 13.
108 Interview with former Hawks investigator.
109 Interview with State Advocate B.

6 Citations

ACLU of California. 'Metadata: Piecing Together a Privacy Solution', February 2014. https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf.

Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Parliament of the Commonwealth of Australia, 15 February 2015. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report.

amaBhungane and Another v the Minister of Justice and Correctional Services and Others, No. 2598/17 (North Gauteng High Court of South Africa September 2019).

Amici Curiae submission. *amaBhungane and Another v the Minister of Justice and Correctional Services and Others*, No. 2598/17. Accessed 29 May 2019.

Applicants' founding affidavit. *amaBhungane and Another v the Minister of Justice and Correctional Services and Others*, No. 2598/17. Accessed 29 May 2019.

Big Brother Watch and Others v The United Kingdom [2018] ECHR 722 (n.d.).

Burgess, Annelise. *Heist! South Africa's Cash-in-Transit Epidemic Uncovered*. Cape Town: Penguin Books, 2018.

CIGI-Ipsos. '2018 CIGI-Ipsos Global Survey on Internet Security and Trust', 2018. www.cigionline.org/internet-survey-2018.

Constitution of the Republic of South Africa (n.d.).

Criminal Procedure Act, Act 51 of 1977 (n.d.).

Department of Justice answering affidavit. *amaBhungane and Another v the Minister of Justice and Correctional Services and Others*, No. 2598/17. Accessed 29 May 2019.

Duncan, Jane. 'Communications Surveillance in South Africa: The Case of the Sunday Times Newspaper'. In *Global Information Society Watch 2014: Communications Surveillance in the Digital Age*, 2014.

———. *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*. Johannesburg: Wits University Press, 2018.

Grobler, Liza. *Crossing the Line: When Cops Become Criminals*. Pretoria: Jacana, 2013.

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.

Hunter, Murray, and Tymon Smith. 'Spooked: Surveillance of Journalists in South Africa'. Right2Know Campaign, July 2018. https://r2k.org.za/spooked.

Institute for Security Studies, and Corruption Watch. 'State Capture and the Political Manipulation of Criminal Justice Agencies', Joint Submission to the Judicial Commission of Inquiry into Allegations of State Capture, April 2019.

Intelligence Services Oversight Act 40 of 1994. http://www.justice.gov.za/legislation/acts/2002–070.pdf. Accessed 21 May 2019.

International Principles on the Application of Human Rights to Communications Surveillance, 2013. https://necessaryandproportionate.org/.

Mare, Admire, and Jane Duncan. 'An Analysis of the Communications Surveillance Legislative Framework in South Africa'. Media Policy and Democracy Project, November 2015.

Minister of Police notice of appeal. *amaBhungane and Another v Minister of Justice and Correctional Services and Others*, No. 278/19. Accessed 7 January 2019.

Newham, Gareth, and Andrew Faull. 'Protector or Predator? Tackling Police Corruption in South Africa'. ISS Monograph Number 182, August 2011.

Niekerk, Anna-Marie van. 'The Analysis of a Cell Phone Record as a Source of Intelligence in the Investigation of Copper Cable Theft'. Master's Thesis, University of South Africa, 2015.

Pinetown Magistrates Court. M201/08/2016, No. M201/08/2016 (n.d.).

Police answering affidavit. *amaBhungane and Another v the Minister of Justice and Correctional Services and Others*, No. 2598/17. Accessed 29 May 2019.

RICA, Act 70 of 2002. Accessed 21 May 2019. http://www.justice.gov.za/legislation/acts/2002–070.pdf.

S v Brown and Others (CC 18/2017) [2019] ZAECPEHC 11; [2019] 2 All SA 552 (ECP) (5 February 2019) (n.d.).

S v Scheepers, No. SH7/38/16 (n.d.).

S v Shange and Others (CC169/07) [2012] ZAKZPHC 69 (29 June 2012) (n.d.).

Schmitz, Peter, and others. 'Breaking Alibis Through Cell Phone Mapping'. In *Crime Mapping Case Studies: Successes in the Field*, Vol. 2. Police Executive Research Forum, 2000.

Schmitz, Peter, Shareen Riley, and Joe Dryden. 'Mapping Time and Space as a Forensic Tool'. *PositionIT*, September 2010.

State Security Agency answering affidavit. *amaBhungane and Another v the Minister of Justice and Correctional Services and Other*s, No. 2598/17. Accessed 29 May 2019.

Swart, Heidi. 'Big Brother Is Watching Your Phone Call Records'. *Daily Maverick*, 10 May 2017. https://www.dailymaverick.co.za/article/2017-05-10-op-ed-big-brother-is-watching-your-phone-call-records/.

The Quality of Democracy and Governance in South Africa. *Afrobarometer Round 7*. Afrobarometer, 2018. https://afrobarometer.org/sites/default/files/publications/Summary%20of%20results/saf_r7_sor_13112018.pdf.

UN High Commissioner on Human Rights. 'The Right to Privacy in the Digital Age', June 2014. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.

———. 'The Right to Privacy in the Digital Age', August 2018. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx.

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit **mediaanddemocracy**.com for more information.

This report was supported by a grant from the Open Society Foundation for South Africa (OSF-SA)

OPEN SOCIETY FOUNDATION
FOR SOUTH AFRICA