

Operational Security: Failure Within the South African Government

OSINT Industries
21st February 2024



Executive Summary

The disclosure of South African parliament members' personal contact details on parliament.gov.za has inadvertently magnified their vulnerability to operational security threats. The practice of publishing personal emails and phone numbers, divergent from the typical use of official parliamentary addresses, creates a significant security gap.

This information, easily enriched through OSINT (Open Source Intelligence) tools, lays out a comprehensive digital footprint of the legislators, from their personal habits to their private engagements, documented through extensive public Google reviews, fitness app data and more. The straightforward access to such a depth of personal exposure elevates the risk of espionage and opens numerous avenues for targeted influence campaigns & spying. The current state of affairs highlights an urgent need for a stringent review and rectification of privacy protocols to mitigate the potential exploitation of this information.

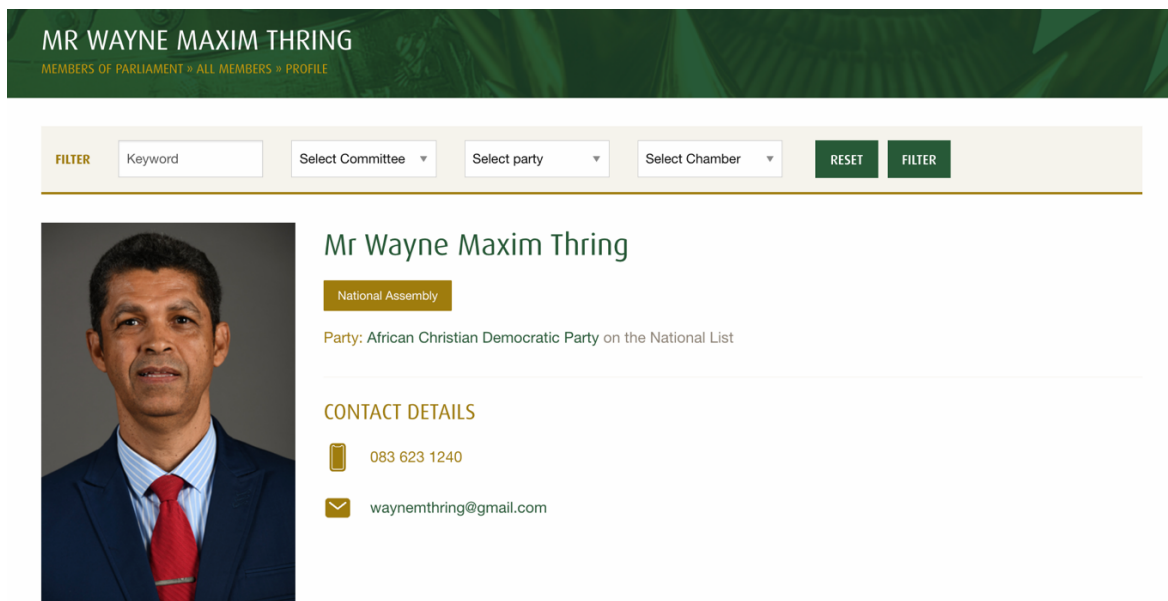
Key Takeaways:

- Espionage, targeted influence campaigns, and spying activities are made trivially easy through simple OSINT enrichment of listed contact details using commercially available tools.
- Legislators have exposed their families, patterns of life, domestic & international traveling arrangements & history, personal lifestyles and more, to the internet.
- Parliamentarians have left over 1,500 public Google reviews using officially listed emails showing intimate travel details, including where they like to dine, take holidays, receive medical treatment and more...
- Some members of the legislative body have registered and are using Strava accounts with their publicly listed emails and are leaking real-time GPS data of where they are, including historic runs and cycles which give away where they and their family live along with making them easy kidnapping targets.
- Some members of the legislative body have registered and used Airbnb accounts on their listed emails and used these to book international and domestic travel, including to locations such as Dubai.

This research will highlight some of the operational security risks presented by the exposure of extensive PII on the internet by almost every legislator within the South African Government.


Context & Data Gathering

The website for the Parliament of South (parliament.gov.za) has published the mostly personal phone numbers and email addresses of every member of parliament. Publishing contact details for parliamentarians is a practice that most every country in the world undertakes. What makes South Africa different is that it has published (in most cases), the personal email and phone numbers of members of Parliament rather than the more corporate @parliament.gov.za emails that most countries utilise for official work.



MR WAYNE MAXIM THRING
MEMBERS OF PARLIAMENT » ALL MEMBERS » PROFILE

FILTER Keyword Select Committee Select party Select Chamber RESET FILTER

 Mr Wayne Maxim Thring

National Assembly

Party: African Christian Democratic Party on the National List

CONTACT DETAILS

083 623 1240

waynemthring@gmail.com

Figure 1 - Legislator Mr Wayne Maxim Thring has a personal Gmail listed as his official email on Parliament.gov.za.
Source: <https://www.parliament.gov.za/person-details/357>

Utilising personal emails for government work is a tried and tested bad idea^{1 2 3}. It exposes parliamentarians to complicated freedom of information (FOI) requests that could violate their privacy, entrusts unvetted email providers with potentially top-secret national security and classified government information along with drastically increasing the chances of a data leak.

Third party websites such as the Peoples Assembly (pa.org.za), run by mysociety.org (a non profit), curates the parliamentary information and publishes it in a more machine (and user) friendly manner.

¹ <https://nypost.com/2023/03/18/federal-officials-are-still-using-personal-emails/>

² <https://www.tsl.texas.gov/slrn/blog/2015/11/using-personal-email-for-government-business-is-a-bad-idea-heres-why/>

³ https://www.dol.gov/sites/dolgov/files/SOL/files/Ethics-and-Use-of-Social-Media_2020.pdf

Investigation

Taking the 600 or so emails published on the parliament.gov.za website and using the automated OSINT tool, OSINT.Industries returns several thousand profiles being used on both @parliament.gov.za and personal email addresses that represent operational security risks.

OSINT Industries provides real-time intelligence, focusing on discovering the digital footprint of selectors (phone numbers and email addresses).

A wide range of accounts are registered on the parliamentarians' emails:

Website	Website	Website	Website	Website					
microsoft	628	bible	49	fitbit	12	xvideos.com	5	bodybuilding.com	2
skype	451	eventbrite.com	47	myfitnesspal	11	zoho.com	4	activision.com	2
google	241	pinterest.com	45	talent.com	11	myspace.com	4	bitmoji.com	2
maps	234	playgames	36	firefox.com	10	envato.com	4	poshmark	2
apple	204	airbnb	36	etsy	10	notion	4	any.do	2
facebook	185	academia.edu	36	paypal.com	9	runkeeper	4	pandora	2
linkedin	177	quora.com	33	edx.org	9	deezer.com	4	gaana.com	2
youtube	151	soundcloud.com	33	flickr	8	pornhub.com	4	indiatimes.com	2
dropbox	141	goodreads	32	care2.com	8	vsco	3	callofduty.com	1
apple.com	126	nike.com	17	gravatar	8	uber.com	3	calendar	1
change.org	112	picsart	16	smule	7	aboutme	3	redtube.com	1
samsung.com	103	duolingo	15	foursquare	6	yelp	3		
instagram.com	101	vivino	14	smule.com	5	imvu	3		
spotify.com	75	strava	14	github	5	dhgate.com	3		
twitter.com	71	garmin	14	khanacademy	5				

This is a pretty standard distribution of accounts for individuals to have on their personal accounts. It is not however a normal distribution to have on a corporate, let alone legislative, email. In most government environments emails are limited to registering on purely corporate services such as Microsoft, Notion, Eventbrite, LinkedIn, with a few rare exceptions for specialised roles such as social media managers.

Some of the accounts that parliamentarians have registered are mundane. Take Goodreads for example. All the Goodread accounts belonging to parliamentarian emails are:

URL	Reviews Count
https://www.goodreads.com/user/show/110900074-julius-malema	1
https://www.goodreads.com/user/show/43041321-tandi	3
https://www.goodreads.com/user/show/26812099-veronica-mente	0
https://www.goodreads.com/user/show/58574294-alexandra-abrahams	4
https://www.goodreads.com/user/show/83333603-patsy-bagraim	0
https://www.goodreads.com/user/show/48383886-darren-bergman	44
https://www.goodreads.com/user/show/128780366-floyd-shivambu	0
https://www.goodreads.com/user/show/12078789-jacques-smalle	3
https://www.goodreads.com/user/show/174358930-ian-de	8
https://www.goodreads.com/user/show/8440751-angel	0
https://www.goodreads.com/user/show/71542028-kevin	0
https://www.goodreads.com/user/show/23558135-lindiwe-zulu	0
https://www.goodreads.com/user/show/21247663-shelley-makhubela	0

https://www.goodreads.com/user/show/47827947-machwene	1
https://www.goodreads.com/user/show/118756684-manny-de	1
https://www.goodreads.com/user/show/93180351-thandeka-mbabama	0
https://www.goodreads.com/user/show/156837392-mncedisi	7
https://www.goodreads.com/user/show/169986871-qanief-hendricks	1
https://www.goodreads.com/user/show/107873448-nicholas-myburgh	0
https://www.goodreads.com/user/show/29116859-lithas	6
https://www.goodreads.com/user/show/35981064-ntshabap@gmail-com	1
https://www.goodreads.com/user/show/43859161-bheki-ghudelimzwezwe	13
https://www.goodreads.com/user/show/101050541-lorato-f	4
https://www.goodreads.com/user/show/96937165-sindile-madlingozi	4
https://www.goodreads.com/user/show/134583258-sam-matiase	0
https://www.goodreads.com/user/show/156539901-samantha-graham-mar	85
https://www.goodreads.com/user/show/93629145-sbongile	1
https://www.goodreads.com/user/show/167026965-m-kruger	0
https://www.goodreads.com/user/show/150043770-muhle	1
https://www.goodreads.com/user/show/128161873-wilma-newhoudt-druchen	5
https://www.goodreads.com/user/show/19793124-yoliswa	1
https://www.goodreads.com/user/show/136564702-zola-mlenzana	4

The top user of Goodreads amongst the registered accounts with 85 books reviewed is Ms Samantha Jane Graham. She was elected to the National Assembly of South Africa in the 2019 general election as a member of the Democratic Alliance. Graham has been the party's Shadow Minister of Electricity since 2023⁴.



Figure 2 – The ‘currently reading’ section of Ms Samantha Jane Graham’s profile on Goodreads (<https://www.goodreads.com/review/list/156539901-samantha-graham-mar?shelf=currently-reading&view=covers>)

Information on what people are reading can seem mundane and uninteresting, but in the building of a pretextual attack it could provide valuable insights into a personality that can be leveraged against parliamentarians in social engineering (SE) attacks. A single Goodreads account alone, is unlikely to pose a risk.

Different parliamentarians use their Goodreads accounts different amounts, while most don’t have any account at all. Each account that a member of parliament has registered and posted information on is leaking information to potential hostile actors. In most cases (including Goodreads) this information is not risky to share, but when combined across tens of accounts and used to build a detailed profile, it can be weaponised.

⁴ <https://www.parliament.gov.za/person-details/72>

Overall Goodreads does not represent an existential threat to the South African legislator, but it is a good lead into some more problematic accounts.

Some of the accounts present a much larger risk to parliamentarian’s security. The largest of them being Google Maps (due to the scale of information available). Parliamentarians have left over 1800 public reviews across the world since 2015 using their officially listed emails.

Location & frequency of reviews:

<i>Year</i>	<i>Location</i>	<i>Review Frequency</i>
2024	South Africa	99
2023	South Africa	379
2023	Mauritius	9
2023	Thailand	3
2023	Malaysia	39
2023	Singapore	9
2023	United Arab Emirates	18
2023	Jersey	2
2023	United Kingdom	1
2023	Israel	39
2022	South Africa	318
2022	India	3
2020	South Africa	410
2020	Israel	7
2020	France	3
2020	Hong Kong	9
2018	South Africa	114
2018	Italy	12
2018	Thailand	5
2018	Mauritius	3
2019	South Africa	155
2019	Israel	2
2019	Zambia	1
2019	Egypt	3
2024	South Africa	99
2021	South Africa	80
2017	South Africa	48
2017	Thailand	3
2017	United Arab Emirates	1
2016	South Africa	3
2015	South Africa	9

Information disclosed in these reviews includes:

Review Type	Operational Risk
Medical Facility Reviews	<p>Reviews left at medical facilities are disclosing, in many cases, intimate personal medical details including treatment elected officials or their family are undergoing.</p> <p>Risk: Hostile agents can infiltrate medical facilities with relative ease, knowing where to target to get potentially compromising information on members of the parliament.</p>

<p>Foreign Travel Reviews</p>	<p>Reviews left across the world during foreign travel, including at night clubs, hotels that are regularly visited and more. Disclosing publicly your foreign travel, including to Dubai and other nations with ambiguous security controls, is a bad idea for an individual, and even worse for a parliamentarian.</p> <p>Risk: Foreign travel plans, especially unofficial travel, is the highest risk activity legislators undertake. Publicly reviewing hotels, destinations, night clubs and tourist locations provides ample information to a foreign intelligence agency to easily run influence operations.</p>
<p>Negative Reviews</p>	<p>Reviews left in anger attacking businesses including complaining about lost money, bad service and disclosing complaints.</p>
<p>Frequent Service Reviews</p>	<p>Reviews left at places that parliamentarians frequent provides detailed information to potential threat actors on pattern of life (when and where they go for services such as check-ups, haircuts, coffee), along with information on where they and their families live.</p> <p>Risk: Pattern of life information including where members of parliament periodically dine, or purchase services is valuable information to anyone looking to target or do harm to them.</p>
<p>Family Reviews</p>	<p>Reviews left at places for members of their families, including private schools for children (both locally and internationally), family services and family-owned businesses.</p> <p>Risk: Exposes personal information including on potential kidnap targets (children of parliamentarians).</p>

Google reviews, along with Yelp reviews, pose a potential inadvertent leakage of information parliamentarians may not realise could be weaponised against them. Strava takes the risk one step further leaking parliament members potentially live location, along with historic running routes.

Strava has been used in the past to allegedly assassinate people ⁵and uncover top secret American military bases⁶.

⁵ <https://www.cnn.com/2023/07/11/europe/russian-submarine-commander-killed-krasnador-intl/index.html>

⁶ <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>

There are 14 members of the SA parliament that have Strava accounts. Some are not using them, but several are actively using them as recently as yesterday.

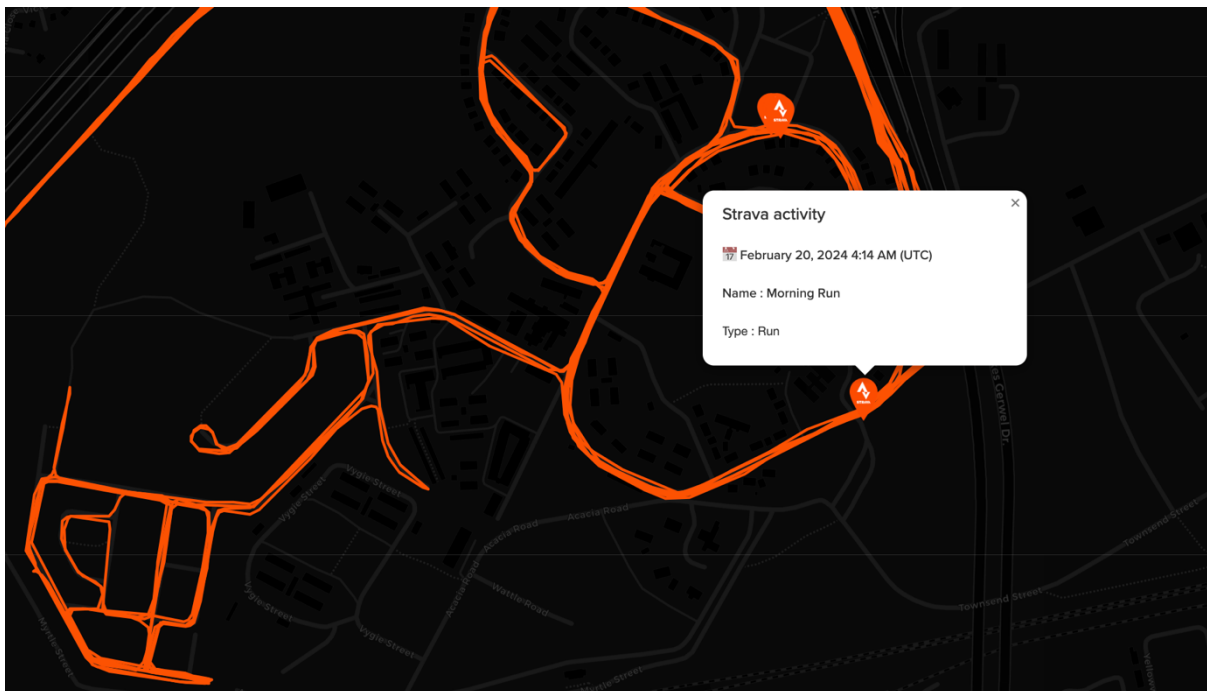


Figure 3 – Strava running route from 1 day ago from a parliamentarian from the South African government

Strava can (and is) utilised by malicious actors to discover when and where people are, conduct kidnappings, organise home robberies when people are out on runs and more. Strava leaks (in many cases) your personal address as it is the location you start your run at.

Conclusion, Suggested Actions, and Next Steps

The prevalent exposure of South African parliament members' personal information online poses serious security threats. This exposure, through the use of personal contact details for public and official purposes, has led to a digital footprint that could be exploited for espionage and malicious targeting.

Suggested Actions:

1. Immediate transition to using official parliament.gov.za email addresses for all legislative work to contain the spread of personal data.
2. Conduct a comprehensive audit of all current personal email and phone number listings, with a swift removal process.
3. Implement mandatory operational security training for all parliament members and associated staff, focusing on the risks of sharing personal information online.