DIGITAL PROFITEERS

WHO PROFITS NEXT FROM SOCIAL GRANTS?

An Open Secrets Investigation

Published by Open Secrets in November 2021

Second Floor Community House
41 Salt River Road
Salt River, Cape Town 7925

+27 21 447 2701

+27 72 565 0173

www.opensecrets.org.za

researcher@opensecrets.org.za

@OpenSecretsZA

@OpenSecrets.org.za

@opensecrets_za

YouTube: Open Secrets

LinkedIn: OpenSecretsZA

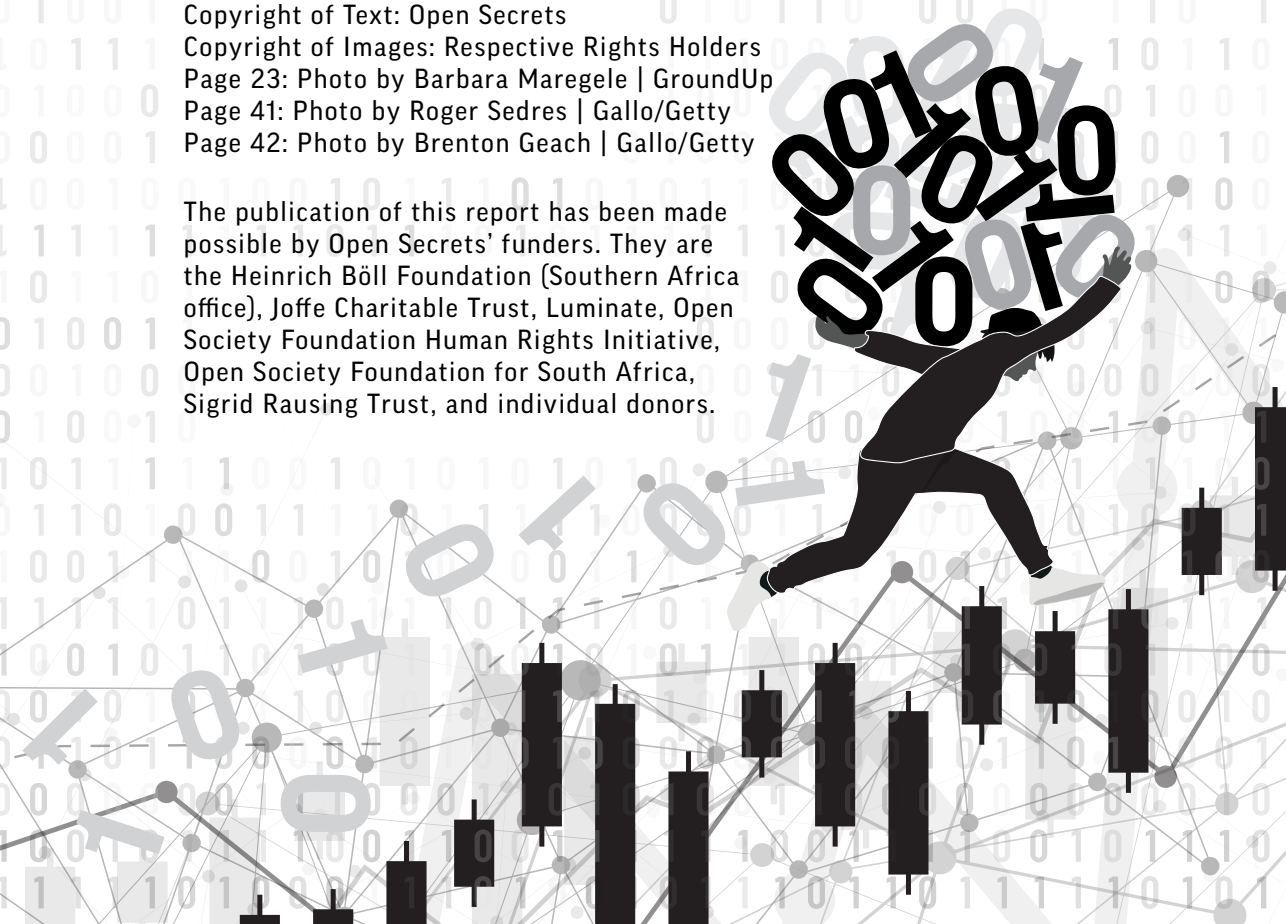
To communicate with us securely visit our website for more details:
www.opensecrets.org.za/#contact

NPC number: 2017/078276/08

Research by Michael Marchant, Abby May, Erin Torkelson, and Zen Mathe
Copy Editor: Kudrat Virk | www.inksmartediting.com
Designer: Gaelen Pinnock | www.polygram.co.za

Page 23: Photo by Barbara Maregele | GroundUp
Page 41: Photo by Roger Sedres | Gallo/Getty
Page 42: Photo by Brenton Geach | Gallo/Getty

The publication of this report has been made possible by Open Secrets' funders. They are the Heinrich Böll Foundation (Southern Africa office), Joffe Charitable Trust, Luminate, Open Society Foundation Human Rights Initiative, Open Society Foundation for South Africa, Sigrid Rausing Trust, and individual donors.



DIGITAL PROFITEERS

WHO PROFITS NEXT FROM SOCIAL GRANTS?

An Open Secrets Investigation

2021

open secrets

power & profit | truth & justice

NUMBERS AT A GLANCE:

13 MILLION

THE NUMBER OF PEOPLE WHO APPLIED FOR THE COVID-19 SRD GRANT IN THE FIRST MONTH AFTER IT WAS REINTRODUCED IN AUGUST 2021.

8 MILLION

OF THOSE 13 MILLION APPLICANTS, THE NUMBER THAT RECEIVED THE R350 GRANT.

61.5%

THE PROPORTION OF APPLICANTS FOR THE COVID-19 SRD GRANT WHO COULD NOT COMPLETE THE APPLICATION DUE TO INSUFFICIENT CELLULAR DATA DURING THE FIRST PHASE IN 2020.

25.5%

THE PROPORTION OF GRANT RECIPIENTS SURVEYED IN OCTOBER AND NOVEMBER 2016 WHO SAID THAT MONEY WAS DEDUCTED FROM THEIR GRANTS WITHOUT CONSENT.

R75 trillion

amazon

Google

THE COMBINED MARKET VALUATION OF APPLE, AMAZON, ALPHABET (GOOGLE'S PARENT COMPANY), AND FACEBOOK.

CAPITAL APPRECIATION

R20 MILLION

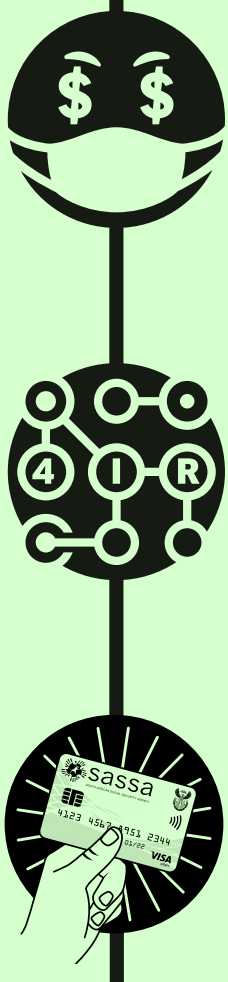
CAPPREC'S INVESTMENT IN GOVCHAT VIA ITS ENTERPRISE DEVELOPMENT FUND. IT NOW HOLDS A 35% STAKE IN GOVCHAT.

govchat

RO

THE AMOUNT GOVCHAT CHARGED SASSA FOR ESTABLISHING THE DIGITAL APPLICATION PLATFORM FOR THE COVID-19 SRD GRANT.

TABLE OF CONTENTS



ABBREVIATIONS

- **4IR** Fourth Industrial Revolution
- **AI** artificial intelligence
- **AGSA** Auditor-General of South Africa
- **ARC** African Rainbow Capital
- **B-BBEE** Broad-Based Black Economic Empowerment programme
- **BSP** business service provider
- **CAPPREC** Capital Appreciation
- **CEO** chief executive officer
- **COGTA** Department of Cooperative Governance and Traditional Affairs
- **CPS** Cash Paymaster Services
- **CSG** Child Support Grant
- **DRC** Democratic Republic of the Congo
- **DSD** Department of Social Development
- **EU** European Union
- **fintech** financial technology
- **GDPR** General Data Protection Regulation (European Union)
- **HANIS** Home Affairs National Identification System
- **ID** identification
- **IFC** International Finance Corporation
- **JSE** Johannesburg Stock Exchange
- **NPS** National Payment System
- **NSFAS** National Student Financial Aid Scheme
- **OAG** Old Age Grant
- **OTT** over-the-top (messaging)
- **PAIA** Promotion of Access to Information Act
- **PERSAL** Personnel and Salary System
- **POPIA** Protection of Personal Information Act
- **SASSA** South African Social Security Agency
- **SOCPEN** Social Pension for Indigent Senior Citizens
- **SRD** Social Relief of Distress grant
- **UEPS** Universal Electronic Payment System
- **UIDAI** Unique Identification Authority of India
- **UIF** Unemployment Insurance Fund
- **UK** United Kingdom
- **U.S.** United States
- **USSD** Unstructured Supplementary Service Data
- **WABA** WhatsApp Business account

KEY TERMS

BIOMETRICS

The physiological and behavioural characteristics of individuals, including fingerprints; voice, face, retina, and iris patterns; hand geometry, gait, and DNA profile. A biometric system uses biometric technologies to capture and store characteristics in a database in order to identify individuals. Information in this database is cross-referenced to verify or authenticate an individual's identity in a range of contexts, such as when accessing government services, crossing borders, voting, accessing bank accounts, and accessing health services.

DIGITAL WELFARE STATE

A term used to describe the use of digital technology systems in state-managed social security programmes. This includes the use of digital technology in administering services related to the provision of social grant benefits, state provision of health care services, and other forms of assistance provided by government departments.

DIGITALISATION

The process of changing existing business models using digitisation. Its purpose is value creation; technology is leveraged to expand a business into new markets, offer new products and services, and appeal to new customers.

DIGITISATION

The process whereby information is converted from a physical format to a digital one.

FINTECH

Short for financial technology, fintech refers to computer programmes and other technology used to create, support, or enable banking and financial services.

FOURTH INDUSTRIAL REVOLUTION (4IR)

An era when people are using smart, connected, and converging cyber, physical, and biological systems and smart business models to redefine and reshape the social, economic, and political spheres.

GRANT BENEFICIARY

An individual who qualifies to receive a social grant. Many beneficiaries are children who do not collect the grant themselves.

GRANT RECIPIENT

An individual who collects the actual payment of a social grant. This can be the beneficiary themself or someone collecting on behalf of a beneficiary, such as a parent collecting on behalf of a child.

MONETISATION OF DATA

The process of generating revenue from data, particularly personal data, collected in various ways. Ways of monetising data include: selling the data a business collects from customers or clients to advertisers, using the data collected to improve sales of products to customers, data analysis of customer behaviour to maximise services, and charging an access fee for a service (or on the rare occasion, access to hardware like a computer).

NATIONAL STUDENT FINANCIAL AID SCHEME (NSFAS)

A South African government student financial aid scheme for undergraduate students to help them pay the cost of their tertiary education. It is funded by the Department of Higher Education and Training.

PERSONNEL AND SALARY SYSTEM (PERSAL)

The government system used for administrating the public service payroll.

PLATFORM

A digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet and digital technology systems. It can be best understood as an intermediary between users that extracts value from their activities on the basis of the data generated. Facebook and Google are quintessential examples of platforms.

SOCIAL PENSION FOR INDIGENT SENIOR CITIZENS (SOCPEN)

The South African Social Security Agency's primary database for beneficiary information management. It is used when processing applications for the old age, disability, war veterans, child support, foster care, and care dependency grants; generating a monthly pay file for more than16 million grants; and automatically producing a list of beneficiaries due to be re-assessed.

UNEMPLOYMENT INSURANCE FUND (UIF)

A fund that provides short-term relief to workers when they become unemployed or are unable to work because of maternity leave, adoption leave, or illness. It also provides relief to the dependants of a deceased contributor. Employers register, declare, and pay UIF contributions taken from employees' salaries.

USSD

Stands for Unstructured Supplementary Service Data. It is a communications protocol used by cellular devices on second-generation cell networks to communicate between the device and the mobile network company's computers. USSD creates a real-time connection that allows for the sharing of data and is thus used regularly for menu-based information services, mobile money services, and various location-based services.

INTRODUCTION: PANDEMIC, PROFIT, AND PRIVACY

The Covid-19 pandemic has dramatically increased global inequality: while millions of people lost their jobs and were pushed into poverty, billionaires increased their cumulative wealth by R55 trillion between March and December 2020.[1] South Africa was already the most unequal country in the world prior to the pandemic, and Covid-19 has made survival more difficult for millions of people. At the time of writing, the official unemployment rate is over 34 per cent and tops 44 per cent when including people who have stopped searching for work.[2]

At the same time, the Johannesburg Stock Exchange (JSE) recovered from its crash in March 2020 and reached record highs by early 2021. While poor and working-class South Africans have suffered losses of income, the most affluent South Africans have sustained or even grown their wealth.

To address some of the worst economic effects of Covid-19, President Cyril Ramaphosa announced a range of social assistance interventions in April 2020, including a new Social Relief of Distress (SRD) grant for unemployed people between the ages of 18 and 59. This was a major development in the South African social assistance landscape, as this age cohort had never previously been able to access benefits. Attesting to the scale of poverty and unemployment, 12 million people applied for this Covid-19 SRD grant and 7 million received it between April 2020 and April 2021 (when it came to a sudden and premature end). In August 2021, after extensive civil society campaigns, led by the Black Sash and #PaytheGrants, the Covid-19 SRD grant was reinstated. By the end of the

first month, 13 million people applied once more for the grant and 8 million people received it.

While the Covid-19 SRD grant is a vital social initiative, the pandemic introduced changes to the grant application and distribution system that have not been sufficiently investigated. This report focuses on one of these changes, namely how Covid-19 has been used to justify the rapid digitalisation of the welfare state.

For the last five years, the South African Social Security Agency (SASSA) has expressed its intention to "intensify automation of the social grant application processes/systems".[3] However, such efforts were given extraordinary impetus by the onset of the pandemic. Covid-19 is an infectious airborne disease, and in-person government services, with long queues and crowded offices, are perfect grounds for the virus to spread. To protect workers and grant recipients, SASSA had to engineer systems to deliver this grant safely. Since the grant was a new initiative, the qualifying 18–59-year-olds were not already registered on SASSA's Social Pension of Indigent Senior Citizens (SOCPEN) database. SASSA had to rely on three private partners – GovChat, Vodacom, and Prosense – to design a registration process for this age cohort, using WhatsApp, **Unstructured Supplementary Service Data (USSD),** and web and email platforms, respectively. It is worth mentioning that other government agencies were also contracting with private service providers to digitise social services during this period, including the Department of Health, first for Covid-19 testing and then for the national vaccination roll-out.

KEY TERM

UNSTRUCTURED SUPPLEMENTARY SERVICE DATA

USSD is a communications protocol used by cellular devices on second-generation cell networks to communicate between the device and the mobile network company's computers. USSD creates a real-time connection that allows for the sharing of data and is thus used regularly for menu-based information services, mobile money services, and various location-based services.

KEY TERM

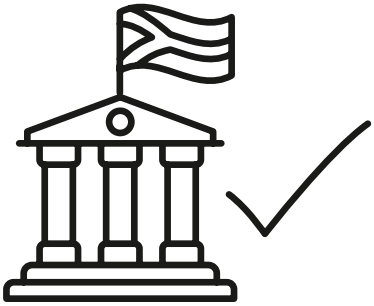
DIGITALISATION

In this report, we choose to use the term digitalisation. This differs from digitisation which simply refers to the process whereby information is converted from a physical format to a digital one. Digitalisation is the process of changing existing business models using digitisation. Its purpose is value creation; technology is leveraged to expand a business into new markets, offer new products and services, and appeal to new customers. It is this term that is used in this report as it makes explicit the use of data and technology to benefit private businesses.

Globally, there has been inadequate scrutiny of how companies are profiting from their access to personal data gathered through government contracts under the auspices of providing public services. When there is inadequate regulation and poor transparency, these new digital developments can create possibilities for massive profit taking on the part of corporations and greater political control by the state. Both are achieved through the surveillance of individuals via the data they submit to access social protection guaranteed by the Constitution.

In this report, we focus on GovChat, a small South African technology company, and SASSA's most visible partner in its digitalization drive. In early 2020, GovChat offered its services to SASSA for free to set up a WhatsApp platform for the Covid-19 SRD grant application process. GovChat now appears to be SASSA's partner of choice for its future digitalisation plans and has rolled out a trial application platform for disability grant recipients as well.

GovChat boasts that it provides these services to SASSA at no cost and is primarily concerned with creating social impact. Yet GovChat is financially backed by a few private actors, notably Capital Appreciation (CAPPREC), a publicly listed company predominantly focused on financial technology (fintech). Through its relationship with SASSA, GovChat has access to the personal data of millions of South Africans, and CAPPREC is keen to "monetise" GovChat's model. This report considers what monetisation could



POPIA – DATA PROTECTION IS A CONSTITUTIONAL IMPERATIVE

The Protection of Personal Information Act (POPIA) was signed into law in 2013. However, it was not until July 2021 that the law came into full effect. POPIA is a vital piece of legislation that seeks to give effect to fundamental constitutional rights, including the right to privacy.[4] In terms of POPIA, everyone is a "data subject"* and has numerous rights in terms of how their personal data is collected, processed, retained, and disseminated. These rights are contained in section 5 of POPIA and should be kept in mind when reading the rest of this report. The rights of all individuals include the following:[5]

- To be notified when your personal information is collected, by whom it is collected, and why it is being collected.
- To find out, free of charge, whether any party holds your personal information, and if so, to access that information. This includes the right to know if any third parties have had access to that information.
- To object to the processing of your personal information and to request that the information be deleted.
- To not be subject to any decision that results in legal consequences – such as whether to receive a social grant – based solely on the automated processing of personal information.
- To object to your personal information being used for direct marketing through unsolicited electronic communication.
- To be notified when your personal information is accessed by an unauthorised person and to be informed of what the possible consequences of the data breach may be.

POPIA also established the Information Regulator, an independent regulatory body tasked with monitoring and enforcing the Act and its provisions.[6] However, as we discuss in more detail in the report, the Regulator has been consistently under-resourced by the state which raises concerns about the body's capacity to tackle the extensive and far-reaching data protection issues that it will face in the coming years. Speaking to journalists in August 2020, a member of the Information Regulator, Professor Sizwe Snail ka Mtuze said: "Right from the beginning, the office of the regulator was really given a minute budget... we are in discussion with [National] Treasury, we are in constant discussion every year".[7]

This is concerning because international experience shows that while impressive strides have been made towards enshrining data rights in many places, the regulation and enforcement of those laws and protection of rights has been inconsistent at best. A recent European Commission review of the European Union's (EU's) General Data Protection Regulation (GDPR) – which contains many of the same rights enshrined in POPIA - raised serious concerns about inconsistent enforcement of the law, particularly against large technology firms like Facebook, in part due to a lack of resources for regulatory bodies.[8]

As we argue in this report, a well-resourced, functioning, and energetic Information Regulator is vital in ensuring that any possible abuses of a digital welfare system are halted in their tracks. This report raises concerns about the treatment of individuals' data that may amount to breaches of POPIA by state and private actors. As such, we have submitted it to the Information Regulator for investigation and urgent follow-up.

*"Data subject" simply means the person to whom personal information relates.

look like, and why we should be concerned about many possible paths that put profit over human rights. GovChat may be offering its services for free now, but at what cost?

This report argues that GovChat is making a "data play". Eldrid Jordaan, Chief Executive Officer (CEO) of GovChat, initially used this term in an interview with Open Secrets to describe Facebook's business strategy. But we argue that it can be applied to GovChat as well. GovChat has substantial backing from CAPPREC precisely because it is well positioned to design, build, and control the digital systems for social grants in South Africa, during the Covid-19 crisis and beyond. Before the pandemic, SASSA was paying more than 18 million grants to over 11 million beneficiaries, with the significant majority of these payments made up of the Child Support Grant (CSG) and Old Age Grant (OAG).[9] This means that SASSA already held the data of 18 million recipients and beneficiaries on its legacy SOCPEN database. However, the Covid-19 grant has generated a new dataset of at least 13 million individuals, between the ages of 18 and 59, who have declared that they have little or no income.

A fully automated grant application process, including all new and previous records, could thus generate an extraordinary database of the personal information of around half of South Africa's population. The plan to digitise has opened up the possibility that this data will be available to a variety of public and private actors. Access to the personal data of more than 30 million people would constitute the kind of big "data play" that financial and technology firms dream of.

This is not just a concern in South Africa but globally. One hundred and ninety-one countries introduced new social assistance initiatives during the pandemic, and almost all of them made use of digital elements.[10] When the United Nations (UN) Special Rapporteur on Extreme Poverty and Human Rights, Philip Alston, reviewed global efforts to digitise social assistance systems, he warned of the "grave risk of stumbling zombie-like into a digital welfare dystopia".[11]

We do not want to be zombies. We also do not live in a zombie state, where constitutional rights are trampled upon by the powerful in a calculated, devious manner. That being so, we seek to shine a light onto those who seek to profiteer from South Africa's accelerated entry into a digital era of welfare delivery. We follow the story of SASSA's digitisation of welfare over the past decade, starting with its previous contract with Cash Paymaster Services (CPS) before moving on to its current relationship with GovChat. By taking a long historical view, we show the progressive intensification and evolution of data profiteering via social services.

SASSA already has a poor record of protecting vulnerable grant recipients from the predatory conduct of private actors that seek to profit from access to their information and data. The first case study in this report speaks in detail of how it failed to hold Net1 and CPS to account for their abuse of the grants process. This failure is a stark warning that the digitalisation process led by SASSA with GovChat as its partner, in particular how the process is controlled and regulated, requires ever greater scrutiny. Without this, digital profiteers in the private sector will be lining up at the trough.

NOTE ON TERMINOLOGY:

DIGITAL PROFITEERS

Throughout this report we refer to the role of private companies in "profiteering" from access to our data. The use of this term is deliberate. We mean "profiteer" in the sense that companies generate excessive or unfair profits from systems that harm vulnerable people. This does not mean that the conduct of these profiteers is always unlawful; often it is not. That is not accidental. Writing about the role of large technology companies in the United States (U.S.), Harvard University's Shoshana Zuboff has argued that these companies have operated at a new frontier of capitalism and used their power, wealth, and access to vigorously resist attempts to regulate their activities.[12]

By arguing that attempts to regulate them will stifle innovation, these companies have created and operated in a "human rights free zone",[13] and all other concerns have been subordinated to their relentless pursuit of super profits. South Africa is no different, with legislative mechanisms and regulation of the digital space playing catch-up with the capabilities and reach of technology firms. The case studies in this report should be viewed against the nascency of regulation and legal mechanisms to hold these private actors accountable.

What is in this report?

Chapter One Chapter 1 offers a brief introduction to South Africa's intention of benefitting from a Fourth Industrial Revolution (4IR). This is examined against critical literature on the digitalisation of public services.

Chapter Two Chapter 2 looks to the past and revisits the story of Net1 and its subsidiary, CPS, between 2012 and 2018. Net 1's monopolistic control of the grant payment system allowed it to aggressively sell financial products to grant recipients and engage in making unlawful deductions from social grants.

Chapter Three Chapter 3 looks to the present and discusses the rise of GovChat as SASSA's new partner of choice in digitalising social welfare. It traces how GovChat's angel investors are seeking financial returns on this project by monetising the personal data of grant recipients.

Chapter Four Chapter 4 looks to the future and discusses the possible risks for grant recipients from digitalisation. Using the Aadhaar identification (ID) system in India as a case study, we show how promises of efficiency and accessibility are often oversold, and that digital processes are often exclusionary and ineffective. We also detail concerns about the security of the data gathered, and the ability of companies and states to use that data to surveil citizens.

Chapter Five Chapter 5 concludes the report and provides recommendations, including the urgent need to demand greater transparency in how digital processes work, effective regulation of the companies profiting from these processes, and equitable access to digital tools.

> "[There is] a grave risk of stumbling zombie-like into a digital welfare dystopia"
>
> **~ Philip Alston**
> United Nations Special Rapporteur
> on Extreme Poverty and Human Rights

If the digital future is to be our home, it is we who must make it so.[1]

1

SOUTH AFRICA'S 4IR FUTURE: A BIG DATA BONANZA

Covid-19 has raised many profound human rights issues, which begs the question: why are we focusing on data and digitalisation? South Africa is moving toward a digital future, and Covid-19 has provided the rationale to accelerate that future. President Cyril Ramaphosa and many South African government departments are enthusiastic about the so-called Fourth Industrial Revolution. According to Klaus Schwab, who coined the term, instead of old production-centric industries, the Fourth Industrial Revolution will be characterized by the fusion of digital, biological, and physical processes through the growing use of artificial intelligence (AI), cloud computing, wireless technologies, digital currencies, and big data, amongst many others.[2] Schwab, it should be remembered, is one of the original "influencers" of the modern era, the person behind the annual Davos meeting. Schwab's World Economic Forum brings together the globe's richest and most powerful for "agenda setting" which profoundly impacts billions of people who have no seat at the table with the denizens of Davos. Such are the origins of the Fourth Industrial Revolution.

Ramaphosa established a Presidential Commission on the Fourth Industrial Revolution to provide guidance on how to stimulate it in South Africa.[3] Likewise, his son, Tumelo Ramaphosa, attempted to host an elite AI and blockchain conference in 2019.[4] Mpho Dagada, a member of the Presidential Commission on the Fourth Industrial Revolution and author of *Mr Bitcoin: How I*

Became a Millionaire at 21, has been tasked with planning a similar conference for March 2022.[5]

The many efforts to kick-start a homegrown Fourth Industrial Revolution have proceeded largely without comment. Yet this complacency needs to be challenged. The Fourth Industrial Revolution is made possible by the rapid acceleration of global capacity to "store, communicate and compute information".[6] Business magazines have referred to this information or data as the "new oil", highlighting its capacity as a precious commodity that stores value. Big and small corporations, as well as public and non-governmental organizations, have hopped on the bandwagon to "mine" this "new oil" for profit.

Shoshana Zuboff, author of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, describes how the largest technology companies today – notably Google and Facebook – create new sources of value by capturing our personal information and the mundane details of our daily lives through our phones and computers, with and without our consent. Google and Facebook collect information on where we go, who we are, what we like, and what we think. [7] Such data collection is an emerging frontier of capitalism that commodifies human experience.[8]

A COUNTER TO ZUBOFF

A key criticism of Zuboff's thesis is that the act of capturing personal information about individuals' daily lives to commodify human experiences is not entirely new. Similar instances have occurred throughout the history of abusive capitalistic systems, from the apartheid migrant labour system's compound hostels to the transatlantic and Indo-Oceanic slave trade. These systems were intimately linked to black or othered bodies. The only differences with surveillance capitalism are that the mechanisms are shifting towards digital tools in an online space, and those who have always been considered the penultimate human (i.e. cishet white men) are no longer excluded from the processes of extraction.

The trend must be more widely understood and subject to public debate to ensure that it does not become a bonanza for exploitation and a torment to the poor and working classes.

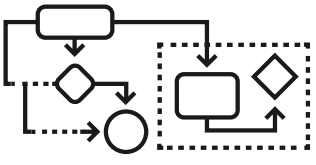
Let us begin by discussing how data is the "new oil" and how corporations profit from gathering it. Technology companies do not make money by producing products like cars or clothing. Rather, millions of users produce the core content of sites like Google and Facebook, and the more data users generate for these companies, the more valuable these companies become.[9] The commodification of data happens in the aggregate: every search or post helps improve the platforms' data analysis functions. Platforms collect data on users' behaviour and then run additional analytics or algorithms to process the data they collect.[10] **Algorithms** analyse that data to improve predictive accuracy about human behaviour and mine the commercial possibilities that arise from the analysis.

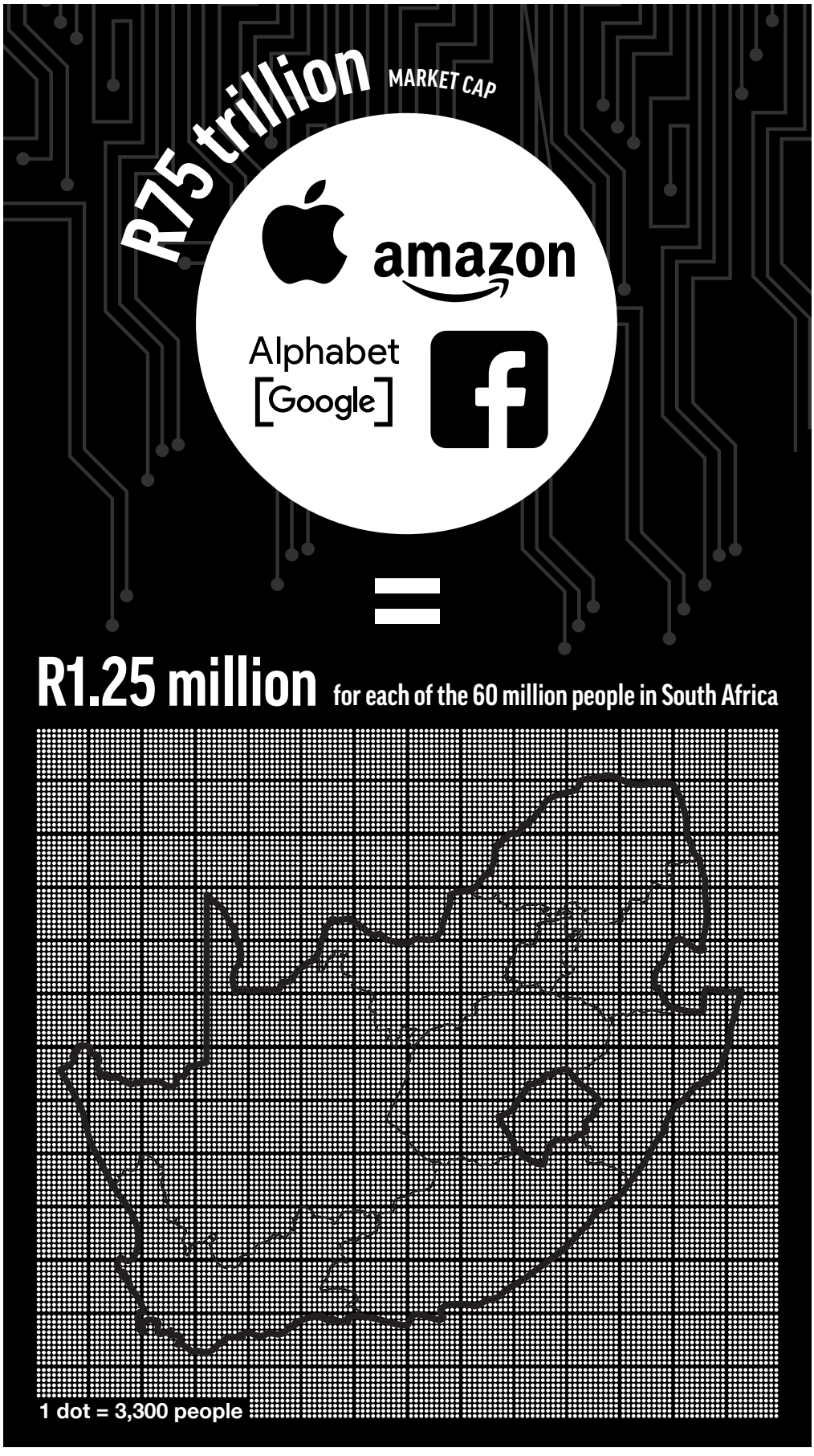
Platforms monetise this data by charging an access fee for their data, selling targeted advertising opportunities, or manipulating user behaviour.[11] As Zuboff compellingly shows, data analysis can be used "to tune and herd and shape and push us in the direction that creates the highest probability of their business' success".[12] For example, in 2014, Facebook conducted a secret experiment on hundreds of users, manipulating their feeds to see if they could create an "emotional contagion" or emotional response to certain products or political issues without the users being aware of it.[13] While companies have long sought to modify behaviour for profit, the ability of technology companies to access, analyse, and sell vast sets of personal data has presented a series of new avenues for profit.

KEY TERM

ALGORITHMS

Algorithms are a set of instructions designed to perform a specific task or solve a specific problem, often used within computer programmes.




R75 trillion
MARKET CAP
amazon
Alphabet
[Google]
=
R1.25 million
for each of the 60 million people in South Africa
1 dot = 3,300 people

Like oil, data is big business. Platforms that commodify data are some of the most profitable companies in history. The combined market valuation of Apple, Amazon, Alphabet (Google's parent company), and Facebook was more than $5 trillion in the second quarter of 2020.[14] To understand the scale of these fortunes and the power they wield, consider: if this market value (R75 trillion) were to be distributed equally amongst all 60 million people in South Africa, every person would receive R1.25 million in their pocket.

Recently, these platforms have become more profitable for their shareholders because the Covid-19 pandemic has led to an unprecedented surge in the use of online platforms for everything from online grocery shopping to accessing healthcare and other social services.[15] When these platforms are used for public services, there is a risk that government services are effectively outsourced to private corporations who then get privileged and monopoly access to personal data.

Companies like Facebook and Google have also routinely shown that they share and sell our personal data without properly explaining that to us. In September 2021, Irish authorities fined Facebook $270 million (R4 billion) for failing to be transparent and disclose to WhatsApp users how the company uses the data it gathers, and particularly how it shares that data with Facebook's many other subsidiaries.[16]

The manner in which data is used to generate profit can appear innocuous at first. As Durham University's Louise Amoore describes, algorithmic models were initially built by finding associations between various items in accumulated data.[17] Using data gathered about supermarket shopping preferences – like through your Clicks, Shoprite, or Checkers card – computers are trained to predict likely associations. For example, shopping data can be used to understand that if a person buys two products (a Coke and chips), they will also likely buy a third (paper serviettes). Serviette companies can pay for this data to draw probable futures from immediate purchasing decisions and target their market toward specific customers.

Such data is also highly attractive to companies selling financial products. For instance, if a person has an income under R100,000 and their browsing history shows searches for design magazines and do-it-yourself YouTube videos, it is likely they will be amenable to taking an unsecured loan for house construction. This cumulative data thus provides "insider" information on human consumption to corporations. While ethically dubious, this is not deemed illicit. This also is one of the explanations for why so many traditional retailers and other companies have accelerated and grown their sale of financial products.

The 4IR agenda becomes particularly worrisome when the commercial possibilities coalesce with national security agendas. Numerous examples reveal how seemingly bland, unimportant data is manipulated with dire consequences. As Amoore reveals, data has political value; for example, if a person has a certain pattern of browsing behaviour, they will be more amenable to political parties and so will be targeted by candidates.[18] More troubling is that in the "war on terror", where the claimed intent is to stop violent actions before they occur, a series of seemingly banal choices captured as data can take on profound and even lethal proportions. If a person pays for their flight ticket in cash, orders a certain meal, and has a flight history deemed "suspicious", a red flag appears on a border guard's screen, and they are denied access into a country. Or, if they are between certain ages, Muslim, and male, they are too easily deemed a combatant and could be subject to a drone strike and almost certain death.

CORPORATIONS AND THE STATE ALIGN: THE DIGITAL WELFARE STATE

We certainly do not want social welfare data, which has been collected for the express purpose of providing for the basic needs of the public, to be used for nefarious purposes. Yet this is already happening globally. The United Kingdom (UK) has already transitioned its extensive system of social assistance onto

a primarily digital platform. An investigation by non-profit organisation Privacy International revealed that these digital processes undermine people's rights to privacy and dignity. Grant recipients are forced to subject themselves to "monitoring and surveillance by the state… facilitated by the private sector", so that UK authorities can identify how benefit money is spent and purportedly stop people fraudulently claiming social assistance.[19]

The UK Department for Work and Pensions calls upon a range of private companies to hand over data about people's income and expenditure to it. This data is combined with the department's ongoing physical and electronic surveillance of grant recipients. The corporations providing the information face little accountability regarding how the department uses the data gathered for its own commercial purposes.[20] Privacy International adds that as a result, poor people in the United Kingdom are increasingly forced to make a difficult choice:

> **"The lack of integration of privacy, data protection, and security within this sector means that individuals are currently having to accept a trade-off between accessing social protection programmes and their fundamental rights to privacy and non-discrimination, amongst others".[21]**

Given South Africa's commitment to a 4IR future, what are the risks when the government partners with private, profit-driven companies to deliver social services? Will we face the same sorts of breaches of privacy and dignity, as well as monetization and surveillance, as the United Kingdom? As part of South Africa's 4IR programme, many government departments are now engaging technology companies to provide public services, blurring the boundary between people as citizens and people as consumers or service users, or the products themselves. The ambiguity stems from the structural weakness of the state to provide services independently. Both hollow and corrupt, the South African state contracts private-sector actors to create or co-create digital services and platforms, due to the technical expertise required to develop these kinds of technologies.[22]

The data collected through these public programmes can be controlled, manipulated, and analysed in different ways for different purposes by both private corporations and governments. Reflecting on similar systems in India, researchers Sudeep Jain and Daniela Gabor note that citizens who "submit themselves to greater *commercial* surveillance become simultaneously (more) vulnerable to the repressive arm of the state".[23] At the same time, citizens who submit themselves to greater *state* surveillance to access services become vulnerable to commercial profiteering as well. This confluence of state and private-sector data capture is nowhere more concerning than in the provision of social assistance like grants.

Such commercial profiteering was typified by the conduct of Net1 and CPS in what we call version 1.0 of digitalising social welfare in South Africa.


sassa
SOUTH AFRICAN SOCIAL SECURITY AGENCY
4123 4567 8951 2344
01/22
VISA
DEBIT

2

NET1 AND CPS: THE DIGITALISATION OF SOCIAL WELFARE

VERSION 1.0

Between 2012 and 2018, South Africa's social grant payment system, designed by Cash Paymaster Services, proved irrefutably how social welfare can be used for profiteering through the sale of financial products.[1] This is a well-known story, though it risks fading from public memory in the wake of state capture and the torrent of corruption stories. In revisiting it and highlighting some of the most pertinent details, we want to show how the more recent developments in South African welfare delivery are part of a longer transition toward a digital welfare state.

The social grant system designed by CPS evolved alongside a global effort to bundle cash transfer payments with so-called "financial inclusion" initiatives. While cash transfer promotes "just giving money to the poor",[2] financial inclusion promotes giving money to the poor in conjunction with a suite of other financial products (such as savings, loans, payments, and insurance).[3] Despite these different stated purposes, mainstream development agencies (like the World Bank) and new development actors (including banks, mobile companies, technology firms, MasterCard/Visa, and think tanks) have advocated for cash transfer payments to be linked with financial products and services.[4]

Financial inclusion advocates say that poverty is not related to an absolute lack of cash but a lack of cash at certain key times.[5] They argue that a broad range of techno-financial products can help people manage their money more effectively, particularly in times of

emergency. Linking savings, credit, and insurance products to social grants seems an obvious way of helping people budget for the future. And yet it also contains the possibility of being inescapably exploitative. As the Chair of the Digital Frontiers Institute, David Porteous, warned in 2006, "The regular cash flow of grant recipients may also make them an attractive target for lenders who may use irresponsible marketing techniques to lead to unsustainable indebtedness."[6]

The South African Social Security Agency contracted CPS, in 2012, to distribute grants nationwide. At the time, this was the second largest government contract ever issued, after the infamously corrupt Arms Deal, which was a R30 billion (at the time) purchase of weapons in 1999. Under the terms of the SASSA contract, CPS was empowered to embark on a massive enrolment drive, collecting the personal information of around **17 million beneficiaries and opening bank accounts for 10 million recipients**.[7] CPS's parent company, Net1 UEPS Technologies, jointly listed on the Johannesburg and New York-based NASDAQ stock exchanges, used its subsidiaries to sell financial products to grant recipients. These products included loans (Moneyline), funeral insurance (Smartlife), airtime and electricity (uManje Mobile), and payments (EasyPay). Even at the start of the contract, SASSA knew CPS's business model included making additional profits by selling financial products and services to grantees.[8]

Net1 and its subsidiaries had unrestricted access to South African grant recipients, both in person and via their electronic data. Net1 could make grant payments, sell financial products, and extract repayments for those products without bearing any risk.[9] Grant recipients could not default on their debts, because Net1 controlled the entire financial flow from the National Treasury into individual bank accounts and could debit those accounts early and automatically. This created immense hardship for grant recipients, who turned to other formal and informal lenders when their grant payments were depleted.

This was a profitable strategy for Net1, which made more money on "financial inclusion" products than from grant distribution between 2015 and 2017.[10] It is difficult to estimate the exact cost to grantees of Net1's control of the data. However, the Black Sash, a leading South African social justice organisation, conducted quarterly surveys with grant recipients at pay points.[11] Between October and November 2016, 25.5 per cent of recipients surveyed nationally said that money was deducted from their grants without consent. In some "hot spots", like Khayelitsha, around 50 per cent of recipients said that they experienced deductions without consent.[12]

> **"I cry every month for my money"**[13]
>
> ~ Grant recipient in an interview with GroundUp

Despite these unethical and unlawful deductions, the largest shareholder in Net1, at the time, was the International Finance Corporation (IFC), the private financial arm of the World Bank. The IFC invested $107 million (over R1.5 billion) to support Net1's expansion into African countries with "limited banking infrastructure and financial services".[14] The IFC intended this support to expand CPS's model worldwide and did not balk at the reports from South Africa of unauthorised deductions from grant recipients.[15]

THE UNLAWFUL CPS CONTRACT

So how did CPS get their foot in the door with SASSA? CPS has a long history with South Africa's social development administration. It had been paying grants in rural provinces since the 1980s (while owned by First Na-

GRANT BENEFICIARIES

A grant beneficiary is an individual who qualifies to receive a social grant. Many "beneficiaries" are children who do not collect the grant themselves. Meanwhile, a grant recipient is an individual who collects the actual payment of a social grant. This can be the beneficiary themselves, or someone collecting on behalf of a beneficiary such as a parent collecting on behalf of a child.

tional Bank), which it continued to do after being purchased by Net1 in the 1990s.[16] We deal with this history further in the next chapter. When SASSA announced that it wanted to consolidate grant payment under one company, CPS emerged as the clear favourite because of its experience paying in relatively remote areas. CPS was chosen in a bidding process which was later ruled invalid by the Constitutional Court in 2013.[17]

AllPay, a subsidiary of ABSA, took SASSA to court over a last-minute change to the tender specifications. The original request for proposals had indicated that it was "preferential" to have **biometric verification capabilities.** Just days before proposals were due, SASSA changed the word "preferential" to "mandatory", ensuring that there was effectively only one company that could be awarded the contract: CPS.[18] While both AllPay and CPS had the capacity to verify recipient biometrics during enrolment, SASSA now specified that they wanted a service provider to be able to do biometric "proof of life" checks every month. CPS claimed to have the capacity to verify grantees via fingerprint or voice biometrics each month, though the latter never worked and was stopped. The Constitutional Court ruled that this last-minute

KEY TERM

BIOMETRICS

Biometrics refers to the physiological and behavioural characteristics of individuals, including fingerprints; voice, face, retina, and iris patterns; hand geometry, gait, and DNA profile. A biometric system uses biometric technologies to capture and store characteristics in a database in order to identify individuals. Information in this database is cross-referenced to verify or authenticate an individual's identity in a range of contexts, such as when accessing government services, crossing borders, voting, accessing bank accounts, and accessing health services.

change reduced the number of viable bids to one and precluded a proper comparison of costs.[19]

Despite these contractual irregularities, the Constitutional Court decided to allow CPS to continue acting in terms of the contract to ensure grant recipients were paid. Years later, in 2017, the Constitutional Court ordered that CPS pay back the profits it made in terms of the unlawful contract. SASSA says this amounts to over R500 million. Despite the order, CPS has continued to fight against repayment. In April 2021, the Court again ordered CPS to completely open its records to an independent auditor to determine the profits it must pay back.[20]

KEYS TO YOUR DATA AND YOUR BANK ACCOUNT: THE NET1 PROPRIETARY BANKING SYSTEM

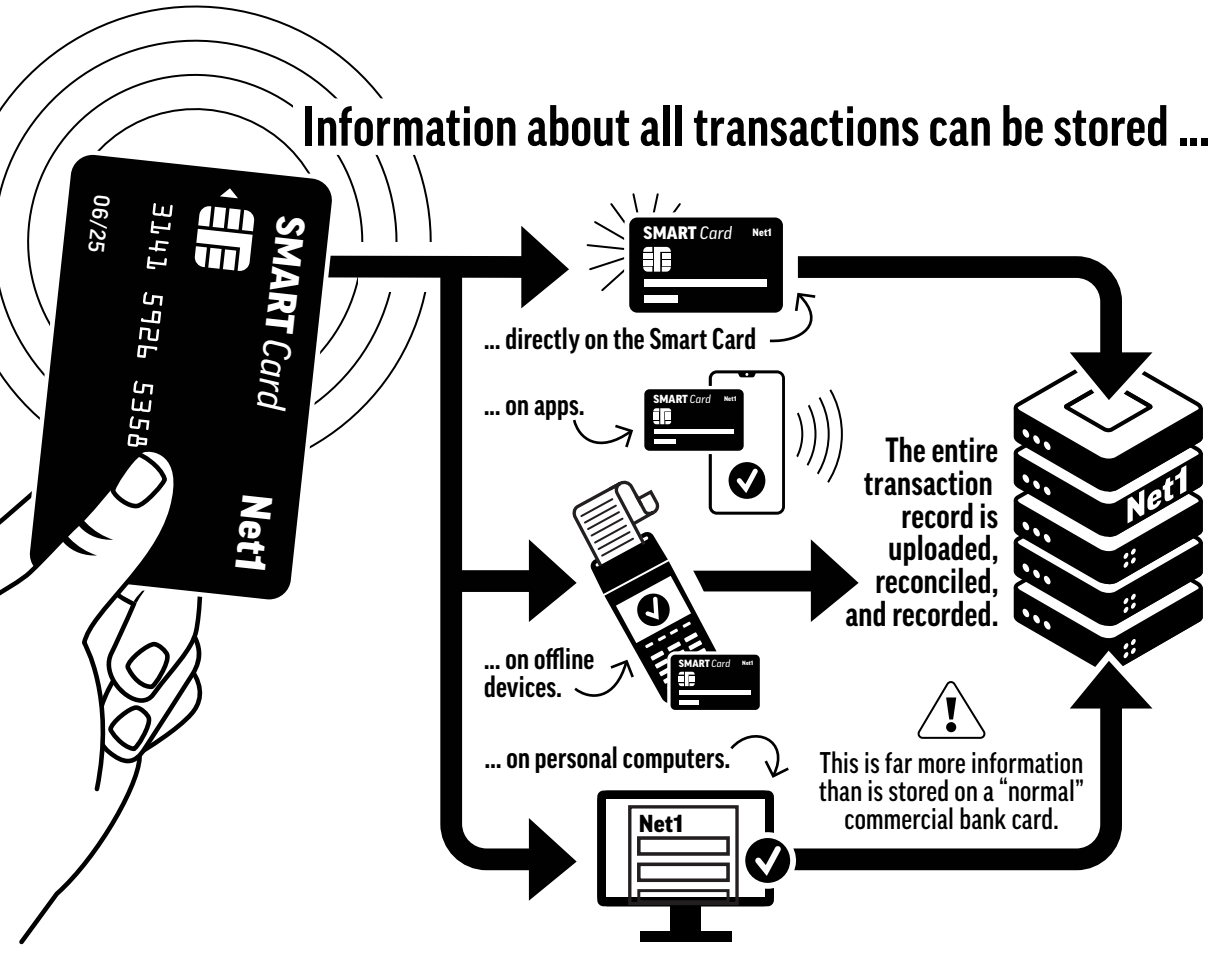
Once contracted, CPS had considerable autonomy to design and implement its grant payment system under the guidance of SASSA. Neither the National Treasury nor the Reserve Bank was consulted on the specifications for this new payment system. In 2017, Minister of Finance Pravin Gordhan stressed that the role of the National Treasury is not to intervene in the various government departments but to offer advice upon request.[21] Without such a request, the design proceeded under the authority of the Department of Social Development (DSD) and SASSA, which arguably did not have the technical capacity to oversee the development of financial infrastructure.

As a result, CPS was able to build a system for grant recipients, separate from the National Payment System (NPS), which is the South African banking standard. Governed by the Reserve Bank, the NPS is the clearinghouse for all payments and settlements between banks. Net1 created a parallel banking system, which could be linked to the NPS but was not directly part of the NPS, giving it significant control over the bank accounts of grant recipients beyond official oversight.[22]

Since CPS did not have a banking licence of its own, it needed a banking partner. It did not partner with one of South Africa's big commercial banks, but it chose instead to work with Grindrod Limited, a shipping company with a bank for high-income clients owned by Johan Rupert's Remgro group. Since Grindrod's bank had a very small clientele, Net1 had to design its information technology system to quickly roll out accounts for 10 million new customers. CPS consultants opened Grindrod bank accounts for every social grant recipient during enrolment. This happened automatically and non-competitively, without grantees being able to choose their own bank. Only later could grantees opt out and request to be paid through another bank account by filing a declaration with SASSA. Most did not know this was possible, and less than one per cent ever filed the declaration.[23] Grindrod, in partnership with Net1, held the monopoly over the banking of social grantees. Through this privileged position, Grindrod grew to become the second largest bank in South Africa by number of accounts, and its profits tripled in the first year.[24]

Though Grindrod served as the bank of choice for grantees, the more covert and intrusive actions took place through the CPS-issued grant recipient Smart Cards. The CEO of Net1, Serge Belamant, initially developed the Smart Card-based Universal Electronic Payment System (UEPS) for Nedbank in the 1990s.[25] The advantage of a Smart Card-based payment system is that it can operate offline in rural and remote areas.[26] Smart Cards are very small computers with operating software, data processing, and memory. Information about all transactions can be stored on Smart Cards and Smart Card readers offline. When a grant recipient slots their Smart Card into a card reader, both make an encrypted record of the transaction offline, which is linked with previous and future transactions (in a blockchain system). When either the Smart Card or the card reader interacts with an online environment, the entire transaction record is uploaded, reconciled, and recorded. This is far more information than is stored on a "normal" commercial bank card.[27]

Every subsidiary in the Net1 group used the same card readers. When grant recipients put their Smart Cards into these card readers and placed their thumbs on biometric scanners, their entire financial history was suddenly accessible. Their thumbprints served as digital consent to share their personal and



financial information with Net1 subsidiaries, though this was rarely explained to grantees. An insurance company like Smartlife or a microlender like Moneyline could see exactly how much money grant recipients had entering and leaving their accounts every month. This information essentially served as a very good credit check for all the Net1 subsidiaries. Moneyline could get a near complete picture of the spending habits and liabilities of their customers and make lending decisions on this basis. The corporate intimacy gave Net1's subsidiaries a sizable competitive advantage, as they did not need to ask a borrower for their bank statements, proof of address, income, or identification. All that was already contained on the Smart Card and available in the Net1 computer system.

Because of its contract with SASSA, Net1 had vehicles, staff, mobile infrastructure, and knowledge of where the millions of grant recipients lived. Since grants were only paid in the first week of the month, Net1 officials could subsequently return to the very same places to sell financial products. Thus, grantees often thought that Net1 staff and SASSA staff were the one and the same, as the very same people who paid their grants in the beginning of the month returned to sell products later in the month.[28] In urban areas, Net1 set up permanent offices, and grantees could come to them. In rural areas, Net1 officials drove around selling products from their car boots. This aggressive marketing landed many grantees in cycles of debt that depleted the value of their social entitlements. Many people could no longer afford to cover their immediate needs on a reduced grant and had to seek additional debt to cover household shortages. While borrowing money would resolve a crisis in the present, it would exacerbate longer-term crises in the future.[29]

> **"You see, with this deductions story, first they steal our money, and then we are forced to beg them for a loan".**[30]
>
> ~ Grant recipient

THE HARMFUL EFFECTS OF FINANCIAL PRODUCT SALES

CPS's sister companies, like Moneyline, did not market their loans to low-income consumers in general but to social grant recipients specifically. Investigative journalist Craig McKune, of *amaBhungane*, demonstrated how Net1's financial statements were very explicit about how it targeted grant recipients. In fact, Net1 had two microlending businesses: one that was accessible to anyone and another that was only for grantees (Moneyline). The former business was unprofitable because of the high default rate on loans, but the latter was very profitable because grant recipients were prevented from defaulting on loans. As Net1 put it, "[W]e consider [social grant-based] lending [to be] less risky than traditional microfinance loans because the grants are distributed to these lenders by us".[31]

Social grantees could not default because Net1 had monopoly control over the entire grant payment process and would deduct what was due before paying the grant. How did this work? At the time, the National Treasury would transfer a lump sum for grant payments into a DSD account held at the Reserve Bank. Then, DSD would transfer this money into nine provincial SASSA accounts, also held at the Reserve Bank. SASSA would transfer this money to nine CPS accounts at Nedbank, and then CPS would transfer it to nine accounts at the Grindrod bank. All this took place about a week before grant payments were due to recipients, earning Net1 about R12.6 million in interest per month.[32] CPS then paid this money into grantee bank accounts; but, in doing so, it could reconcile all debits on grantee accounts at the same time.[33] CPS ensured that these debits were paid early and automatically before grantees received their money. CPS has always denied that there was anything wrong with this, arguing that it was simply applying an early debit order, like most banks do. However, that does not take into account that CPS was in charge of both the payment of the grant and the deduction, and it was not at arm's length from participants in the transaction. This dispute has never been settled by a court.

Net1 thus bore none of the risk of a typical microfinance business when lending to grant recipients. Through their control over grant payments, Net1's own website confirmed that it could "apply an automatic debit against any incoming funds to the card in respect of the premium amount".[34] As soon as grantees scanned their thumbs, all debits were immediately deducted from the total sum and only the remains were distributed. Recipients were unable to choose to have these deductions occur later in the month, on a day of their choosing. There was also no protective threshold under which money could not be deducted from grantee accounts. Any of these possibilities, though empowering to the grantee, would have introduced more risk for the lender. The result was that cash transfers could be whittled away to nothing, even less than nothing, as grantee accounts could run negative balances from Net1-affiliated products.

Since the government guaranteed grants and Net1 controlled the distribution process, there was virtually no risk that these debts would go unpaid. Because Net1 could access personal data, through grantees' biometric consent, it knew when they would receive their money and when their grants might cease. It knew what day temporary disability grants would expire and when children would age out at 18. It knew if the grantee had taken other loans or had other debits coming off their accounts.

Of its "traditional" moneylending business, Net1 reported: "Despite the fact that we attempt to reduce credit risk by employing credit profiling techniques, the rate of default on loans has been high due to the high credit risk of these borrowers".[35] No such difficulty collecting payments was experienced with Moneyline. One Net1 insider revealed that Moneyline's default rate was close to zero, bragging that it was "the lowest in the entire microfinance industry".[36]

Given the vastly reduced risk of default, credit linked to social grants should not have been priced at the same rate as other "unsecured" credit. And yet, even though the risk of non-payment was nearly zero, interest rates on social grant-based credit were significant. Net1's Belamant often asserted that his products were the cheapest available: "To me, we've been able to reduce costs and without a shadow of a doubt, our loans are probably 1/3rd [*sic*] of the price of any other lender in the country, 1/3rd [*sic*] of the cost".[37] There was some truth here. Moneyline's official interest rates were zero per cent per month, but the costs of credit were hidden in service fees

of 5.33 per cent per month (on a six-month loan of R1,000). This was within the law and the limits set by the National Credit Regulator,[38] but it amounted to an effective interest rate (service fees plus interest) of 32 per cent on such a loan.

Moneyline was not the only lender benefiting from CPS's grant distribution system. All other lenders could access grantee accounts in a similar way, and many made the Net1 bank account a precondition of lending to grant recipients.[39] Net1's payment system included a perverse incentive that led to over-indebtedness for many borrowers: lenders could give grantees more loans than could be repaid each month through their grant incomes. Even though these lenders had their charges reversed in some months, the loan period could automatically be extended and eventually be paid off through the regularity of the grant. Meanwhile, for every processed payment or bounced transaction, Net1 and Grindrod took a fee from the recipient, profiting from reckless lending without screening for abuses. Net1's banking system lowered the risk for all formal (and even some informal) lenders.

WITH THE WRITING ON THE WALL: NET1 PIVOTS TO EASYPAY

By the time political sentiment turned against Net1, it had created another product exclusively geared toward grantees: the EasyPay account, also hosted by the Grindrod bank. Net1 got spooked that its profitability might be curtailed when the then Minister of Social Development, Bathabile Dlamini, attempted to amend the Social Assistance Act to stop debit orders on the CPS/Grindrod bank account. Net1 also wanted to ensure that it had continued access to grantees' bank accounts when its government contract ended. This second account, the EasyPay account, gave Net1 more control over grantee banking beyond SASSA's purview.

Net1 aggressively marketed EasyPay to grant recipients. Black Sash paralegals found that some people were told that the EasyPay card was the "new SASSA card"; others were told that credit was "not allowed on the old SASSA card"; and still others that EasyPay is the cheapest, safest bank account "for life".[40] Over two million grantees opened EasyPay accounts without filing the necessary declaration with SASSA to have their grant paid into a new bank account. Through the CPS contract, grantees could "consent" to new product offerings with their fingerprints. Upon giving "consent", they were moved out of the CPS banking environment, which had some oversight by SASSA, into a private arrangement with EasyPay.

Grantees had even greater difficulty finding recourse in the EasyPay system. With the original CPS account, beneficiaries could go to SASSA and fill out a form to dispute their deductions. After this recourse system was introduced, SASSA received about 70,000 complaints in the first three months but had to forward them to CPS for investigation. CPS settled over 60,000 claims without reimbursement and less than 10,000 people got any money back.[41] This recourse system was highly individualised, and the burden to fight for payback was placed on grant recipients themselves.

With the EasyPay account, recourse became even more difficult because grantees were not allowed to go to SASSA for assistance. They had to visit one of only 144 Net1 branches in the country or use the call centre. At the time, the call centre was not free for grantees, who reported long wait times, expensive phone calls, and consultants who could not speak their home languages.[42] If grantees requested a bank statement over the phone, they would need access to an email address, computer, and printer. This infrastructure relied on digital access, which was in many instances not accessible to grant recipients.

In sum, the Net1 and CPS plan was a relatively simple and straightforward process of profiteering by attaching financial products to welfare payments. It relied upon Net1's ability to collect and store grantee information in a proprietary format and achieve consent with the touch of a finger. It also relied upon Net1's ability to control the entire payment stream from the Reserve Bank into grantee accounts and deduct repayments automatically. Moreover, it relied on significant regulatory gaps and a lack of oversight. But if this was version 1.0 of the digitalization of welfare, what is version 2.0?

“If their services to you as end-user are free, where are they making their money? So, what are you giving them? You’re giving them information [data] ... they found innovative ways to monetise this data. And sell these packages to business ... we have to understand to use these free services there has to be monetisation somewhere in the chain”.[1]

~ Nerushka Bowan
Director and Head of Technology, Norton Rose Fulbright South Africa

3

GOVCHAT: THE DIGITALISATION OF SOCIAL WELFARE VERSION 2.0

Net1's usurious profiteering from social grant distribution was likely a precursor to future, more sophisticated forms of digital extraction: the digitalisation of welfare 2.0. What this profiteering will look like largely depends on the systems that the South African Social Security Agency introduces, and how these are monitored and regulated. The Covid-19 pandemic created renewed urgency for the digitalisation process while creating an opportunity for diminished oversight of the contracting process. After the South African government made money available to pay for a special Covid-19 Social Relief of Distress grant, SASSA had to scramble to design and implement a disbursement system in quick time.

Enter GovChat – a small private technology company that promises "technology for good".[2] GovChat offered to build a new application platform for SASSA for free, and in doing so, it has become one of SASSA's most important partners in the latter's mission to digitalise the provision of social grants. GovChat has dedicated significant resources to this digitalisation process and has already been chosen by SASSA to trial digital applications for other types of grants.

As this chapter shows, the ways in which GovChat will benefit from these contracts is still emerging. Our investigation has not uncovered unlawful conduct akin to that of Net1 and Cash Paymaster Services. Nonetheless, our investigation has revealed several red flags that we believe necessitate much closer scrutiny of GovChat's relationship with

SASSA. First, GovChat secured its contract without any competitive bidding process. Second, and perhaps most important, GovChat's claim that it is providing its services for free needs scrutiny. GovChat's financial backers are not philanthropists but shrewd fintech businesspeople, who have unambiguously stated their intention to monetise GovChat's model to secure returns for shareholders. This demands the question: what's in it for GovChat and its investors?

COVID-19 – AN ECONOMIC CRISIS AND A DIGITAL RESPONSE

On 22 April 2020, President Cyril Ramaphosa's government announced a social relief and economic support package of R500 billion, consisting of various interventions to mitigate the harms caused by the Covid-19 pandemic.[3] An important part of the package was a temporary six-month increase, totalling around R30 billion, in all existing grant payments.[4] Additionally, a special Covid-19 Social Relief of Distress grant was introduced for an initial period of six months, with R350 to be paid to individuals aged 18–59 who were unemployed and did not receive any other form of social grant or Unemployment Insurance Fund (UIF) payment. A total of R15.6 billion had gone to recipients of the Covid-19 SRD grant by July 2021.[5]

The relief provided by the Covid-19 SRD grant, though limited, took on even greater import in the context of failures of other parts of the relief package. Due to poor implementation and various barriers to access, less than half of the promised R500 billion had been spent by July 2021. This was in large part due to inadequate spending on a job creation programme and low take-up of the credit guarantee scheme.[6]

The April 2020 announcement of the Covid-19 SRD grant signalled an urgent need for safe application and distribution processes amidst the pandemic. The responsibility fell to the Department of Social Development and SASSA. On 29 April 2020, Minister of Social Development Lindiwe Zulu announced that because the SRD grant targeted individuals who were not on existing SASSA or other government grant databases, a new system was required.

While the subsequent transition to electronic application processes was partly aimed at addressing Covid-19 safety regulations, the pandemic was not the trigger for the change from paper and in-person processes. The transition followed an existing trend toward digitalisation of service delivery infrastructure across all sectors, albeit with varied degrees of success, by the South African government. This meant that filling in paper applications, standing in lines, or having to provide physical copies of documents would no longer be necessary to access government services. Instead, required information would be provided and processed primarily online and in digital formats.[7]

However, designing and managing such digital processes comes at a cost. Digitalisation requires the creation and maintenance of physical infrastructure like that for electricity and efficient Internet access. It also requires substantial legal and policy processes to protect people's privacy and ensure that government officials have the necessary mandates. Further costs include those related to human resource capacity to build the technologies and then to maintain the digital infrastructure over the long term. Many state-led e-government initiatives have not met their goals due to government institutions lacking sufficient resources, both in terms of time and in terms of money, to facilitate digitalisation processes.[8]

In fact, those with the capacity to execute such projects have mostly been in the private sector, and they have benefited from state contracts. The Presidential Commission on the Fourth Industrial Revolution has indicated the government's desire to leverage expertise and private investment towards building the infrastructure that can support digitalisation for South Africa's Fourth Industrial Revolution.[9] This reliance on the private sector has serious consequences because it usually entails a shift in how money is spent and managed. Digitalisation tends to move away from capacitating the government itself to provide services and towards outsourcing state services to a single or small number of technology companies.

The state's reliance on the private sector was evident in SASSA's approach to set up a digital application process for the Covid-19 SRD grant. By 29 April 2020, a trial system was set up for the grant application process to assess the best way of facilitating online

applications. Applicants could either send a WhatsApp message to GovChat on 0600 123 456 and select SASSA or send an e-mail to SRD@sassa.gov.za.[10] The 0600 WhatsApp number was the same as the number used for the Department of Health WhatsApp line. It was only used during the trial run and was later changed to a dedicated number for the grant applications.[11]

On 11 May 2020, at the launch of the WhatsApp line for Covid-19 SRD grant applications, Minister Zulu thanked private and civil society partners in a speech, which also made special mention of the role of GovChat.[12] It was announced that applications for the SRD grant could be made via various digital platforms: a website run by Prosense, a USSD platform run by Vodacom, and the WhatsApp platform run by GovChat.[13] Twelve million people – 20 per cent of South Africans – applied for the grant in the first few months, and of them, seven million successfully qualified for it. Eighty per cent of the grant applications were made through the USSD platform, and yet GovChat's WhatsApp platform garnered most of the media attention, seemingly finding favour with SASSA and DSD officials.[14] As we discuss below, this focus on GovChat can be explained in part by the tendency of SASSA officials, as well as Minister Zulu, to focus on GovChat at public events. However, it also reflects an apparent media bias towards new technology platforms without asking critical questions.

However, another reason for the re-registration process was to force all applicants to submit to external verification of their income. All applicants were once again vetted against SASSA's legacy database (SOCPEN), the Personnel and Salary System (PERSAL), the Unemployment Insurance Fund, and the National Student Financial Aid Scheme (NSFAS) to ensure that they were not already receiving an income. This was a punitive process leading to a high rate of rejections, including errors that saw many people who did in fact meet the qualifying criteria get rejected. We return to this issue in the next chapter.

The Covid-19 SRD grant had a limited 12-month lifespan and was ended in April 2021. However, in July 2021, under significant pressure from civil society and in the midst of a third wave of the Covid-19 pandemic, President Ramaphosa announced the reinstatement of the SRD grant. In August, new applications started to be accepted. All the application platforms had to be upgraded for this reinstatement, and all grantees had to re-register. One of the primary reasons for this re-registration was to gather people's bank account details during the application process. Given that the South African Post Office had struggled to pay recipients quickly and efficiently in 2020, SASSA set out to ensure prompt payment directly into bank accounts and thereby decrease its reliance on the services of the Post Office.

The initial re-application rush crashed SASSA's website in August 2021. In an interview with *MoneyWeb*, SASSA's spokesperson told applicants to use the GovChat service instead, steering them towards the service while failing to mention the USSD platform at all.[15] At the time, SASSA was still negotiating with Vodacom for the latter to redesign the USSD platform to ask for banking details in the initial application process, delaying the platform's readiness for the surge in new applications. This delay was particularly worrying as the USSD platform was the cheapest and most accessible service in the first round of the Covid-19 SRD grant.

GOVCHAT'S GENEROUS OFFER

A point to which both SASSA and GovChat often return is that GovChat offered its services to SASSA for free in a time of need. As mentioned earlier, this seemingly generous offer has placed GovChat in an ideal position to benefit from future contracts linked to the distribution of social assistance. However, it is apparent that GovChat has been granted a significant advantage without the normal legal requirement of a competitive procurement process, and the public scrutiny that such a process provides.

In September 2020, Open Secrets submitted a Promotion of Access to Information Act (PAIA) request to SASSA for information about how the contract came about, the details of the contract, and minutes of meetings between GovChat and SASSA. SASSA, with the agreement of GovChat as the third party, released all the requested records in November 2020.

The documents reveal that instead of following a formal procurement process, SASSA's Chief Information Officer, Abraham Mahlangu, phoned GovChat's CEO, Eldrid Jordaan, on 4 May 2020, to ask if GovChat could assist them in the roll-out of the Covid-19 SRD grant.[16] Jordaan enthusiastically agreed and confirmed in a letter that same day that GovChat would provide the WhatsApp service to SASSA at no cost.[17] Two days later, on 6 May, SASSA CEO Busisiwe Memela approved the agreement.[18] Five days later, on 11 May, the WhatsApp application service was launched. The developers, Synthesis Software Technologies, took but two days to create the entire platform. The consequences of this haste were revealed when the platform crashed during a live demonstration for Minister Zulu on 14 May.[19]

SASSA chose to turn to GovChat because its own capacity to facilitate the increasing numbers of applications for the Covid-19 SRD grant was limited.[20] What seemed to have swayed officials is that GovChat had previously created a successful online application process for a pilot project setting up the Department of Health's Covid-19 WhatsApp line. Given that SASSA sought a similar solution for the Covid-19 SRD grant, GovChat was well placed to provide the service.[21] GovChat's role was to facilitate the onboarding of the SRD application process onto the WhatsApp platform.[22]

Fast and furious:
GovChat swoops in and bags SASSA contract.

4 May 2020
SASSA's Chief Information Officer, Abraham Mahlangu, asks GovChat's CEO, Eldrid Jordaan, if GovChat could assist them in the roll-out of the Covid-19 SRD grant.

4 May 2020
Jordaan agrees and confirms in a letter that same day that GovChat would provide the WhatsApp service to SASSA at no cost.

6 May 2020
SASSA CEO Busisiwe Memela approves the agreement.

11 May 2020
The WhatsApp application service is launched.

14 May 2020
The platform crashes during a live demonstration for Minister Lindiwe Zulu.

However, GovChat was not the first technology company to be involved in meeting SASSA's need to onboard beneficiaries onto the WhatsApp platform. For the trial of the WhatsApp application process, SASSA used another South African technology firm, Praekelt,[23] a company owned by Gustav Praekelt[24] and one of only four official WhatsApp business service providers (BSPs) in South Africa.[25] WhatsApp defines a BSP as an approved third party that assists businesses and other clients to communicate with people on WhatsApp, including by reading, storing, and responding to messages on behalf of the business.[26] According to GovChat's Jordaan, SASSA and Praekelt's partnership fell through just before the trial was finalised.[27] In a SASSA memo, Mahlangu indicated that they also considered securing SASSA's own WhatsApp line directly through Google and Facebook, but they assumed it would require a long approval process.[28] With Praekelt and an in-house SASSA WhatsApp line no longer viable options, Mahlangu proceeded to call Jordaan, and GovChat agreed to facilitate the service seven days before the Covid-19 SRD grant application would go public.[29]

It remains to be seen whether future contracts between SASSA and GovChat will come with a price tag or if GovChat will continue to provide its services free of charge. Regardless, this initial relationship has placed GovChat in a prime position to benefit from SASSA's future digitalisation drive. GovChat's affiliations with private financial firms and increasing number of contracts with state entities mean that its platform is widening its reach as an intermediary between these groups. The way it facilitates technological and commercial interactions between these stakeholders is deepening the uncertainty as well. Perhaps this was always the intention? To overcome this opaqueness and understand how GovChat can provide its services to SASSA at no cost, or how the true costs are hidden, we must begin by (re-) viewing the initial business model GovChat envisioned and the investors who sought to finance it.

GOVCHAT'S INITIAL VISION

GovChat is best known for the platform technology it produces, which shares the company's name. GovChat – the platform – is the "official South African citizen government engagement platform" that facilitates citizen engagement with local government structures. The platform was co-created by GovChat and the Department of Cooperative Governance and Traditional Affairs (COGTA), the department in charge of managing service delivery and local governance structures.[30] People can use the platform to get the contact details of their ward councillor, submit a complaint about service disruption and potholes, and rate their experience of government services at places like police stations. This partnership with COGTA increased the GovChat platform's status and visibility, positioning it centrally within South Africa's digitalisation processes.

Since the Covid-19 pandemic began, GovChat has announced remarkable growth in users on its platform, reaching over 7 million active users by August 2020, who have sent hundreds of millions of messages.[31] In addition to partnerships with COGTA and SASSA, GovChat also announced a partnership with the Department of Health and BCX/Telkom to launch a digital platform for information on COVID testing and symptom tracking.[32] GovChat further partnered with ABSA Group and the Department of Social Development in a hygiene education and public awareness campaign.[33]

Jordaan began developing the idea for communication technology to connect users with local government representatives between January 2013 and December 2015.[34] During this time, he worked concurrently as an advisory Board member of technology firm Mxit and as a special advisor to the then Minister of Public Enterprises, Lynne Brown (who has been implicated by numerous witnesses at the Zondo Commission in conduct alleged to have enabled state capture at the time).

Shortly after his stint with Brown, Jordaan founded GovChat, the company that would go on to create the eponymous GovChat platform.[35] Jordaan has said that as a result of his experience working for Brown, "state-owned enterprises is what I really know";[36] and that his dual experience at Mxit and in the state nurtured the idea of a platform to link citizens with government.[37]

Jordaan's political connections in South Africa and the rest of the continent appear to be significant, giving him access to senior decision-makers. He has often appeared at events alongside senior government officials,

including Minister of Public Service and Administration Ayanda Dlodlo at the Open Government Partnership Summit in Tbilisi, Georgia, in July 2018.[38] At that summit, Jordaan's speaker profile indicated that he was at the time serving as "digital communications advisor to various African [g]overnments" – though the governments were not specified.[39] Two months earlier, in May 2018, Jordaan and representatives of the South African government travelled to the African Union's Transform Africa Summit in Kigali, Rwanda, to speak about the GovChat platform and "unveil GovChat Africa to governments across all member states".[40]

GOVCHAT EXPANDS ACROSS THE AFRICAN CONTINENT

In 2019, GovChat expressed keen interest and plans to expand beyond South Africa into other African countries, including the Democratic Republic of the Congo (DRC), Gambia, Ghana, Nigeria, and Zimbabwe, and beyond Africa into some parts of Southeast Asia.[41] To date, GovChat has already launched GovChat Ghana.[42] This deal was struck at the Tbilisi summit, to which GovChat CEO Eldrid Jordaan travelled with Minister Ayanda Dlodlo. In September 2020, Jordaan confirmed that in addition to Ghana, GovChat had signed agreements with the governments of the DRC, Nigeria, and Zimbabwe. He added that extending into other African markets was GovChat's next big priority.[43]

Speaking with Open Secrets investigators, 42-year-old Jordaan said that the goal of GovChat could be summed up by the idea that "GovChat enables democracy between the ballot boxes".[44] Jordaan is clearly passionate about the potential of the GovChat **platform** to simultaneously allow local government to be held accountable and to improve service delivery.[45] Importantly, GovChat is not a standalone application but a platform that can be accessed through numerous existing platforms, such as USSD, Facebook, Telegram, and WhatsApp – making it easily accessible to many South Africans through tools they already use.

KEY TERM

PLATFORMS

A platform is a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet and digital technology systems. It can be best understood as an intermediary between users that extracts value from their activities on the basis of the data generated. Facebook and Google are quintessential examples of platforms.

According to the GovChat website, for three years, Jordaan self-funded a prototype of the GovChat project and an awareness campaign directed towards the South African government.[46] However, in March 2017, Jordaan realised that he needed a skilled technology partner to make the platform a reality, and he was looking to sell. He approached several technology companies with a request for tender that laid out a plan to set up a holding company in Mauritius to take up a 74 per cent stake in GovChat. As reported in the *Mail & Guardian*, the intention was for the holding company to be sold to a multinational partner "with existing technology readily available".[47] According to media reports, the likely buyer would be a foreign company, but Jordaan claimed that several South African technology companies had already expressed their intention to bid.[48]

Though this planned sale did not come to fruition in 2017, the tender process and documents provide some insight into the ways GovChat envisioned making its services profitable and the importance of its data collection capacity to its envisaged profitability. While the tender documents indicated that the company could not guarantee "commercial value",[49] they suggested that revenue could be drawn from "the commercial value of relevant data analytics".[50]

The tender documents further reveal a brazen commitment to violations of people's privacy in the interests of securitization. In the request for tender, Jordaan indicated that the data GovChat gathered was expected to be used for image recognition, citizen engagement, data mining, and identification of protest patterns, which could be used by South Africa's state security apparatus.[51]

Jordaan confirmed that the platform would automatically store the geolocation data from all users during their sessions.[52]

Jordaan was not able to continue the project without significant external investment that would develop the technical capacity of GovChat and allow him to draw an income. By early 2018, a little over two years after the company was formally registered, and less than a year after the request for tender, he had run out of money and was in financial distress.[53] This put GovChat's agreement with the South African government to become the official citizen engagement platform, signed already in January 2018, at risk.[54]

CAPITAL APPRECIATION – AN ANGEL INVESTOR TO THE RESCUE

Despite the apparent funding shortfall, GovChat soon received financial lifelines in the form of investments from private actors in the financial services and fintech sectors. The first funding came from an "angel investor" – who Jordaan says he did not know at all – that found him on LinkedIn and provided the necessary funds to "finish the project".[55] The mystery investor was Dewald Dempers.[56] In a video address published in January 2020 at the launch of GovChat's new headquarters next to Parliament in Cape Town,[57] Jordaan said that Dempers had been "watching [him] on social media" and approached him with an offer of R10 million to "turn [his] concept into something tangible".[58] Dempers' investment was crucial in the rejuvenation of GovChat in late 2018.

Dempers worked as a senior executive in the financial services and healthcare sectors, and also worked closely with subsequent GovChat investors. From 2012 to 2015,[59] he served as the CEO of AfroCentric Investment Corporation Limited, an "investment holding company providing services and products to the healthcare sector".[60] Michael "Motty" Sacks (more on him later) was a co-founder of AfroCentric and a non-executive director while Dempers was CEO.[61] Until 2018, Dempers was also a director at African Rainbow Capital (ARC) Health, an investment company created to "reform and restructure SA's [South Africa's] private healthcare sector" by ARC, a financial services company chaired by one of South Africa's richest people, billionaire Patrice Motsepe.[62] ARC was also an early anchor shareholder of Capital Appreciation, a JSE-listed fintech group, and invested R50 million in the private placement of shares when CAPPREC listed in 2015.[63]

Given these corporate intimacies, CAPPREC was the next party to invest in GovChat. In May 2019, GovChat signed an agreement with CAPPREC for R20 million in funding from CAPPREC's Enterprise Development Fund in return for 35 per cent of GovChat.[64] CAPPREC is a holding company that owns three firms – Dashpay, African Resonance, and Synthesis Software Technologies.[65] All three focus on selling technological solutions to financial and banking clients:

The CAPPREC Stable

All of CAPPREC's subsidiaries sell technological solutions to financial and banking clients.

1. **Synthesis** provides technology for the financial services sector. It created GovChat's technology platform for R6 million following CAPPREC's investment. [66]

2. **African Resonance** primarily provides payment technology to blue-chip companies and counts the big four South African banks among its clients.[67]

3. **Dashpay** also provides payment technology but targets smaller merchants and small, medium, and micro enterprises.[68]

Having acquired the companies in May 2017, CAPPREC moved to the software and computer services sector on the JSE a month later.

Once GovChat and CAPPREC reached an agreement, Motty Sacks, the non-executive chairman of the CAPPREC Board, was also appointed as chairman of GovChat's Board.[69] Sacks further became a registered director of GovChat in 2019.[70] Tandi Haslam – GovChat's former chief financial officer – managed the process of raising capital from CAPPREC and was then also appointed as an executive director of GovChat.[71]

CAPPREC'S BOARD OF HEAVY HITTERS

Capital Appreciation is a JSE-listed fintech group. In its interim financial statements at the end of 2019, CAPPREC announced a R20 million investment in GovChat. It tellingly gave a nod to the markets that this investment had the prospect of being profitable: "The relationship with GovChat presents a number of potential commercial opportunities which are consistent with the strategic objectives of Capital Appreciation". Here are the individual executives and board members at CAPPREC that will direct how the company pursues these "commercial opportunities":

EXECUTIVE LEADERSHIP

Michael Pimstein is the joint Chief Executive Officer of CAPPREC. He is the former CEO of steel giant **Macsteel**, a position he held from 1999 to 2013.

Bradley Sacks is the joint CEO of CAPPREC. The son of Michael Sacks, he began his career as a lawyer at a corporate law firm based in New York and was later a Managing Director at the **Bank of America**. He is also a partner at Centric Capital Ventures LLC, a private investment firm based in New York.

Alan Solomon is the Chief Financial Officer of CAPPREC. He served as the CEO of **Bidvest Bank**, a subsidiary of the Bidvest Group Ltd, for eight years.

CAPITAL APPRECIATION

BOARD OF DIRECTORS

Bukelwa Bulo has served on the board of CAPPREC since September 2015. She also serves on the Boards of other listed companies, including **Netcare Ltd**, Sephaku Holdings Ltd, and Value Group Ltd.

Jacob Meyer Kahn was a co-founder, along with Michael Sacks, of **Afrocentric Investment Corporation Limited**, where he served as a director for many years.

Charles Valkin is a long time senior lawyer at corporate law firm **Bowmans**, previously known as Bowmans Gilfillan.

Michael "Motty" Sacks co-founded Network Healthcare Holdings (**Netcare**), and was founder and chairman of **Aplitec** (which later became Net1) at the time it bought Cash Paymaster Services in 1999. Sacks has served on numerous other company boards, including as independent non-executive director of **Adcock Ingram Holdings** and as non-executive director of ADvTECH.

Roshan Morar has held several high-profile positions, including as non-executive chairman of South African National Roads Agency SOC Ltd, Board director of the **Ithala Development Finance Corporation**, and the independent non-executive deputy chairman of the **Public Investment Corporation**. Morar is also a director at the **Takatso** consortium that was recently awarded a 51% stake in embattled South African Airways.

Errol Kruger was previously the Registrar of Banks at the **South African Reserve Bank**, where he worked from 1978 to 2011. From 2009 to 2011, he represented South Africa as a full member of the Basel Committee on Banking Supervision. He currently serves as an independent non-executive on **Nedbank**'s Board.

Victor M. Sekese is the CEO and partner at prominent audit firm **SizweNtsalubaGobodo Grant Thornton**. He also serves on the Boards of Blue Chip Investments (Pty) Ltd, Firefly Investments 87 (Pty) Ltd and Sizwentsaluba VSP Services (Pty) Ltd.

Michael Shapiro serves as an executive director on the CAPPREC Board. He is also the Managing Director of **Synthesis Software Technologies**, a CAPPREC subsidiary, working there since 2003.

Kuseni Dlamini is the former head of **Anglo-American South Africa**, a member of the executive committee of Anglo America plc in London, and a director of Anglo Platinum. He is also the non-executive chairman of **Aspen PharmaCare** Holdings Ltd and **Massmart** Holdings Ltd.

Rorisang "Roxy" Maqache is a graduate of the Gordon Institute of Business Science and is the CEO of Consulting Group, **Desert Arabia**.

CAPPREC secured a hugely favourable deal when investing in GovChat – a nominal R1 investment bought a 35 per cent equity stake in GovChat. In return, CAPPREC extended a R20 million line of credit to assist GovChat's development. It appears that R1.5 million of this was paid as a no-interest "enterprise development loan", which is repayable by GovChat on demand.[72] It is not clear from CAPPREC's annual report whether the entire line of credit is on these terms.

So what do these corporate arrangements tell us? Millions of rands were invested in GovChat to secure its success. As with any investment, there is the expectation of generating profit. Yet, with GovChat providing its digital services to SASSA and other state entities nominally free of charge, how exactly will the company ensure that its investors, who saved it from financial ruin, remain content?

MONETISING DATA: NET1 AND CPS IN A DIFFERENT GUISE?

The answer is data. Data. Data. GovChat CEO Jordaan is adamant that while he understands the inherent risks of having access to people's personal data, GovChat will never engage in unethical profiteering from that personal data.[73] However, while he argues that monetisation is not his immediate priority,[74] CAPPREC is promising its shareholders that it will monetise the GovChat business in the future. The question is as to how GovChat's monetisation plan differs from Net1's earlier attempts to profit from the data of social welfare recipients. The promise that GovChat will not do so unethically, based on the nobly worded intentions of its founder, may provide comfort. However, given the cut-throat corporate environment in South Africa, is this enough to warrant public trust?

Tellingly, when Minister Zulu announced the Covid-19 SRD grant would go live on 11 May 2020, CAPPREC's share price went up nearly 8 per cent. Hours later, CAPPREC announced that "shareholders would be pleased to learn that the company's affiliate – GovChat – had announced a partnership with SASSA to support the digitalisation of the Covid19 [sic] social relief programme".[75] At the time, financial commentator Khaya Sithole pointed out that not only was this the first significant jump in CAPPREC's share price since it listed but also that there were individuals on CAPRREC's Board who had a history with scandal-ridden Net1.[76] These were former Net1 executives Motty Sacks and Hanoch Neishlos. A company having Board members associated with the Net1 debacle should have set the alarm bells ringing for most reasonable people – particularly for the SASSA officials who appointed GovChat and knew the full background of Net1's past profiteering from social grants.

Sacks was the founder and chairman of Aplitec (which later became Net1) at the time it bought CPS in 1999.[77] Neishlos served on the CAPPREC Board alongside Sacks and was a significant shareholder until 2019 when he was bought out.[78] A fellow founder of Net1 alongside Sacks, Neishlos left his position as head of computer science at the University of the Witwatersrand (Wits) after allegations of conflicts of interest linked to a project between Wits, First National Bank, and Aplitec aimed at designing a smart card for money transfers.[79] The allegations maintained that Neishlos owned R100 million in Net1 shares and was a director at the company while working at Wits, and that Net1 intended to benefit from the operating system that the project would produce.[80]

These links caused concern over GovChat's subsequent partnership with SASSA with regard to Covid-19 SRD grant distribution in May 2020.[81] However, GovChat and SASSA quickly dismissed concerns over the historic connections to Net1 and CPS arguing that Sacks and Neishlos had left Net1 (in the early 2000s), long before the Net1 and SASSA contract scandal and long before the GovChat deal took place.[82] At the time, Jordaan told journalists that neither Sacks nor Neishlos had anything to do with GovChat landing the SASSA deal and reiterated that GovChat was running on a not-for-profit basis.[83]

There is no proof that the GovChat contract with SASSA was intended to clandestinely usher Net1 back to the social grants table.

> **Yet, as Sithole pointed out, "[F]or a company that has [people linked to] CPS and Net1, for them to enter into another transaction, with the same type of entity, it's just ridiculously clumsy".[84]**

GOVCHAT AND CAPPREC TELL DIFFERENT STORIES

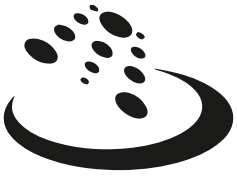
Even if the corporate players are different this time around, the pertinent question remains as to whether and how the new players will profit from access to the data of social grant recipients. The public statements of GovChat CEO Jordaan and CAPPREC are inconsistent on this question. Jordaan has always publicly stressed that the services to government are offered pro bono. He presented CAPPREC's investment in GovChat as "grant funding" and also described GovChat's investors as being "interested in government accountability".[85] In interviews with the media, he reiterated,

> **[T]he return-on-investment [ROI] question is an important one, but our ROI is measured more around social impact. If you're asking how... we pay our bills, we provide anonymised data to research and academic institutions so that they can better understand public sector challenges and successes.[86]**

In another public interview, in late 2020, Jordaan confirmed that GovChat also sells data to the government. While he said that it provided some data to the government for free, to "see what is going on" at a local government level, he also mentioned two subscription packages: a premium package and a silver package. These packages promise to provide access to comparable data across municipalities as well as predictive datasets and data analytics.[87] Jordaan said that it was through these subscriptions that GovChat intended to pay its bills in the future.[88]

Curiously, Jordaan presented himself as a non-profit worker of sorts when interviewed by Open Secrets investigators in June 2021, stating that at present he "does not have a business model for GovChat" and claiming that having one is not his priority. Rather, his focus is on getting the GovChat platform working properly, and thus, he is grateful towards the private sector for aiding him in this endeavour.[89] He added that GovChat, at the time of the interview, had not received any money from the government for its digitalisation services, while reiterating that his priority is not monetisation.[90]

However, Jordaan did concede that the data collected by GovChat is indeed very valuable.[91] In an apparent nod to the Net1 scandal, he suggested that it could be used to sell financial products to "vulnerable people" but that he "wouldn't allow this to happen".[92] Jordaan claimed that all data gained through the SASSA contract would be owned by the government and that payment systems, such as that provided by CAPPREC subsidiary African Resonance, would not benefit from the



THE AUDITOR-GENERAL RAISES RED FLAGS TO SASSA ON DATA SECURITY

In November 2020, the office of the Auditor-General of South Africa (AGSA) released its second special report on the financial management of the government's Covid-19 initiatives. With regard to the distribution of the Covid-19 SRD grant, AGSA alerted SASSA that it was concerned about the access of developers from one service provider – presumably GovChat - to the Covid-19 SRD grant database and the online system's production environment. The report noted: "We found that developers had been granted excessive access on the SRD system that allowed them to perform operational functions and payment job scheduling. They also had unrestricted access to the SRD database, which may result in unauthorised changes to the system or unauthorised access to the system data".

While acknowledging that access was required to fulfil certain functions related to the system, the Auditor-General was concerned that "this access was not monitored, which could result in unauthorised activities not being detected timeously. This access also allows audit trails to be deleted, eliminating any trace of activities carried out." The AGSA report called on SASSA to implement more proactive measures to "monitor developer access to the SRD environment, irrespective of the type of access granted".

work in any way.[93] Despite the assurance, the fact that GovChat will sell packages of analysed data implies its access to the data and ownership of at least the data analysis.

Jordaan's assurances that monetisation is not his priority show a disconnect from CAPPREC's stated intent of deriving profit from fintech solutions aimed at benefiting big banks and financial institutions. When announcing its 2019 financial results, CAPPREC touted "platform economics" as a new economic model that promised "brutal efficiency" because it creates an "opportunity to integrate multiple disparate products on a single platform".[94]As discussed earlier, GovChat is a platform that can accommodate numerous products or services and integrate itself onto various applications. GovChat's partnership with SASSA brings millions of people onto this platform rapidly and makes significant data on each of them available to GovChat. Does CAPPREC see GovChat as a means to access data that can benefit the financial institutions that count among its clients?

Public statements by both CAPPREC and GovChat further suggest that Jordaan's assurances reveal only part of the truth. In its interim financial statements at the end of 2019, CAPPREC announced a R20 million investment in GovChat. It tellingly gave a nod to the markets that this investment had the prospect of being profitable: "The relationship with GovChat presents a number of potential commercial opportunities which are consistent with the strategic objectives of Capital Appreciation".[95] Given GovChat's access to the personal data of millions of citizens, and its increasingly embedded relationship with many government departments, it is very concerning but not at all surprising that CAPPREC sees this investment as promising commercial opportunity.

CAPPREC's 2020 integrated annual report also gives insight into how the company envisions its investment in GovChat developing. Labelled as a "transformation initiative", it is discussed at length in the chairman's letter and review by the joint chief executives.[96] Together, they talk up the fact that CAPPREC and Synthesis contributed their expertise to assist government in meeting the needs of the Covid-19 crisis, through GovChat. They also stress that their investment in GovChat as a black-owned technology firm is part of their transformation initiative to contribute to the Broad-Based Black Economic Empowerment (B-BBEE) programme.[97]

But the devil is in the detail. In a section focused on the risks and opportunities facing CAPPREC investors, GovChat is listed as one of two identified opportunities. Specifically, "to monetise GovChat – the Group [CAPPREC] has identified a variety of potential revenue opportunities, both locally and abroad, all of which will be explored".[98] However, CAPPREC executives have remained coy about how precisely they intend on making money from GovChat. While expressing excitement about the contract with SASSA, Bradley Sacks, CEO of CAPPREC and son of Michael Sacks, said:

> **"The strategy for GovChat to make money for the company is 'evolving'. You can see by the user data that the GovChat platform is generating and the nature of the reports that it is able to deliver to government and whole municipalities to make them accountable for their quality of service. Here is a tremendous opportunity to be able to derive value and deliver value".**[99]

Other GovChat directors have likewise touted this monetization potential. For example, Haslam (GovChat's former chief financial officer) made it clear that in 2019, GovChat envisioned growing commercial relationships with its partners. On the announcement of the R20 million funding from CAPPREC, she said:

> **"Our first focus is increasing our capacity in South Africa, increasing the user and subscriber base and marketing, and rolling out new lines for engagement and inquiry, including new and innovative applications. We continue to receive expressions of interest in our model and operating platform and look forward to welcoming commercial relationships with product and services partners in the foreseeable future".**[100]

Given Haslam's references to monetisation and "product and services partners", it seems highly unlikely that the commercial opportunities envisioned by both GovChat and CAPPREC remain limited to providing anonymized data to academic institutions or comparative data analysis to government departments.

THE LONG (DATA) PLAY: GOVCHAT AND SASSA IN THE FUTURE

While CAPPREC's strategy to monetise GovChat's business might be "evolving", GovChat is perfectly placed to obtain data on a significant number of people in South Africa. The initial source of the data lies in GovChat's control of the Covid-19 SRD grant application process. Any company holding such data can build progressively more detailed profiles of individuals. Its next source of data could lie in future digitalisation projects at SASSA, as it is already well positioned to win future contracts. A final source of data could be established through GovChat partnering with other government departments; for example, health data collected on individuals could be linked with financial data on them.

Our insights into how data is collected and analysed come from GovChat CEO Jordaan's public interviews as well as his interviews with Open Secrets. Together, they reveal that GovChat is automatically collecting a large amount of personal data from grant applicants, and that it can and does access state databases to verify much of this data. In *The Synthesis Podcast* – run by Synthesis Software Technologies – Jordaan explains that GovChat uses chatbot technology to simplify the grant's qualifying questions. A chatbot is a programme powered by artificial intelligence to mimic a human conversation and is often used in messaging platforms to engage a human user.[101]

Speaking with Open Secrets, Jordaan further explained that GovChat collects information via the WhatsApp platform to assess whether the applicant is eligible for the Covid-19 SRD grant.[102] Since WhatsApp does not allow for the collection of a personal identity marker like the South African ID number, applicants are diverted to a secure web portal on GovChat's site, where GovChat collects the ID numbers. Though the data costs on WhatsApp are low, shifting to this secure web portal incurs additional costs for applicants and often leaves them unable

Below: Elderly people waiting in line for their SASSA payouts at Makhaza Mall in Khayelitsha during lockdown level 4 on 4 May, 2020.

Above: Grant beneficiaries protest outside the SASSA office on 30 April, 2021 in Bellville. It was reported that some people were queuing since the previous day, hoping to receive their R350 grant before it ended. Applications opened again in August 2021 .

to complete their application process.[103] GovChat then verifies the ID numbers against the Department of Home Affairs' database.

After an application is made through GovChat, SASSA cross-checks the applicant's eligibility by running their information through other databases such as SOCPEN, PERSAL, UIF, and NSFAS.[104] According to Jordaan, GovChat has the capacity to facilitate this cross-checking too, but currently, it is solely SASSA's responsibility. If GovChat were to begin pulling data from the other databases (i.e. SOCPEN, etc.), it could combine that data with that which it already holds and build more complete financial profiles of individual applicants. Such profiles would be appealing to financial firms who seek ever more detailed profiles of individuals to better target their products.[105]

GovChat is also already running trials for the digitalisation of application processes for other grants. SASSA has a clear commitment to digitalising social welfare in South Africa, and GovChat is now well placed to profit from this process. Published in 2019, SASSA's 2020–2025 strategic plan emphasises a shift towards a digital model. This includes rapidly moving towards fully automated grant application processes, automated identity verification, and development of a data strategy that will allow for "unlocking" of the data's "potential".[106] The plan is silent on what this means but says that it will ensure that online grant application processes will be accessible, efficient, and secure.[107] To that end, from 14 to 25 September 2020, SASSA conducted a "trial run" of an online application process for the Child Support Grant, Foster Child Grant, and Old Persons Grant.[108] The application could be made by accessing the SASSA website using a laptop or mobile phone,[109] and it required an email address to login. Applicants could submit certified documents in support of their application, check the status of that application, and update information, such as their address or banking details.[110] It is not clear whether SASSA used any external service providers to assist in the creation of the online portal, but GovChat has been involved in other similar trial systems.

An example showing GovChat's growing presence within grant delivery systems is the 28 April 2021 SASSA announcement of its role in creating the online platform for the disability grant. The online booking system for applications for the disability grant was launched at a media event at GovChat's office in Cape Town.[111] GovChat's system integrates with SASSA's current Electronic Medical Assessment Statistics Template system, allowing grantees to make medical appointments.[112]

The multimillion-rand question is this: will a company like GovChat have access to the data of millions of basic income grant recipients? In other words, is this the bonanza that GovChat and its investors are betting on? By offering its initial services for free, GovChat may have sidestepped the need for going through formal procurement processes in the future, or at least made itself a preferred partner to work with. Furthermore, the more departments GovChat works with, the greater it metastasizes through state organs and the more data and power it collects, anticipating a time when it holds a monopoly role in managing the data provided to state entities.

Jordaan has strongly hinted at the opportunities provided by GovChat's digitalisation drive. Speaking in September 2020, Jordaan was hopeful of future work with SASSA, telling the press, "There are a number of opportunities, including, but not limited to, supporting new grant applications, verifying identity, status updates and cross-validating across multiple data-points. There are a lot of opportunities; we're here to assist SASSA where needed".[113] Speaking to Open Secrets in October 2021, Jordaan said that each SASSA grant would require a unique application process, adding that GovChat had set up teams to think through "how to get every grant digitised".[114]

THE BIG QUESTION

It is not just GovChat's role in the digitalisation of existing grants that provides it with opportunities. The economic and social devastation caused by the Covid-19 pandemic, soaring unemployment, and increased hunger have rejuvenated calls for a basic income support grant. The Black Sash has initiated a campaign calling on the government to implement basic income support of R1,268[115] for all people aged 18–59 who receive little or no income.[116] While far from being a panacea for the challenges facing South Africa, basic income support appears vital to fulfilling the right to social assistance contained in section 27 of the Constitution, as well as being indispensable for ensuring the dignity of those living in poverty.

If the government were to indeed implement basic income support, SASSA's digitisation programme would dovetail with bringing millions of new people into its systems and dramatically increase the amount of money being distributed. Importantly, it would also see the data of millions of people collected in the process – and therein lies great opportunity for private sector corporations seeking to profiteer.

govchat
VS
facebook

GOVCHAT VS. WHATSAPP AND FACEBOOK: A COMPETITION DISPUTE

A recent, significant legal dispute between GovChat and WhatsApp provides further evidence that the profit motive is driving GovChat's work with SASSA and other government departments. This dispute exposes the lucrative profits that can be made in the digitalisation of state services. Why else would GovChat be in a market competition dispute with the one of the world's technology giants – one with deep pockets and part of the megacorporation Facebook? It would be easy to frame this as a David vs. Goliath dispute and root for the relatively small local firm battling the big blue-chip giant. However, this misses a crucial point: a competition dispute, by its very definition, entails fighting over market share. In this case, the battle is over accessing our data and the profit this will generate.

In early January 2021,[117] GovChat submitted a request for interim relief to the Competition Tribunal on behalf of itself and its subsidiary Hashtag Let's Talk (#LetsTalk) against WhatsApp and its parent company, Facebook. An online hearing was held on 13 January 2021.[118] GovChat CEO Jordaan told Open Secrets that it had engaged the "best competition law experts" and had spent R4 million on the case preparing for the preliminary hearing.[119]

The dispute arose because WhatsApp and Facebook were attempting to "off-board" – i.e. remove – the GovChat platform from WhatsApp, potentially placing the Covid-19 SRD grant application process at risk. Allegations of misconduct and underhanded business practice were hurled by both sides. WhatsApp accused GovChat of insidiously violating its terms of service, while GovChat accused WhatsApp and Facebook of attempting to steal GovChat's government clients.[120] WhatsApp and Facebook contended that GovChat used its wholly owned subsidiary, #LetsTalk, to bypass a review process in order to access the WhatsApp platform and provide WhatsApp services to its government clients. WhatsApp asserted that this was in direct violation of its policies, and so, it decided to terminate #LetsTalk's business account.[121] GovChat countered that WhatsApp's threat

to remove the GovChat platform potentially risked pushing it out of business, given its extensive reliance on WhatsApp services. Moreover, if the off-boarding were to occur, it would result in the immediate ending of services to its government partners such as the Department of Social Development.[122]

GovChat approached the Competition Commission on the basis that this was a competition issue, but what markets do GovChat and WhatsApp compete in? GovChat claimed that there are two markets in which it competes with WhatsApp. The first is the market for over-the-top (OTT) messaging applications via smartphones – these are messaging applications like WhatsApp, Facebook Messenger, and WeChat. The second is the government messaging services market in South Africa.[123] GovChat claimed that it, along with #LetsTalk, and WhatsApp (and Facebook) are competitors in these two markets.[124]

On 21 January 2021, the Competition Tribunal ruled in favour of GovChat's request for interim relief,[125] preventing #LetsTalk from being off-boarded from WhatsApp.[126] The Tribunal offered the following rationale for its decision: 1) WhatsApp has at least prima facie dominance in the market for government messaging services through OTT messaging applications;[127] 2) WhatsApp and GovChat are *potential competitors* in the market for mobile payment services through OTT messaging for government departments;[128] and 3) the off-boarding of GovChat from the WhatsApp platform would harm the public during a pandemic (Covid-19) owing to GovChat's role in the processing of Covid-19 SRD grant applications.[129]

MORE TO THE DISPUTE

The dispute also revealed that Praekelt – the same company that initially aided SASSA in their WhatsApp process for the SRD grant – also initially aided GovChat with onboarding its platform on to WhatsApp. However, GovChat says that its contract with Praekelt fell through due to its concerns over Praekelt's chatbox technology.

The fact that this dispute played out before the Competition Tribunal reveals that there is a significant market for the provision of government messaging services by private technology companies. WhatsApp and Facebook might be interested in GovChat's government clients because personal data is at the centre of profit-making activities in the digital age. The business models of mega technology companies like Facebook are based entirely on capturing and accessing people's personal information, both with and without their consent. When we asked Jordaan what he thought, he said that it was a "data play".[130] Jordaan says that Facebook wants full control over the valuable data GovChat currently holds due to its partnerships with so many government departments. Tellingly, he said that GovChat's access to such detailed and "powerful data" could "in the wrong hands mean disastrous things".[131]

So far, we know that GovChat has access to increasing amounts of data about the South African public from its privileged position with SASSA, the Department of Health, and COGTA. We know that one of the world's biggest technology companies, Facebook, also has more than a passing interest in the market that GovChat has cornered. Facebook is the social media platform with the largest user base in South Africa, with 28 million accounts – close to 50 per cent of the country's population. Accessing an additional layer of data (currently held by GovChat) would no doubt only deepen its influence in South Africa.[132]

As we have shown, GovChat's shareholders have expressed an intention to monetise the data to which it has access, and GovChat is considering selling this data to government and other stakeholders. Furthermore, we reveal in the next chapter that GovChat's current privacy policy is very thin and has significant gaps, as does South Africa's regulatory environment. Finally, we know that the GovChat application system has not proven attractive to users: 80 per cent of users have opted for the USSD platform instead of WhatsApp due to lack of access to smartphones and the cost of data. If this is version 2.0 of the digitalisation of social welfare, what might the next frontier of the digitalisation of welfare look like?

A META THREAT

Facebook's attempts to capture more of the market for providing digital services to government departments in South Africa should be of grave concern. Facebook's track record reveals that it routinely violates people's privacy and sells their data without proper consent; most recently, it was fined R4 billion by Irish authorities for violating the European Union's data privacy law.[133] While still popularly known as a "social networking website", Facebook is better understood as "data infrastructure" made up of a "family" of applications and websites, which generates profit through the extraction, analysis, and distribution of our data.[134] This economic model has led Facebook to have a market value of over $1 trillion while granting it extraordinary economic and political power.

As we discuss in the following chapter, abuse of personal data is not the only threat that a company like Facebook poses. It has been at the centre of numerous scandals regarding the spread of misinformation and divisive content. This includes the manipulation of democratic elections around the world by renting the company's capabilities to political groups for the purposes of microtargeting and manipulating users with misinformation.[135] Researchers in numerous countries have also revealed how Facebook's profit-driven algorithms ensure the viral spread of divisive content that fuels the growth of extremist groups, with Facebook's flimsy "content moderation" department unwilling to stop this from happening.[136]

In October 2021, former Facebook data scientist and now whistle-blower Frances Haugen appeared before the U.S. Congress and testified to what she saw while working at Facebook. Haugen testified that Facebook was aware that its algorithms amplified misinformation and could be abused by third parties to urge violence, but the company had made a decision to prioritise growth and profit over reforms; and that it deliberately withheld research identifying the harm caused by Facebook products.[137] Haugen added,

With so many dangers and harms of Facebook's operations known, it is little surprise that the company has ratcheted up its lobbying efforts, giving money to lawmakers to guard its interests and push back against more effective regulation. In 2020, Facebook spent $20 million (R300 million) lobbying American politicians – i.e., in the same year that the company faced multiple hearings in the U.S. Congress on its role in manipulating elections.[139] This was more money spent on lobbying than by any other big technology firm.

Given this track record, Facebook's appetite for contracts with South African government departments and private sector actors to hoover up more data must be watched closely by regulators and civil society. Open Secrets will certainly be doing so.

> **“During my time at Facebook, I came to realize a devastating truth: [a]lmost no one outside of Facebook knows what happens inside Facebook… The company intentionally hides vital information from the public, from the U.S. government, and from governments around the world”.**[138]


AADHAAR

4

AADHAAR: LESSONS FROM INDIA FOR SOUTH AFRICA'S DIGITAL FUTURE

By the end of August 2021, GovChat announced that it had over 8 million active users on its citizen engagement platform and had processed over 500 million messages.[1] It is important to note that every time someone engages with the platform, the details of their location and what device they are using is collected, usually along with their age and gender. This data is collected too from the over 12 million Covid-19 SRD grant applications that the GovChat platform has processed since it was first implemented.[2] As we explained in the previous chapter, these applications also provide GovChat with basic financial information and the ID numbers of applicants, which GovChat checks against a database at the Department of Home Affairs. The result is that GovChat is in the position to develop increasingly detailed profiles of the millions of individuals who interact on its platform, whether they do so to apply for a grant, complain about an electricity outage, or locate a Covid-19 testing site.

Eldrid Jordaan has talked up GovChat's ability to process, analyse, and explain this data. In an interview with Open Secrets, Jordaan said that GovChat enables government departments to improve service delivery because it has the ability to analyse and map the rich data it receives in a way that the state is unable to and use it to "tell a story" to the government.[3] GovChat's story is that this is a victory for open government, transparency, and greater accountability. This rather rosy perspective suggests that an accessible

technology platform to engage local government or to access government services might have great potential to transform governance in South Africa.

Yet digitalising state services via private companies can also result in more opaque, potentially harmful systems that many people find very difficult to navigate, and a blurring of the line between the private and public sphere in terms of governance. GovChat's sprawling role across different parts of the state and the resulting access to millions of people's personal data gives it disturbing power. The implications for people's privacy are significant. Similarly, the surveillance powers of the state, GovChat, and any other party that accesses the data are greatly increased. GovChat is also financially backed by a private company focused on finance and fintech, with the stated goal of monetising GovChat's services – creating a risk that monetisation could take place at the expense of people's rights.

This chapter discusses these risks. It is necessarily forward-looking. Some of the risks discussed have already emerged, but many of them loom on the horizon. Our goal is to identify them, challenge them, and avoid the worst possible outcomes. To do this, we first consider the Aadhaar system – India's digital welfare system that is significantly more advanced than ours. The experience of Indian citizens with this system is a stark warning of the severe and sometimes deadly consequences of an unchecked and unaccountable digital welfare state. We then deduce relevant lessons from Aadhaar for South Africa.

A CAUTIONARY TALE: THE AADHAAR SYSTEM IN INDIA

The problems we are confronting in South Africa are not unique. Precedents exist around the world that allow us valuable insight into our situation, providing stark warning of the risks we face. The largest biometric identification system in the world is the Aadhaar system in India. Arguably, the Aadhaar system is a perfect example of the phenomenon of "digital financialisation" where data is the prize.[4] The data gathered through this system offers a digital footprint that is harvested and transformed into a detailed profile of customers. This in turn is monetised by allowing companies to better target those customers with financial products.[5] It is through this process that profits are made, at the expense of data privacy. This erodes the traditional distinction between financial corporations and technology firms.

Launched in 2010, more than 1.2 billion Indians are now part of the Aadhaar system and have a 12-digit unique identification number.[6] This 12-digit number contains an extraordinary amount of data about its holder, which includes demographic data (such as age, gender, and income) along with biometric information that includes a photograph, fingerprints, and even an iris scan.[7] Having an Aadhaar number is mandatory to access welfare benefits in India, including cash transfers and food. The Aadhaar number is also linked to citizens' bank accounts – particularly those used to pay tax or make investments – as well as their mobile phone numbers.

The Indian government has instructed any service provider to block services to any person who refuses to link their personal information to Aadhaar.[8] Though not yet mandatory, the Aadhaar number is often used to manage people's access to healthcare too. There have been reports of people being turned away from hospitals unless their Aadhaar profiles show up on the online system.[9]

The Aadhaar system was welcomed with much fanfare in India and by international organisations like the World Bank. Its creator, Nandan Nilekani – described as a "genial software billionaire" – had long advocated for Indians to be urgently provided with ID numbers and bank accounts. He argued that the Aadhaar system not only ensured financial inclusion and access to welfare for many poor people in India but also could help eliminate corruption and "wastage".[10] A government agency, the Unique Identification Authority of India (UIDAI), was built around Nilekani to oversee and run the Aadhaar project. When the UIDAI was formed, the headquarters was a typical government bureaucracy in New Delhi. However, the technology and data processing was based in a luxurious campus in Bangalore and run almost entirely by former employees of mega technology corporations such as Google and Intel.[11]

As a "financial inclusion" cheerleader, the World Bank has not only endorsed the system but also encouraged other countries to

learn from it, arguing that its ability to be "inclusive" and overcome information gaps between citizens and governments is transformative.[12] Despite this, critics of the system have alleged that the project is predominantly aimed at profit for the private companies that provide various services for the system. In 2017, journalists at the *Indian Express* reported that numerous current or former executives at the UIDAI were launching companies or start-ups that were then offering Aadhaar-linked services such as "user authentication" for lucrative fees.[13]

Other journalists have called the Aadhaar system the "New Oil". They note that those private companies that have access to Aadhaar-specific application programming interfaces – including those who do background checks on employees for companies at a fee – have access to an extraordinary amount of data through Aadhaar and the other databases that they use for verification.[14]

Researchers from the Centre for Human Rights and Global Justice at New York University say that private profit is precisely what the Aadhaar system was designed for and that:

> **"From the outset, the Aadhaar 'business model' would benefit private companies by growing India's 'digital economy' and creating a rich and valuable dataset. In particular, it was envisioned that the Aadhaar database could be used by banks and fintech companies to develop products and services, which further propelled the drive to get all Indians onto the database. Given the breadth and reach of the database, it is an attractive asset to private enterprises for profit-making and is seen as providing the foundation for the creation of an 'Indian Silicon Valley'.[15]**

This exemplifies the phenomenon of "digital financialisation", where data, like oil, is a profitable commodity, harvested at the expense of privacy.

In addition to profiteering, there are a series of other risks and harms resulting from the Aadhaar system that arguably far outweigh any benefits. For one, the system provides the Indian state with far-reaching surveillance powers that constitute severe invasions of individual privacy. Indeed, requiring citizens to link almost all aspects of their lives to a state identification system can open them up to "dystopian levels of state surveillance".[16]

The Aadhaar system provides spooky new capabilities to spy on government critics. For example, the Electronic Frontier Foundation points out that iris scanning – as is required by the Aadhaar system – allows law enforcement and other parts of the state to "track people covertly, at a distance or in motion, without their knowledge or consent", raising serious concerns about privacy rights.[17] The Indian government has shown a willingness to surveil and harass critics of the Aadhaar system, as well as other civil society activists.[18]

Another big risk, revealed by journalists, is the failure to secure and protect the data. One journalist bought access to a portal that provided data linked to anyone who held an Aadhaar card.[19] The journalist did so to raise awareness of privacy risks, and was later sued by the state. In another example, the Indian Centre for Internet and Society published a report about government websites leaking millions of Aadhaar numbers. The report's authors were served with legal threats and allege they were harassed by law enforcement.[20]

These breaches could be the tip of the iceberg. The Electronic Frontier Foundation explains:

> **"Databases of iris biometric [information] are a honeypot of sensitive, highly personal data that will be targeted by criminals. Data breaches and hacks are at an all-time high. Biometric information is a special risk because it's not possible to revoke, cancel, or reissue an eyeball if digital biometric information is stolen or compromised".[21]**

Despite these serious concerns, in 2018, a majority of the Indian Supreme Court found the Aadhaar programme to be constitutional and not an unfair infringement of people's right to privacy.[22] However, the court also demanded greater controls over the system and

struck down a series of efforts by the state and private sector that had sought to extend the reach of the programme, including preventing private banks and cell phone companies from using Aadhaar numbers to verify customer identities.[23]

A prescient warning about the potential abuse of Aadhaar by authoritarian forces wishing to achieve social control comes from Indian author and social critic Arundhati Roy:

> *It's like digital surveillance, phone surveillance, and the collection of private data, not just through Facebook and so forth but also by governments. It is going to be the way in which human populations are going to be controlled. It is already a way in which humans are controlled but on a scale that you can't even imagine. It makes you just want to die.*[24]

Proponents of digital systems argue that the risks to privacy and security are worth the opportunity to provide access to "inclusive" services. However, the Aadhaar system is also a case study in how those promises can be oversold, and of the very real risks of excluding people from services for technical reasons. The bulky centralized database has often resulted in errors that have denied people access to essential food and other services. Between 2017 and 2018, at least 15 people, including an 11-year-old child and an 11-month-old infant, died after being refused subsidised food rations and medical care.[25] The reasons given ranged from technical glitches, biometric failures, missed deadlines, and failure to present an Aadhaar ID card.[26]

These failures are not isolated to the Indian system. Researchers from the Child Poverty Action Group in the UK reported that many people were refused benefits when applying through an online system. They also did not receive information about why their claims were denied or how to access recourse.[27] There are significant risks when such determinations are transferred from human caseworkers to automated systems where "decision-making is embedded in secret and proprietary code".[28]

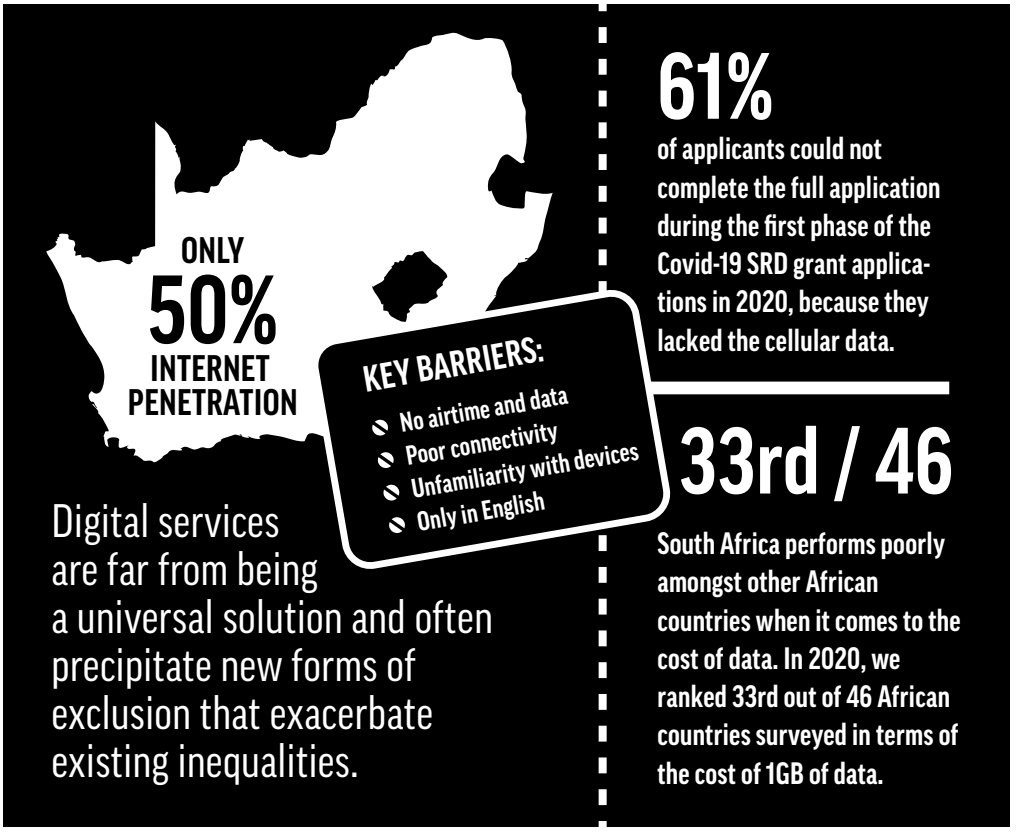
Errors of exclusion often result from an outsized emphasis on catching out fraudulent claims. Any small data entry error by applicants can be flagged as fraud or an effort to "work" the system. This is particularly so in places where negative perceptions of welfare recipients prevail. For example, when the U.S. state of Indiana created an automated eligibility programme to screen applicants for welfare, one million applications were denied in the first three years; this represented a 54 per cent increase over the previous three-year period.[29] Researchers demonstrated this was because the algorithm coded any single mistake in the application process (which could amount to over 100 pages) as a "failure to cooperate in establishing eligibility".[30]

Such examples highlight the social risks contra the grand promises of inclusivity. Despite the numerous concerns around the dangers of the Aadhaar system, South Africa has begun to adopt similarly far-reaching biometric identification programmes as a prerequisite to access the state's welfare services. The South African Social Security Agency is already the largest collector of biometric data (e.g. fingerprints, photographs, and voice recordings) of every individual receiving a social grant.[31] Likewise, the Department of Home Affairs already has a biometric database of all South African adults – the Home Affairs National Identification System (HANIS) – and in 2021, announced its intention to collect photographs and fingerprints of every baby born and to assign them a digital ID number without conferring citizenship.[32] The Department of Home Affairs intends to collect much more detailed biometric data in the future, including DNA and photographs of eyes, ears, hands, and feet in order to create a "legal record of existence".[33]

There is a real risk that these extensive biometric databases will be combined and used to create a single detailed biometric ID for all South Africans to access government services. But, while that is still a few years off, let us consider what the Aadhaar system can tell us about current risks embedded within our digitalised welfare system.

“It’s like digital surveillance, phone surveillance, and the collection of private data, not just through Facebook and so forth but also by governments. It is going to be the way in which human populations are going to be controlled. It is already a way in which humans are controlled but on a scale that you can’t even imagine. It makes you just want to die”.

~ Arundhati Roy



INEQUITABLE ACCESS

Companies selling digital solutions to governments promise accessibility. Yet, from what we have seen with both the Net1 and GovChat systems, the reality is very different. A report by the Black Sash investigated the accessibility of digital platforms for the Covid-19 SRD grant, including GovChat's WhatsApp platform. Lack of airtime and data, poor connectivity, and unfamiliarity with some digital devices meant that many South Africans struggled to access and complete the digital application process.[34] In fact, a huge number of applications were initiated but never completed, suggesting people struggled to follow the process through. Additionally, in a nation of 11 official languages, people could only answer the questions in English.[35] These experiences challenge GovChat's claims to be broadening citizenship by enabling "democracy between the ballot boxes".

These findings are unsurprising. At marginally over 50 per cent, South Africa has relatively low Internet penetration when compared to many other African countries, and it has extortionate data costs – especially on pre-paid plans – when compared to the rest of the continent.[36] Speaking to Open Secrets, GovChat CEO Jordaan admitted that during the first phase of the Covid-19 SRD grant applications in 2020, three million out of the 4.9 million applicants could not complete the full application because they lacked the cellular data to access the web portal that was required to input one's ID number.[37] This is a massive drop-off rate and should be of grave concern to SASSA. Likewise, the experiences relayed to the Black Sash by grant applicants show that digital services are far from being a universal solution and often precipitate new forms of exclusion that exacerbate existing inequalities.

OUTSOURCED GOVERNANCE

A major concern about privatised digital welfare systems is that the technology itself is doing the governing, rather than elected representatives. The systems outsourced by SASSA are effectively making decisions about whether or not to grant applicants' benefits. The UN Special Rapporteur on Extreme Poverty and Human Rights, Philip Alston, has found that digital welfare systems have a high

error rate on automated eligibility checks. In his words, **"online portals can create confusion and obfuscate legal decisions, thereby undermining the right of claimants to understand and appeal decisions affecting their social rights".**[38] In effect, an applicant often gets told they are ineligible, with little indication of why or how to challenge the process.

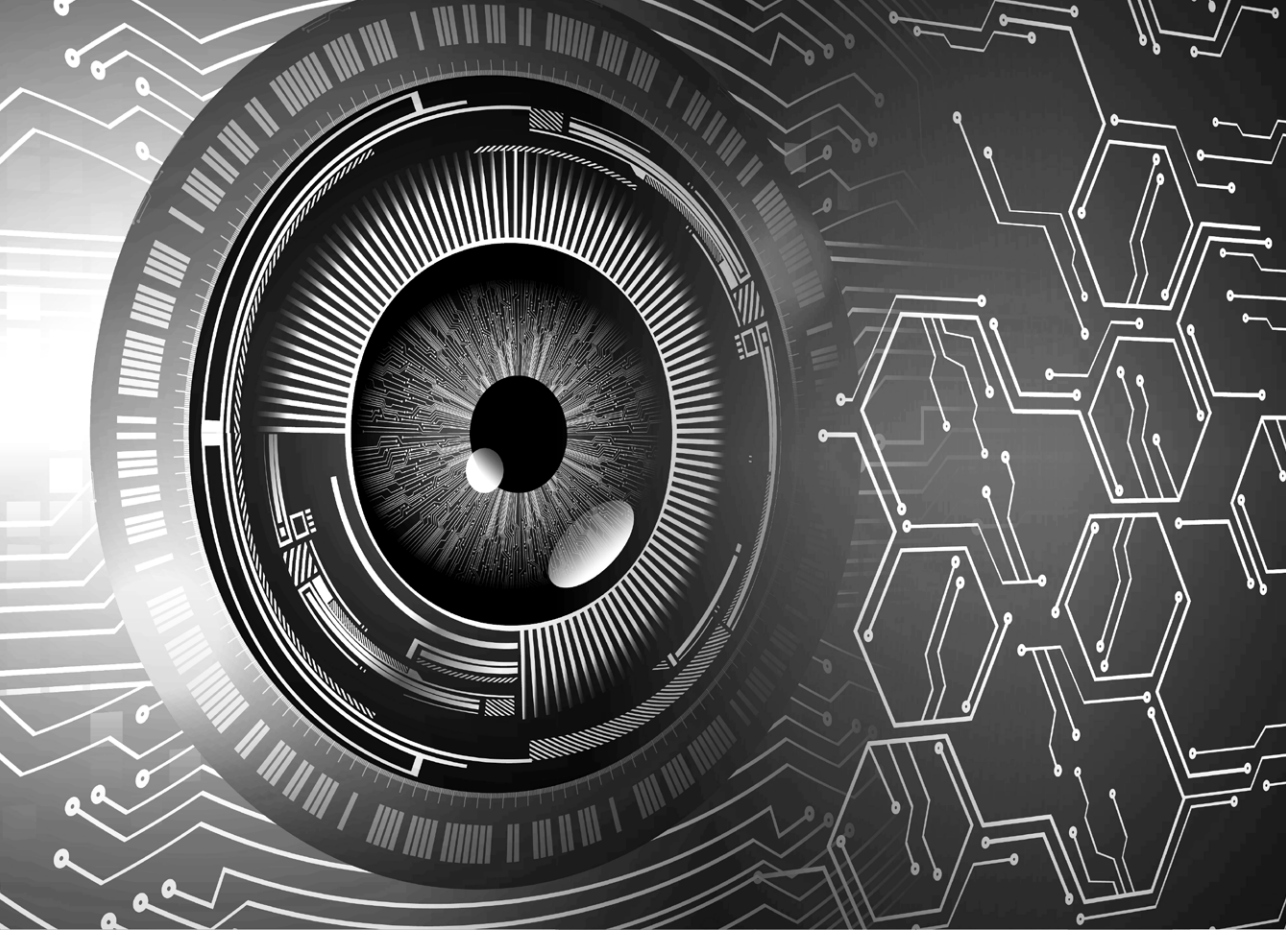
In the case of the Covid-19 SRD grant, applicants who managed to complete the application with GovChat and on other digital platforms were often rejected in error. The Black Sash found that a third of all applicants were declined, and the majority of these were labelled ineligible because their names came up on a South African Revenue Service (SARS), UIF, NSFAS, or SASSA database – purportedly indicating they were receiving income.[39] Many of these databases were outdated (for example, the UIF is known to be two–three years out of date), but there was no easy way for applicants to challenge and correct the data. Applicants could only appeal through the same digital platform that had made the error in the first place and could not submit additional documentation. Unless there had been a change to the database itself, they were sure to be denied again. The appeal process was often delayed, leaving vulnerable people facing hunger.[40]

GovChat and other companies providing a digital application process can always dodge responsibility by saying that the accuracy of the database maintained by the state is not under their control. Yet SASSA is simultaneously pushing applicants to use the digital platforms and reducing the amount of direct contact that an applicant can have with a SASSA employee, whether in person or on the phone. This kind of outsourcing of government function inevitably blurs the lines between the state and the private sector when they co-create and run digital governance platforms. For citizens engaging with these platforms, it is very difficult to know how to respond and hold either actor accountable for fulfilling their constitutional obligations. The absence of proper recourse is also a blatant negation of just administrative action.

In the case of the Covid-19 SRD grant, when the pandemic led the state to step away from face-to-face assistance, the burden of helping grant applicants fell onto community support structures and monitors, such as those working for the Black Sash, and their community advice offices. Due to a lack of confidence in the digital system, as well as barriers to understanding the system, numerous people sought out help from these sources.[41] As the Black Sash noted, "[W]hile the system set out to eliminate face-to-face applications between SASSA and the population, it ended up off-loading this responsibility onto the Black Sash monitors and other local community support structures".[42] This has not stopped GovChat from boasting that its process saved SASSA R7.5 million in call centre costs. This "saving" derived from the unacknowledged labour of the Black Sash and community advice office workers around the country.

Efforts to promote accountability are made even harder by the added layer of complexity and secrecy that is inevitable when private actors like GovChat develop and operate the digital services used by states. Their role is often undefined or under-explained. In the case of GovChat, for example, there is no publicly available information about how and to what extent the company has access to state databases like those of SARS, NSFAS, UIF, or Home Affairs. We now know that it does verify ID numbers against Home Affairs' data, but when we asked about other databases, GovChat CEO Jordaan was vague and said that while GovChat "could do it", SASSA currently fulfilled that role.[43] The opacity is yet greater when corporate confidentiality and the intellectual property concerns of private actors are involved.[44] While the safeguarding of intellectual property rights is quite understandable, this opacity provides an open door to corruption and malfeasance.

South Africa's Protection of Personal Information Act requires that for any automated decision, a person must receive "sufficient information about the underlying logic of the automated processing of the information" relating to that person to allow them to exercise a right to respond to the decision.[45] In the case of the Covid-19 SRD grant, applicants were not informed fully about how their information was being processed and faced significant obstacles in speaking to a SASSA employee about it. Further, given that it was GovChat's proprietary software – built by Synthesis and operated using Amazon Web Services – that was being used, it is unlikely that SASSA employees could explain exactly how the information processing worked to an applicant.[46]



TARGETED MARKETING OF FINANCIAL PRODUCTS

Another significant risk is that of reckless lending to social grant applicants and resulting indebtedness. This was of course what happened under the Net1 distribution system. Net1's subsidiary companies used their intimate knowledge of grant recipients to sell them loans, insurance, airtime, and electricity through the grant application and distribution system itself. With the data GovChat is collecting, there is a significant possibility of even better targeted marketing toward grant beneficiaries in need.

Financial products like those previously provided by Net1 are a red herring: poor people of course need credit, but the way it is given – attached to social welfare benefits – puts the microlenders in a powerful position. Through access to the financial data of grantees, they can aggressively market their products to people who do not have the resources to cover their monthly expenses. They can also use technology to limit the risks of default, while still charging very high (though legal) rates of interest on unsecured credit. This can lead to unsustainable indebtedness for people, who have to turn to additional sources of credit to get through the month.

Other companies, outside of the financial sector, might also desire access to this data to sell things to grant recipients. In 2004, academic C.K. Prahalad wrote a book that referred to poor people as holding a "fortune at the bottom of the pyramid", and it has been used since then by people like Bill Gates to espouse the idea of "fighting poverty with profitability".[47] Since that time, and even before, corporations have tried to tap into this so-called fortune, often providing inappropriate products at considerable cost and only exacerbating inequality.

THE NEW SURVEILLANCE STATE: THE END OF PRIVACY?

The capacity of corporations and governments to surveil citizens in increasingly intrusive ways for the sake of profit and control is increased dramatically by platforms like GovChat. This is, very briefly, acknowledged

in the 150-page report of the Presidential Commission on the Fourth Industrial Revolution. There is one throwaway line at the bottom of page 18 that reads: "Digitalisation also increases the surveillance capacity of the government and firms in ever more areas of individuals' lives"".[48] Surveillance is not mentioned again, but given our constitutional right to privacy, should be of grave concern.

GovChat's position as the "official citizen engagement platform", coupled with its role processing social grant applications, gives it extraordinary access to the personal data of millions of people, including location data, grant data (including financial information), health data, status of infrastructure data, criminal activity reporting data, and more. GovChat CEO Jordaan told Open Secrets that the company not only collects the data but also successfully maps and visualises the data for it to be used "more effectively by government".[49] He assured Open Secrets that all data is anonymised, encrypted, and inaccessible even to GovChat employees.[50] However, in our PAIA request, we asked the Department of Cooperative Governance and Traditional Affairs for the documents related to its contract with GovChat, including the privacy policy. We were surprised to find that the document is a brief six pages, which explain that GovChat can use the data it collects to compile anonymous statistical data and analysis and share it with third parties, including any party that provides services for GovChat, such as CAPPREC's subsidiary, Synthesis.[51]

While the policy and Jordaan claim that the data GovChat keeps is always fully anonymised, this is at best a half-truth. Research now shows conclusively that if you have access to enough data points on an individual, it is incredibly easy to "re-identify" them within "anonymised" datasets. In fact, a 2019 study by researchers at Imperial College London and the University of Louvain found that 99.98 per cent of Americans could be re-identified in any dataset if one used just 15 demographic attributes (such as age and gender) about each person.[52] These attributes are easily available to third parties, given the extensive data collection that occurs about individuals daily and is regularly bought and sold. Likewise, in 2016, German journalists created a fake company and bought the "anonymous" browsing habits of three million Germans. They were able to easily re-identify individuals – including politicians – and determine their sexual preferences and medical information, amongst other personal information.[53] Complete anonymisation of data is not possible to achieve using current methods of doing so.

Such violations of privacy are lucrative in the new data economy, in which hundreds of companies compile, sell, and purchase data to predict and influence future behaviour.[54] This means that GovChat sits on a veritable gold mine of data. Yet it also poses a serious threat to people's privacy, and the potential impacts are most serious for already vulnerable groups of people. As noted by Chenai Chair, a researcher on the intersection of digital technology and gender:

> **"The collection, processing, use, and dissemination of data takes place amid existing structural inequalities that raise the risk of surveillance, violence, and other human rights violations. Various actors have used surveillance as a tool to control women, gender-diverse people, and sexual expression when something does not fit into the hetero-patriarchal norm. Privacy breaches increase the vulnerability of women and gender-diverse people, as their private data is found online and is used to track and monitor them".[55]**

When it comes to digital applications for grants, applicants have very little choice but to supply their data to whomsoever SASSA happens to contract with. A grant applicant needs the grant for the very basic necessities of survival, and access can be a matter of life or death. As noted by Chair, the capacity to consent is informed by social context and vulnerable groups in dire need may not be able to say no to having their data collected, regardless of how it is used.[56]

The Information Regulator has a vital role to play in protecting our privacy. It has been established to ensure the compliance of public and private entities with the Protection of Personal Information Act.[57] POPIA is a far-reaching Act that lays down crucial principles to prevent the abuse of people's personal data and to ensure openness, security safe-

INFORMATION REGULATOR (SOUTH AFRICA)

guards, the participation of "data subjects" (people), and the accountability of any party that gathers, manages, and processes data.[58] As such, the Information Regulator has the task of protecting the public from potentially harmful surveillance and profiteering practices by the state and private companies seeking to monetise this data.

In April 2021, the Information Regulator took a very encouraging step, when it indicated that it would be tackling WhatsApp and its parent company, Facebook, head-on to ensure that they complied with POPIA and did not use and process unique identifying data, like phone numbers, "with the aim of linking that information jointly with information processed by other Facebook companies".[59] This is an important step, as it targets the same issue as that raised by the case of GovChat, i.e. how the company may use the data gathered through the digitalisation of social grants. The intention to tackle Facebook head-on is a positive sign that the Information Regulator views the way in which technology firms profit from processing personal data as a priority focus area. Digital profiteering risks violating many constitutional rights, so it is crucial to have a regulatory authority willing and able to enforce the regulatory framework pertaining to the monetisation of data.

A final consideration with regard to privacy is how access to such detailed data about individuals can be weaponised by the state in surveilling citizens, particularly when the state is able to "re-identify" individuals within allegedly "anonymized" datasets. In its privacy policy, GovChat says that it will use data to monitor and analyse usage and trends during times of crises.[60] "Crisis" is left undefined, and while the Covid-19 pandemic is an obvious example, the recent widespread public violence and insurrection focused in KwaZulu-Natal and Johannesburg also seems a likely candidate.

As mentioned earlier, Jordaan himself has talked up the ability of GovChat's systems to provide data to law enforcement. In 2017, when he was looking to sell the company and find a technology partner, he indicated that the data GovChat gathered could also be used for image recognition, citizen engagement, data mining, and identification of protest patterns.[61] Jordaan's hope was to have a system that would be able to learn to put faces to names in photographs and "able to smell unrest before it breaks out". He added,

> **"[S]ay there is an uprising in a community, we can then link that data to SAPS [the South African Police Service]... [W]e want to make them more efficient, better informed ... so we can tell them this is what is brewing – let's be ready just in case something happens".[62]**

The South African state has already begun to partner with private firms like Vumacam to establish vast networks of cameras to track millions of people and vehicles, vastly increasing its surveillance capacity.[63] In response to the recent public violence and in policing the rules of the Covid-19 pandemic, the police and military have revealed that poorer communities will bear the brunt of state violence. This is particularly concerning because the dataset from the Covid-19 SRD grant comprised predominantly young unemployed black men – a population that the government certainly wants to surveil for potential unrest. Any dataset that can help it do so is an example of racialised policing and a huge violation of civil liberties.

THE THREAT TO DEMOCRATIC PROCESSES

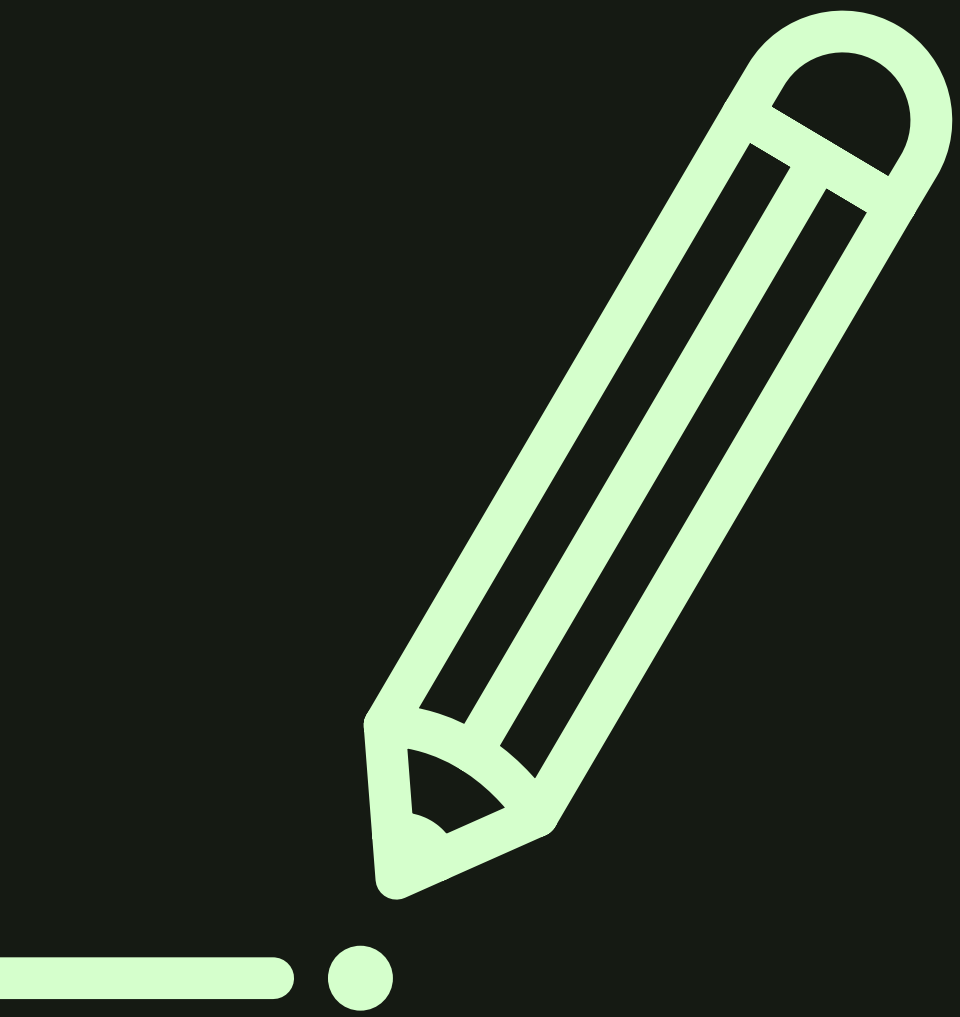
The collection of data by corporations and the state does not only pose a threat to our privacy. It also provides opportunities for the manipulation of elections and other democratic processes. Political parties and candidates aim to influence the outcome of democratic processes by profiling individuals, based on the processing of vast amounts of data, to infer characteristics and political views and preferences, and then targeting them directly with propaganda and misinformation.[64] As noted by Privacy International,

> **"[S]uch an approach to democratic process presents novel challenges due to the scale and range of data available together with the multiplicity, complexity and speed of profiling and targeting techniques. All of this is characterised by its opacity. Existing legal frameworks designed to curtail this exploitation often also fall short, either in substance or enforcement".[65]**

Two cases of electoral manipulation through mass data that have dominated headlines are the targeted misinformation campaigns for Donald Trump's successful 2016 electoral campaign in the United States and the Leave EU campaign in the United Kingdom, both orchestrated by British firm Cambridge Analytica.[66] Yet the reality is that this has become ubiquitous around the world, with political candidates hiring private firms at exorbitant fees to amass and analyse data, all with the aim to "attract or suppress votes from certain constituencies through micro-targeting and direct messaging".[67]

The great risk to democratic processes is that neither the implicated private firms nor political parties properly disclose how citizens' data is used and shared, and voters are "unaware that they are receiving political messages based on bias".[68] Nor have large platforms like Facebook shown sufficient will to prevent the spread of misinformation through their social media channels.

In the South African case, it is hard to imagine that political parties have not or will not see the potential for using GovChat's databases and data analysis for this purpose. GovChat says that it plans to sell detailed analysis of the data on millions of people that it gathers across its platform, to allow government departments to improve service delivery. Yet, as we have witnessed in recent elections, many political parties have consistently shown they will go to great lengths to secure a vote but will do little to improve service delivery for voters. Combining the data they can purchase from social media platforms and other companies with the detailed analytics provided by a company such as GovChat, parties will be able to buy detailed profiles of individual voters for the purposes of electioneering and ultimately manipulating voter behaviour. As we have seen from imperilled democracies such as the United States and the United Kingdom, this kind of abuse of digital information benefits wealthy conservative groupings which have little interest in the democratic project other than as a means to grab power.



5

RECOMMENDATIONS AND CONCLUSION

GREATER TRANSPARENCY

This investigation has shown the considerable risk that exists when private companies co-create the digital infrastructure used by the state to gather data from people and provide essential services to them. A key concern relates to the opaque and complex way digital systems work and how they process, store, and use the data they gather. As noted by German researchers examining corporate power in a digital world,

> **"[T]he growing use and significance of data and algorithms stands completely out of proportion to the stagnancy in our poor understanding of how the data are used".**[1]

Companies and state agencies must thus be fully transparent about how the data gathered as part of a digital grant application process is collected, managed, and secured, and crucially, about the ways in which it will

be monetised. This is imperative, and no element of this transparency can be subordinated to the commercial interests of the companies involved.

Furthermore, state agencies like the South African Social Security Agency must publish simple and easy to understand information in all South African languages that explains these processes. This is vital to ensure that the legal consent requirements in the Protection of Personal Information Act are met. **Such consent must be properly informed, freely given, and continuing. People must be made aware that they can withdraw that consent any time and have a right to be informed of any data breaches. Data management and use processes should be clearly articulated in a user friendly and accessible manner. Consent pages should also be available in different languages to further ensure that users are aware of what they are agreeing to.**

A final but vital part of greater transparency is to require, as far as possible, the use of open-source software for all digital systems created and used for the application and processing of social grants. Open-source software ensures that the programming code is publicly available, and thus how it works and how secure it is will always be open to public scrutiny. This contrasts with the closed-source proprietary software of most major technology companies, such as Amazon and Google, that firms like GovChat still rely on heavily.[2]

EFFECTIVE REGULATORS

Transparency is not a sufficient safeguard against digital profiteering by companies involved in the provision of social grants. Vital provisions of the law must be enforced by the Information Regulator, particularly those relating to the transparency, security, and privacy measures implemented in data processing systems used between government entities and private companies providing digitalisation services.

As discussed in chapter 4, the Information Regulator is mandated by law to protect the public from potentially harmful surveillance and profiteering practices by the state and private companies seeking to monetise their personal data. **With regard to the digital application systems for social grants, the Regulator must thus ensure that the movement of grant applicants' data is fully secure and protected in all interactions with the digital platform being used: at the application stage, in the verification of identification, during the needs assessment, and at the time of payment.**[3] It must also ensure that this data is only used and exchanged for the necessary purposes of the grant application, and nothing else.

Given this vital task, it is concerning that the Information Regulator has been slow to become operational and effective, partly due to lawmakers' failure to provide adequate resources to the institution. Given the Regulator's public interest mandate, this must be rectified, and its leadership must take urgent steps to build the agency's capacity.

Through the discussion of Facebook and GovChat's competition dispute, we have also demonstrated how fundamental the issue of market competitiveness is for our personal data. It is vitally important that competition law is enforced to prevent monopolisation and its abuses. Relevant state actors and institutions, notably the Competition Commission, must ensure a fair and competitive environment. While the Competition Commission has begun to interrogate ways of ensuring this, measures need to be put in place quickly before any technology company is able to monopolise the provision of digitalisation services to government entities.[4]

EQUITABLE ACCESS AND DEMOCRATIC PRINCIPLES

While this report indicates a deep concern about the abuse of digitalisation at the expense of vulnerable people, it does not suggest that digital processes can or should be abandoned. Digital and technological advancements provide significant possibilities and improvements to service, but these advantages are not guaranteed. In this report, we have explained at length how they risk entrenching the very inequalities they claim to address.

This contradiction is obvious in South Africa where a considerable mass of the population lacks the basic resources required to access online services. Despite this, SASSA has promised the automation and digitisation of all its grant application services in roughly the next five years.[5] **It is thus crucial that the entire online social welfare service and application process is provided as a zero-rated data service, with applicants not needing to incur any data or airtime costs to access it. Moreover, the South African government cannot continue to pursue a new digital age without simultaneously ensuring the roll-out of infrastructure to allow greater access to the Internet and ensuring a dramatic decline in the currently extortionate cost of data.**

Accessibility should not be limited to data alone. Ensuring that websites and online platforms communicate information in a variety of South African languages, along with providing spaces for grantees to learn how to work through these new digital systems while making them aware of the implications of providing their data and where it will go, is critical.[6] Further, international experience shows that it remains impossible to run an effective, compassionate, and accurate social welfare system without keeping caseworkers and employees available to assist people through any process. Regardless of the steps taken to ensure greater access, not everyone will be able to navigate digital platforms. A great many people are not able to operate digital technology, nor will they ever be able to do so. Yet, as citizens, they must be considered on their own terms.

The common theme running through the report and the recommendations is that the South African government must prioritise the constitutional rights of all people when digitalising social welfare and introducing digital systems as part of its vision for South Africa's Fourth Industrial Revolution. South Africa's own experience with Net1 and the experience of countries around the world, such as India, facing similar challenges to ours in digitalising social welfare provide a stark warning of how governments and corporations can abuse these systems for surveillance and profit at the expense of people's rights.

It is imperative that the next phase of digitalisation reverses this trend, and that inclusive and transparent systems are built to prevent reckless profiteering or insidious and pervasive surveillance. This will require a proactive and critical approach by civil society and public regulators to rein in the rapacious profit seeking by technology firms from around the world and at home.

NOTES:

INTRODUCTION

1: Esme Berkout et al (2021), *The Inequality Virus: Bringing together a world torn apart by Coronavirus through a fair, just and sustainable economy,* Oxfam, Oxfam Briefing Paper, January 2021.

2: Prinesha Naidoo (24 August 2021), 'South Africa's unemployment rate is now the highest in the world', *Aljazeera,* URL: https://www.aljazeera.com/economy/2021/8/24/south-africas-unemployment-rate-is-now-the-worlds-highest [Accessed 12 September 2021].

3: South African Social Security Agency (2019), SASSA Strategic Plan 2020 – 2025, *SASSA*, URL:https://www.sassa.gov.za/strategic-plans/Documents/SASSA%20Strategic%20Plan%20-%202020-2025.PDF [Accessed 29 June 2021]. SASSA says that the ultimate goal is 'automated social grants beneficiaries records, fully automated social grants application including digital signature and gradual migration from legacy system to modern solutions'.

4: Avani Singh (23 June 2020), 'Why POPIA is about rights – not just compliance', altadvisory, URL: https://altadvisory.africa/2020/06/23/why-popia-is-about-rights-not-just-compliance/ (Accessed 02 November 2021].

5: Section 5 (a)-(i) of the Protection of Personal Information Act 4 of 2013, as analysed in Avani Singh (23 June 2020), 'Why POPIA is about rights – not just compliance', altadvisory, URL: https://altadvisory.africa/2020/06/23/why-popia-is-about-rights-not-just-compliance/ (Accessed 02 November 2021].

6: Section 39 and 40 of the Protection of Personal Information Act 4 of 2013.

7: Simnikiwe Mzekandaba (26 August 2020), 'Information Regulator eyes bigger budget amid surge in data breaches' IT Web, URL: https://www.itweb.co.za/content/GxwQD-71Z580MlPVo [Accessed 02 November 2021].

8: Natasha Lomas (24 June 2020), 'GDPR's two-year review flags lack of vigorous enforcement', Tech Crunch, URL: https://techcrunch.com/2020/06/24/gdprs-two-year-review-flags-lack-of-vigorous-enforcement/ [Accessed 02 November 2021].

9: South African Social Security Agency (March 2021), 'Twelfth Statistical Report: Payment System', Period: March 2021.

10: Ugo Gentilini, Mohamed Almenfi, and Pamela Dale (2020), 'Social Protection and Job Response to Covid-19: A Real-Time Review of Country Measures, 11 December 2020, *World Bank*. URL: https://documents1.worldbank.org/curated/en/467521607723220511/pdf/Social-Protection-and-Jobs-Responses-to-COVID-19-A-Real-Time-Review-of-Country-Measures-December-11-2020.pdf

11: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021], p. 1. Alston specifically cited a submission by civil society organization Black Sash regarding the scandal of Net1 and its subsidiary CPS and the way these private corporations abused and sought to profit from their access to grant recipients' data.

12: Shoshana Zuboff (2019), *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power,* (London: Profile Books), p. 21.

13: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021], p. 1.

SOUTH AFRICA'S 4IR FUTURE: A BIG DATA BONANZA

1: Shoshana Zuboff (2019), *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power,* (London: Profile Books), p. 21.

2: Klaus Schwab (2017), *The Fourth Industrial Revolution,* Currency Press.

3: Department of Communications and Digital Technologies Notice 591 of 2020 (23 October 2020), 'Report of the Presidential Commission on the 4th Industrial Revolution (PC4IR)', Government Gazette No. 42388.

4: Micah Reddy (2019), 'Ramaphosa Jnr's blockchain belly-flop.' *amaBhungane.* 13 December 2019. URL: https://www.businessinsider.co.za/cyril-ramaphosa-tumelo-blockchain-ai-conference-fyre-festival-2019-12

5: Bitcoin Events (2021) 'Blockchain Africa Conference 2022: From Hype to Mainstream." URL: https://blockchainafrica.co/speaker/mpho-dagada/

6: M Hilbert and P López (2011), 'The world's technological capacity to store, communicate, and compute information.' *Science.* 332(6025): 60-65.

7: Shoshana Zuboff (2019), *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power,* (London: Profile Books).

8: Shoshana Zuboff quoted in Joanna Kavenna (4 October 2019), 'Shoshana Zuboff: "Surveillance capitalism is an assault on human autonomy"', *The Guardian*, URL: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy [Accessed 28 June 2021].

9: E Morozov (2015) 'Socialize the Data Centers.' *New Left Review.* Jan/Feb. URL: https://newleftreview.org/issues/ii91/articles/evgeny-morozov-socialize-the-data-centres

10: James Meadway (August 2020), 'Creating a digital commons', *The Centre for Economic Justice at the IPPR*, London, URL: https://www.ippr.org/files/2020-08/creating-a-digital-commons-august20.pdf [Accessed 28 June 2021] p. 9.

11: James Meadway (August 2020), 'Creating a digital commons', *The Centre for Economic Justice at the IPPR*, London, URL: https://www.ippr.org/files/2020-08/creating-a-digital-commons-august20.pdf [Accessed 28 June 2021] p. 9.

12: Shoshana Zuboff quoted in Joanna Kavenna (4 October 2019), 'Shoshana Zuboff: "Surveillance capitalism is an assault on human autonomy"', *The Guardian*, URL: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy [Accessed 28 June 2021].

13: Samuel Gibbs (2 July 2014), 'Facebook apologises for psychological experiments on users', *The Guardian*, URL: https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users [Accessed 28 June 2021].

14: The Finance Innovation Lab (December 2020), *Lifting the lid on FinTech: What does new technology really mean for a financial system that serves people and planet?* URL: https://financeinnovationlab.org/wp-content/uploads/2020/11/Lifting-the-Lid-on-Fintech-Finance-Innovation-Lab.pdf [Accessed 28 June 2021].

15: Jeffrey Chester (31 March 2020), 'Platforms, privacy, pandemic and data profiteering: The Covid-19 crisis further fuels unaccountable growth from the digital tech and media industries', *Center for Digital Democracy*, URL: https://www.democraticmedia.org/article/platforms-privacy-pandemic-and-data-profiteering-covid-19-crisis-further-fuels-unaccountable [Accessed 28 June 2021].

16: Adam Satariano (2 September 2021), 'Facebook's WhatsApp is fined for breaking the E.U's data privacy law', *New York Times*, URL: https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html [Accessed 29 September 2021].

17: Louise Amoore (2009) 'Algorithmic War: Everyday Geographies in the war on Terror.' *Antipode* 41(1): 49-69.

18: Louise Amoore (2009) 'Algorithmic War: Everyday Geographies in the war on Terror.' *Antipode* 41(1): 49-69.
19: Privacy International (2021), 'Shedding light on the DWP Part 2 - A Long Day's Journey Towards Transparency', *Privacy International,* URL: https://privacyinternational.org/long-read/4397/shedding-light-dwp-part-2-long-days-journey-towards-transparency [Accessed 28 June 2021].
20: Privacy International (2021), 'Shedding light on the DWP Part 2 - A Long Day's Journey Towards Transparency', *Privacy International,* URL: https://privacyinternational.org/long-read/4397/shedding-light-dwp-part-2-long-days-journey-towards-transparency [Accessed 28 June 2021].
21: Privacy International (2021), 'When Big Brother Pays Your Benefits', *Privacy International*, URL: https://privacyinternational.org/taxonomy/term/675 [Accessed 28 June 2021].
22: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 818.
23: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 818.

NET1 AND CPS: VERSION 1.0 OF DIGITALISING SOCIAL WELFARE

1: Torkelson, E. (2020). "Collateral Damages: Cash Transfer and Debt Transfer in South Africa. World Development. 126.
2: Hulme, D., Hanlon, J., & Barrientos, A. (2012). *Just give money to the poor: The development revolution from the global South*. Boulder, CO: Kumarian Press.
3: Clemence, Z. & MacLellan, F. (2017). Cash transfers get an upgrade. *FinDev Gateway.* Washington, DC: FinDev Gateway. Retrieved from http://www.findevgateway.org/blog/2017/may/cash-transfers-get-upgrade.
4: Bold, C., Porteous, D., & Rotman, S. (2011). Social cash transfers and financial inclusion: Evidence from four countries. *CGAP Focus Note 77*. Washington, DC: Consultative Group to Assist the Poor.
5: Collins, D., Morduch, J., Rutherford, S., & Ruthven, O. (2009). *Portfolios of the poor: How the world's poor live on $2 per day*. Princeton, NJ: Princeton University Press.
6: Porteous, D. (2006). Scoping report on the payment of social transfers through the financial system. *Bankable Frontier Associates*. London, UK: Department for International Development. p. 23.
7: While there are 17.6 million beneficiaries, there are only 10 million recipients, because some recipients receive grants for multiple beneficiaries, e.g. mothers with multiple children.
8: Robyn Foley and Mark Swilling (2018). 'How One Word Can Change the Game: Case Study of State Capture and the South African Social Security Agency.'; Net1 (2008). *Annual Report*. Net1 UEPS Technologies.
9: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
10: Adapted from: Kotzé, H. (2018). Net 1 UEPS Technologies, Inc. Chairman's letter. *2018. Annual report*. Johannesburg: Net1 UEPS Technologies; The lines represent the three segments of Net1's business as reported in their Annual Reports. "South African transaction processing" and "Financial inclusion and applied technologies" are based in South Africa; while "International transaction processing" is based in South Korea, Hong Kong and the European Union. South African transaction processing consists of the welfare benefit distribution service, ATM infrastructure, and transaction processing for retailers utilities and banks. Financial inclusion and applied technologies consists of short-term loans, bank accounts, prepaid products, life insurance, and the sale of hardware and software.
11: Black Sash. (2016). *Community based monitoring: SASSA paypoints: October 2016-November 2016*. Cape Town: Black Sash. Retrieved from https://cbm.blacksash.org.za/survey-types/sassa-paypoint-citizen.
12: *Poster created by the Black Sash based on a survey conducted by the Social Justice Coalition at a SASSA Pay Point in Khayelitsha between October and November 2016. Over 50% of participants said they had money deducted from their grants without their consent.* Complete survey data available at the Black Sash website: https://cbm.blacksash.org.za/survey-types/sassa-paypoint-citizen.
13: Source link: https://www.groundup.org.za/article/i-cry-every-month-my-money-says-pensioner/
14: International Finance Corporation. (2016). IFC invests in Net1 to promote technology that expands financial services to poor in Africa, April, Washington, DC: World Bank Group. Available at: https://ifcext.ifc.org/IFCExt/Pressroom/IFCPressRoom.nsf/0/D334AA9DF30D017E85257F92006205C5.
15: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
16: Breckenridge, K. (2014). *Biometric state*. Cambridge University Press.
17: Froneman, J. (2013, 29 November). *Allpay Consolidated Investment Holdings (Pty) Ltd and Others v Chief Executive Officer of the South African Social Security Agency and Others.* Johannesburg: Constitutional Court.
18: Torkelson, E. (2017a, March 3). Deductions from social grants. *Ground Up*. Retrieved from https://www.groundup.org.za/article/deductions-social-grants-how-it-works/.
19: *Allpay Consolidated Investment Holdings (Pty) Ltd and Others v Chief Executive Officer of the South African Social Security Agency and Others* (CCT 48/13) [2013] ZACC 42.
20: Emsie Ferreria (1 April 2021), 'ConCourt orders CPS to file all records relating to its illicit profits', *Mail & Guardian*, URL: https://mg.co.za/news/2021-04-01-concourt-orders-cps-to-file-all-records-relating-to-its-illicit-profits/ [Accessed 30 September 2021].
21: Gordhan, P. (2017, March 14). *Presentation to the Standing Committee of Public Accounts: SASSA and related matters*. Cape Town: South African Parliament.
22: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
23: Portfolio Committee for Trade and Industry (2016, 25 November) 'Debt relief measures: Proposals and reports from various stakeholders.' *Parliamentary Monitoring Group*. URL: https://pmg.org.za/committee-meeting/23744/
24: From 18.6 million in 2012 to 57 million in 2013.
25: Keith Breckenridge (2019). The global ambitions of the biometric anti-bank: Net1, lockin, and the technologies of African financialization. *International Review of Applied Economics. 33*(1), 93-118.
26: Keith Breckenridge (2019). The global ambitions of the biometric anti-bank: Net1, lockin, and the technologies of African financialization. *International Review of Applied Economics. 33*(1), 93-118.
27: Interview, Roelof Goosen, Durbanville, 12 May 2017.
28: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
29: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
30: https://www.groundup.org.za/article/deductions-social-grants-how-it-works/
31: McKune, C. (2017, 16 March). Serge Belamant, SASSA, and the war chest of poor people. *Amabungane.* Retrieved from http://amabhungane.co.za/article/2017-03-16-serge-belamant-sassa-and-the-war-chest-of-poor-people
32: Gordhan, P. (2017, March 14). *Presentation to the Standing Committee of Public Accounts: SASSA and related matters*. Cape Town: South African Parliament.

33: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
34: Net1 website. (n.d.). The U.E.P.S. Technology. Retrieved from http://www.net1.com/key-products/the-ueps-technology/.
35: McKune, 2017.
36: McKune, 2017.
37: Hogg, A (2016, 9 August). Net1's Serge Belamant: Business is ugly. Disrupt at your reputational peril. *Biz News*. Retrieved from https://www.biznews.com/entrepreneur/2016/08/09/net1s-serge-belamant-business-is-ugly-disrupt-at-your-reputational-peril
38: The NCR allows interest rates of 5% per month on short-term, unsecured credit (under 6 months), as well as initiation fees up to 15% of the value of the loan, and service fees of R50 per month
39: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.
40: Black Sash. (2016). *Community based monitoring: SASSA paypoints: October 2016-November 2016*. Cape Town: Black Sash. Retrieved from https://cbm.blacksash.org.za/survey-types/sassa-paypoint-citizen.
41: Panel of Experts, *Reports to the Constitutional Court on the SASSA Transition* (Johannesburg, Constitutional Court, 2018).
42: Erin Torkelson (2020). 'Collateral Damages: Cash Transfer and Debt Transfer in South Africa', *World Development*, 126.

GOVCHAT: THE DIGITALISATION OF SOCIAL WELFARE – VERSION 2.0

1: Nerushka Bowan as quoted in conversation with Howard Feldman and Jake Shepherd. See: Howard Feldman (14 January 2021), 'WhatsApp's T&C's and Data Privacy, what's going on?', The Synthesis Podcast, Episode 18, Podcast URL: https://anchor.fm/thesynthesispodcast/episodes/WhatsApp-TCs-and-Data-Privacy--what-is-going-on-ep7erk, minutes: 8:37-12:57.
2: GovChat website, URL: https://www.govchat.org/for-citizens/ [Accessed 27 August 2021].
3: Department of Social Development. 2020. *President Cyril Ramaphosa: Additional Coronavirus COVID-19 economic and social relief measures*. 22 April 2020. Available: https://www.dsd.gov.za/index.php/latest-news/21-latest-news/113-president-cyril-ramaphosa-additional-coronavirus-covid-19-economic-and-social-relief-measures [Accessed, 8 September 2020].
4: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, pp 15-16.
5: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, pp 15-16.
6: Institute for Economic Justice (15 July 2021), 'Economic relief in the face of the third wave', Covid-19 response policy brief #4, URL: https://www.iej.org.za/wp-content/uploads/2021/07/IEJ-COVID-19-policy-brief-series-4-Emergency-relief-package.pdf [Accessed 30 August 2021].
7: Digitalisation can be defined as a process whereby information is converted from a physical format to a digital one. See Maria Petrescu (2008), 'Digitalisation of Cultural Documents' *Philobiblon: Transylvanian Journal of Multidisciplinary Research in Humanities*, vol 13. pp. 547-548.
8: Mircea Georgescu (2012),'EGOVERNMENT: NEW PERSPECTIVES ON THE FUTURE OF GOVERNMENT DIGITALISATION.', *Annales Universitatis Apulensis-Series Oeconomica*, vol 14. Iss. no.2; Vishanth Weerakkody, Vishanth, Irani Zahir , Lee Habin, Osman Ibrahim, and Hindi Nitham Hindi (2015), 'E-government implementation: A bird's eye view of issues relating to costs, opportunities, benefits and risks.', *Information systems frontiers* vol 17, no. 4. pp.889-915.
9: Presidential Commission on the 4th Industrial Revolution (23 October 2020), 'Summary and Recommendations Report', Government Gazette No. 48384, pg 41.
10: Department of Social Development. 2020. *Remarks by the Minister of Social Development, Ms Lindiwe Zulu, on COVID-19 economic and social measures that were announced by President Cyril Ramaphosa. 28 April 2020*. Available: https://www.gov.za/speeches/minister-lindiwe-zulu-coronavirus-covid-19-economic-and-social-measures-29-apr-2020-0000 [Accessed, 8 September 2020].
11: Mambana, D. 2020. New Sassa grants: everything you need to know. 21 May. Drum. Available: https://www-pressreader-com.ezproxy.uct.ac.za/south-africa/drum1/20200521 [Accessed, 8 September 2020].
12: Department of Social Development. 2020. *Statement by Minister Lindiwe Zulu with regards to Social Development Response to Covid 19 for Level 4 Risk Adjusted Approach.* 11 May 2020. Available: https://www.gov.za/speeches/statement-minister-lindiwe-zulu-regards-social-development-response-covid19-level-4-risk [Accessed, 8 September 2020].
13: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 17.
14: Percentage record was taken from Black Sash Report. See: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, pp 17
15: Fifi Peters (11 August 2021), 'Sassa's systems crash due to Covid-19 grant application volumes', *MoneyWeb*, URL: https://www.moneyweb.co.za/moneyweb-radio/safm-market-update/sassas-systems-crash-due-to-volume-of-covid-19-grant-applications/ [Accessed 3 September 2021].
16: Memorandum from Abraham Mahlangu to SASSA CEO Busisiwe Memela, 6 May 2020.
17: Letter from Eldrid Jordaan to Abraham Mahlangu, 4 May 2020.
18: Memorandum from Abraham Mahlangu to SASSA CEO Busisiwe Memela, 6 May 2020.
19: Synthesis Podcast. 2020. GovChat digitalises Sassa. 14 May. Available: https://anchor.fm/thesynthesispodcast/episodes/GovChat-digitalises-Sassa-ee1roa [Accessed, 2 September 2020].
20: Engenas Senona, Erin Torkelson, Wanga Zembe-Mkabile (July 2021), 'Social Protection In a Time of Covid: Lessons for a Basic Income Support', Black Sash, p 16.
21: Abraham Mahlangu, Chief Information Officer of SASSA (6 May 2020), 'Request for Approval to Collaborate with GovChat to Automate Special SRD Application Process using their WhatsApp Line and Technology Platform', South African Social Security Agency, PAIA request Annexure D, page 2, point 3.1-3.2.
22: TBJ Memela-Khambula, Chief Executive Officer of SASSA (8 May 2020), 'GovChat offer to SASSA to use WhatsApp and Unstructured Supplementary Services Data (USSD) Technology platforms for the application, screening and onboarding of Covid-19 Special Social Relief of Distress Applicants', South African Social Security Agency, PAIA request Annexure A, page 2, point 8.
23: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.

24: Gustav Praekelt (2021), Founder of Praekelt.org, LinkedIn Profile, URL: https://www.linkedin.com/in/gustavpraekelt/?originalSubdomain=za [Accessed 29 July 2021].

25: Paul Farlam SC & Luke Kelly Applicant's Counsel, (6 January 2021), 'Applicant's Head's of Argument in matter between: GovChat Propriety Limited (1st Applicant), Hashtag Let'sTalk Propriety Limited (2nd Applicant) & Facebook Inc (1st Respondent), WhatsApp Inc (2nd Respondent) & Facebook Propriety Limited South Africa (3rd Respondent), The Competition Tribunal of South Africa, page 4. The four authorised BSPs in South Africa are InfoBip, Clickatell, Imimobile, and Praekelt. Answering affidavit submitted to Competition tribunal, para 37, p 523.

26: WhatsApp (2021), 'What is a solution provider?', WhatsApp General, URL: https://faq.whatsapp.com/general/whatsapp-business-api/what-is-a-solution-provider/?lang=en

27: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

28: Abraham Mahlangu, Chief Information Officer of SASSA (6 May 2020), 'Request for Approval to Collaborate with GovChat to Automate Special SRD Application Process using their WhatsApp Line and Technology Platform', South African Social Security Agency, PAIA request Annexure D, page 2, point 3.4.

29: Abraham Mahlangu, Chief Information Officer of SASSA (6 May 2020), 'Request for Approval to Collaborate with GovChat to Automate Special SRD Application Process using their WhatsApp Line and Technology Platform', South African Social Security Agency, PAIA request Annexure D.

30: GovChat About Page (2021), 'Co-created with Government', URL: https://www.govchat.org/about/

31: Joanne Carew, (10 August 2020), GovChat CEO: COVID Shows 'Desperate Need' To Digitise Gov't Services, *CIO*, URL: https://www.cio.co.ke/govchat-ceo-covid-shows-desperate-need-to-digitise-govt-services/

32: Simnikiwe Mzekandaba, (15 May 2020), Citizens turn to GovChat to find COVID-19 resources, *ITWeb*, URL: https://www.itweb.co.za/content/rxP3jqBmyNPMA2ye

33: Absa contributes initial R15,7m towards COVID-19 effort, 30 March 2020, *ABSAGroup Media Release*, URL: https://www.absa.africa/media-centre/media-statements/2020/absa-contribution-for-covid-19/

34: Eldrid Jordaan LinkedIn Profile, URL: https://www.linkedin.com/in/eldrid-jordaan-a0839117/?originalSubdomain=za [Accessed 8 September 2020].

35: Dates taken from Eldrid Jordaan's LinkedIn Profile, URL: https://www.linkedin.com/in/eldrid-jordaan-a0839117/?originalSubdomain=za [Accessed 8 September 2020].

36: Eldrid Jordaan interview (15 October 2018), *Die Groot Ontbyt,* URL: https://www.youtube.com/watch?v=tZ9Nz1FvziU&feature=youtu.be

37: Eldrid Jordaan interview (15 October 2018), *Die Groot Ontbyt,* URL: https://www.youtube.com/watch?v=tZ9Nz1FvziU&feature=youtu.be

38: Department of International Relations and Cooperation (26 July 2018), Ubuntu News Flash Weekly Newsletter, Issue 338, URL: http://www.dirco.gov.za/dircoenewsletter/newsflash338-26-07-2018.html [Accessed 9 September 2020].

39: Available online at https://ogpsummit2018.sched.com/eldridjordaan [Accessed 9 September 2020].

40: Goitse Konopi (4 May 2020), 'SA's own government engagement platform heads to the AU', GovChat Press release. *Cape Argus,* URL: https://www.iol.co.za/capeargus/opinion/sas-own-government-engagement-platform-heads-to-au-14781539 [Accessed 9 September 2020].

41: Daniel Mpala, 28 May 2019, SA startup GovChat announces it's secured investment facility of up to R20m, Ventureburn, URL: https://ventureburn.com/2019/05/govchat-r20m-capital-appreciation/

42: Sello Moloi, 16 November 2018, 'South African civic technology platform expands to Ghana', *iAfrikan*, URL: https://www.iafrikan.com/2018/11/16/govchat-ghana-civic-technology-eldrid-jordaan/ [Accessed 1 October 2020].

43: Today with Kieno Kammies, (29 September 2020), *Cape Talk,* URL: https://omny.fm/shows/the-kieno-kammies-show/govchat-org

44: Quote taken from Interview Eldrid Jordan held with Open Secrets Investigators (14 June 2021)

45: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

46: GovChat about page (2021). URL: https://www.govchat.org/about/

47: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ [Accessed 6 September 2020].

48: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ [Accessed 6 September 2020].

49: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ {Accessed 6 September 2020].

50: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ {Accessed 6 September 2020].

51: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ [Accessed 6 September 2020].

52: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ {Accessed 6 September 2020].

53: Eldrid Jordaan interview (15 October 2018), *Die Groot Ontbyt,* URL: https://www.youtube.com/watch?v=tZ9Nz1FvziU&feature=youtu.be

54: GovChat about page (2021). URL: https://www.govchat.org/about/

55: Eldrid Jordaan interview (15 October 2018), *Die Groot Ontbyt,* URL: https://www.youtube.com/watch?v=tZ9Nz1FvziU&feature=youtu.be

56: GovChat CEO address at the launch of the GovChat HQ, Parliament Street, Cape Town, (2 January 2020), URL: https://www.youtube.com/watch?v=cIwdRvQX308

57: The new premises were provided by Capital Appreciation and were talked up by Jordaan when he appeared on the Synthesis podcast.

58: GovChat CEO address at the launch of the GovChat HQ, Parliament Street, Cape Town, (2 January 2020), URL: https://www.youtube.com/watch?v=cIwdRvQX308

59: AfroCentric Investment Corporation Limited (AfroCentric), Integrated Annual Report, (2016), URL:https://www.afrocentric-online.co.za/reports/afrocentric-ar2016/pdf/full.pdf and AfroCentric Investment Corporation Limited (AfroCentric), Integrated Annual Report, (2012).URL: http://www.afrocentric.za.com/pdf/annual-reports/ar-2012.pdf

60: See the company profile here: https://www.afrocentric-online.co.za/au-profile.php [Accessed 14 September 2020].

61: AfroCentric Investment Corporation Limited (AfroCentric), Integrated Annual Report, (2016), URL:https://www.afrocentric-online.co.za/reports/afrocentric-ar2016/pdf/full.pdf

62: Sikhumbuzo Hlabangane, (8 November 2016), Patrice Motsepe's Plan to Reform Private Healthcare, *eHealth News,* URL: https://ehealthnews.co.za/patrice-motsepe-private-healthcare/

63: Capital Appreciation Press Statement (28 September 2015), 'Capital appreciation to list on the JSE main board'.

64: Simnikiwe Mzekandaba (31 May 2019) 'R20 million funding injection for GovChat' , *ITWeb,* URL: https://www.itweb.co.za/content/LPp6V7r4wlOqDKQz [Accessed 8 September 2020].

65: Capital Appreciation Website, 'History', URL: https://capitalappreciation.co.za/about/directors [Accessed 16 October 2020].

66: Khaya Sithole (11 May 2020), 'A revival of the CPS-SASSA sage?', *Embonews*, URL: http://embonews.com/a-revival-of-the-cps-sassa-saga-by-khaya-sithole/ [Accessed 9 September 2020].

67: African Resonance website, URL: http://www.africanresonance.com/ [Accessed 19 October 2020].

68: Capital Appreciation Website, 'Our Portfolio', URL: https://capitalappreciation.co.za/portfolio/overview [Accessed 19 October 2020].

69: Staff Writer (7 June 2019), 'GovChat appoints board chairman', *ITWeb,* URL: https://www.itweb.co.za/content/Olx4zMkgYaYM56km [Accessed 9 September].

70: CIPC records for GovChat, accessed on 1 September 2020.

71: GovChat Website, 'Meet the Team', URL: http://www.govchat.org/ [Accessed 9 September 2020].

72: Capital Appreciation Limited (2020), Integrated Annual Report 2020, p 140.

73: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

74: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

75: Khaya Sithole (11 May 2020), 'A revival of the CPS-SASSA sage?', *Embonews*, URL: http://embonews.com/a-revival-of-the-cps-sassa-saga-by-khaya-sithole/ [Accessed 9 September 2020].

76: Khaya Sithole (11 May 2020), 'A revival of the CPS-SASSA sage?', *Embonews*, URL: http://embonews.com/a-revival-of-the-cps-sassa-saga-by-khaya-sithole/ [Accessed 9 September 2020].

77: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

78: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

79: Khaya Sithole (11 May 2020), 'A revival of the CPS-SASSA sage?', *Embonews*, URL: http://embonews.com/a-revival-of-the-cps-sassa-saga-by-khaya-sithole/ [Accessed 9 September 2020].

80: Khaya Sithole (11 May 2020), 'A revival of the CPS-SASSA sage?', *Embonews*, URL: http://embonews.com/a-revival-of-the-cps-sassa-saga-by-khaya-sithole/ [Accessed 9 September 2020].

81: Khaya Sithole (11 May 2020), 'A revival of the CPS-SASSA sage?', *Embonews*, URL: http://embonews.com/a-revival-of-the-cps-sassa-saga-by-khaya-sithole/ [Accessed 9 September 2020].

82: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

83: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

84: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

85: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

86: Joanne Carrew (30 July 2020), 'GovChat CEO: Covid shows "desperate need" to digitize government services', *CIO.*

87: Today with Kieno Kammies (29 September 2020), *Cape Talk,* URL: https://omny.fm/shows/the-kieno-kammies-show/govchat-org

88: Today with Kieno Kammies (29 September 2020), *Cape Talk,* URL: https://omny.fm/shows/the-kieno-kammies-show/govchat-org

89: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

90: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

91: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

92: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021).

93: Londiwe Buthelezi and Khulekani Magubane (17 May 2020), 'Former Net1-bigwigs linked with SASSA deal', *News24,* URL: https://www.news24.com/fin24/companies/ict/former-net-1-bigwigs-linked-with-sassa-deal-20200517-2 [Accessed 9 September 2020].

94: Capital Appreciation, Full Year Results for the period ended 31 March 2019.

95: Capital Appreciation Media Release (18 November 2019), 'Capital Appreciation demonstrates good momentum, period cut-offs impacts revenues', URL: https://capitalappreciation.co.za/content/1574055120-media-release-capprec-interim-results-for-the-six-months-ended-30-september-2019.pdf [Accessed 9 September 2020].

96: Capital Appreciation Limited (2020), Integrated Annual Report 2020.

97: Capital Appreciation Limited (2020), Integrated Annual Report 2020.

98: Capital Appreciation Limited (2020), Integrated Annual Report 2020.

99: Mudiwe Gavaza (2 June 2020), 'Capital Appreciation sees growth from GovChat adaptations for Covid-19', *Business Day,* URL: https://www.businesslive.co.za/bd/companies/telecoms-and-technology/2020-06-02-capital-appreciation-sees-growth-from-govchat-adaptations-for-covid-19/ [Accessed 20 October 2020].

100: Simnikiwe Mzekandaba (31 May 2019) 'R20 million funding injection for GovChat' , *ITWeb,* URL: https://www.itweb.co.za/content/LPp6V7r4wlOqDKQz [Accessed 8 September 2020].

101: Synthesis Podcast. 2020. GovChat digitalises Sassa. 14 May. Available: https://anchor.fm/thesynthesispodcast/episodes/GovChat-digitalises-Sassa-ee1roa [Accessed, 2 September 2020].

102: Eldrid Jordaan Interview with Open Secrets (14 June 2021).

103: Eldrid Jordaan Interview with Open Secrets (14 June 2021).

104: Eldrid Jordaan Interview with Open Secrets Investigators (14 June 2021)

105: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 820.

106: SASSA Strategic Plan 2020-2025. Available: https://static.pmg.org.za/SASSA_STRATEGIC_PLAN_2020-2025.pdf [Accessed, 9 September 2020]

107: SASSA Strategic Plan 2020-2025. Available: https://static.pmg.org.za/SASSA_STRATEGIC_PLAN_2020-2025.pdf [Accessed, 9 September 2020]

108: Ling Sheperd (28 September 2020), 'SASSA pilot goes digital with online grant applications pilot system', *Daily Vox,* Available: https://www.thedailyvox.co.za/sassa-goes-digital-with-online-grant-applications-pilot-system/ [Accessed 15 October 2020].

109: https://services.sassa.gov.za/

110: Ling Sheperd (28 September 2020), 'SASSA pilot goes digital with online grant applications pilot system', *Daily Vox,* Available: https://www.thedailyvox.co.za/sassa-goes-digital-with-online-grant-applications-pilot-system/ [Accessed 15 October 2020].
111: Siminikiwe Mzekandaba (29 April 2021), 'SASSA adds online feature with the disability grant process', ITWeb, URL: https://www.itweb.co.za/content/OIx4zMknkmG756km
112: Siminikiwe Mzekandaba (29 April 2021), 'SASSA adds online feature with the disability grant process', ITWeb, URL: https://www.itweb.co.za/content/OIx4zMknkmG756km
113: Siminikiwe Mzekandaba (29 September 2020), 'GovChat ready to assist SASSA where needed', ITWeb, URL: https://www.itweb.co.za/content/mYZRXv9aEJavOgA8, [Accessed 6 September 2021]
114: Eldrid Jordaan Interview with Open Secrets Investigators (20 October 2021).
115: The current upper bound poverty line.
116: See more on the campaign here: http://blacksash.org.za/index.php/sash-in-action/advocacy-in-partnership/basic-income-support
117: Duncan Mcleod (12 January 2021), 'GovChat heads to tribunal over WhatsApp de-platforming threat', *TechCentral*, URL: https://techcentral.co.za/govchat-heads-to-tribunal-over-whatsapp-de-platforming-threat/104134/
118: Competition Tribunal South Africa (13 January 2021), 'January 2021: Current and Upcoming Hearings', URL: https://www.comptrib.co.za/hearings
119: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.
120: Gavaza Mudiwa (14 January 2021), 'GovChat accuses WhatsApp owner', Business Day; Dineo Faku (13 January 2021), 'GovChat asks Tribunal to stop its removal from WhatsApp platform', Cape Times.
121: Jerome Wilson SC and Johnathan Berger, Counsel for the respondents, (6 January 2021), 'Respondents Head's of Argument in matter between: GovChat Propriety Limited (1st Applicant), Hashtag Let'sTalk Propriety Limited (2nd Applicant) & Facebook Inc (1st Respondent) and WhatsApp Inc (2nd Respondent), The Competition Tribunal of South Africa, page 4 point 3.2.
122: Paul Farlam SC & Luke Kelly Applicant's Counsel, (6 January 2021), 'Applicant's Head's of Argument in matter between: GovChat Propriety Limited (1st Applicant), Hashtag Let'sTalk Propriety Limited (2nd Applicant) & Facebook Inc (1st Respondent), WhatsApp Inc (2nd Respondent) & Facebook Propriety Limited South Africa (3rd Respondent), The Competition Tribunal of South Africa, page 9 point 12.
123: Paul Farlam SC & Luke Kelly Applicant's Counsel, (6 January 2021), 'Applicant's Head's of Argument in matter between: GovChat Propriety Limited (1st Applicant), Hashtag Let'sTalk Propriety Limited (2nd Applicant) & Facebook Inc (1st Respondent), WhatsApp Inc (2nd Respondent) & Facebook Propriety Limited South Africa (3rd Respondent), The Competition Tribunal of South Africa, page 45-46 point 67-68.
124: The dispute also revealed that Praekelt- the same company that initially aided SASSA in their WhatsApp process for the SRD grant- also initially aided GovChat with onboarding its platform on to WhatsApp. However, GovChat's own contract with Praekelt fell through due to GovChat's consistent issues with WhatsApp and concern over the quality of the chatbot technology Praekelt were asked to develop.
125: The order entails that: During the interim period, Facebook and WhatsApp shall not offboard the WhatsApp Business Account GovChat established in #LetsTalk's name. Facebook and WhatsApp are prohibited from undermining directly or indirectly, GovChat and #LetsTalk's relationships with their clients for the purpose of trying to offboard #LetsTalks WABA GovChat and #LetsTalk shall not on-board any new clients to the WABA and regarding current clients, they may not launch, adopt or sell any new-use cases.
126: Yassim Carrim, Andreas Wessels & Imraan Valodia (21 January 2021), 'Order of Interim Arrangement: Case no. IR165Nov20', Competition Tribunal.
127: Yassim Carrim, Andreas Wessels & Imraan Valodia (11 March 2021), 'Reasons for Decision and Order: Case no. IR165Nov20',The Competition Tribunal of South Africa, p 19, pt 77.1
128: Yassim Carrim, Andreas Wessels & Imraan Valodia (11 March 2021), 'Reasons for Decision and Order: Case no. IR165Nov20',The Competition Tribunal of South Africa, p 19, pt 77.3
129: Yassim Carrim, Andreas Wessels & Imraan Valodia (11 March 2021), 'Reasons for Decision and Order: Case no. IR165Nov20',The Competition Tribunal of South Africa, p 36, pt 170.
130: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.
131: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.
132: Staff Writer (1 July 2021), 'The biggest and most popular social media platforms in South Africa inclusing TikTok', *Business Tech*, URL: https://businesstech.co.za/news/internet/502583/the-biggest-and-most-popular-social-media-platforms-in-south-africa-including-tiktok/ [Accessed 7 October 2021].
133: Adam Satariano (2 September 2021), 'Facebook's Whatsapp is fined for breaking the E.U's data privacy law', *New York Times*, URL: https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html [Accessed 29 September 2021].
134: DB Nieborg and A Helmond, The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance, *Media, Culture & Society*. 2019;41(2):196-218.
135: Shoshana Zuboff (29 January 2021), 'The coup we are not talking about', *New York Times*, URL: https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html [Accessed 7 October 2021].
136: Shoshana Zuboff (29 January 2021), 'The coup we are not talking about', *New York Times*, URL: https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html [Accessed 7 October 2021].
137: Bobby Allyn (5 October 2021), 'Here are four key points from the Facebook whistleblower's testimony on Capitol Hill', *NPR*, URL: https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress, [Accessed 7 October 2021].
138: Bobby Allyn (5 October 2021), 'Here are four key points from the Facebook whistleblower's testimony on Capitol Hill', *NPR*, https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress, [Accessed 7 October 2021].
139: Lauren Feiner (2 January 2021), 'Facebook spent more on lobbying than any other Big Tech company in 2020', *CNBC*, URL: https://www.cnbc.com/2021/01/22/facebook-spent-more-on-lobbying-than-any-other-big-tech-company-in-2020.html [Accessed 7 October 2021].

AADHAAR: LESSONS FROM INDIA FOR SOUTH AFRICA'S DIGITAL FUTURE

1: ITWeb Staff Writer (31 August 2021), 'GovChat accessed by over 8 million users', *ITWeb*, URL: https://www.itweb.co.za/content/WnxpEv4gjWWqV8XL [Accessed 9 September 2021].
2: ITWeb Staff Writer (31 August 2021), 'GovChat accessed by over 8 million users', *ITWeb*, URL: https://www.itweb.co.za/content/WnxpEv4gjWWqV8XL [Accessed 9 September 2021].

3: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.

4: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 819.

5: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 819.

6: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021] p. 6.

7: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021] p. 6.

8: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 818.

9: Privacy International (May 2019), 'Submission on digital technology, social protection and human rights' *Submission to UN Special Rapporteur on extreme poverty and human rights*, p. 2. Available for download at: https://www.ohchr.org/EN/Issues/Poverty/Pages/DigitalTechnology.aspx.

10: Ian Parker (26 September 2011), 'The I.D Man: Can a software mogul's epic project help India's poor?', *The New Yorker*, URL: https://www.newyorker.com/magazine/2011/10/03/the-i-d-man [Accessed 01 July 2021].

11: Ian Parker (26 September 2011), 'The I.D Man: Can a software mogul's epic project help India's poor?', *The New Yorker*, URL: https://www.newyorker.com/magazine/2011/10/03/the-i-d-man [Accessed 01 July 2021].

12: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021] p. 6.

13: Krishn Kaushik (5 October 2017), 'Aadhaar officials part of private firms that use Aadhaar services for profit', *Indian Express*, URL: https://indianexpress.com/article/india/aadhaar-officials-part-of-private-firms-that-use-aadhaar-services-for-profit-4874824/ [Accessed 08 July 2021].

14: Aria Thakar (01 May 2018), 'The New Oil: Aadhaar's mixing of public risk and private profit', *The Caravan*, URL: https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit [Accessed 08 July 2021].

15: Usha Ramanathan interview with Holly Ritson (15 February 2021), 'Putting Profit before Welfare: A Closer Look at India's Digital Identification System', *Center for Human Rights and Global Justice*, New York University, URL: https://chrgj.org/2021/02/15/putting-profit-before-welfare-criticisms-of-indias-digital-identification-system/ [Accessed 08 July 2021].

16: Sudeep Jain and Daniela Gabor (2020), 'The Rise of Digital Financialisation: The Case of India', *New Political Economy*, 25:5, 818.

17: Electronic Frontier Foundation (25 October 2019), 'Street-level surveillance: Iris recognition', *Electronic Frontier Foundation*, URL: https://www.eff.org/pages/iris-recognition [Accessed 02 July 2021].

18: Rahul Batia (13 February 2018), 'Critics of India's ID card project say they have been harassed, put under surveillance', *Reuters*, URL: https://www.reuters.com/article/us-india-aadhaar-breach/critics-of-indias-id-card-project-say-they-have-been-harassed-put-under-surveillance-idUSKBN1FX0H0 [Accessed 01 July 2021].

19: Rahul Batia (13 February 2018), 'Critics of India's ID card project say they have been harassed, put under surveillance', *Reuters*, URL: https://www.reuters.com/article/us-india-aadhaar-breach/critics-of-indias-id-card-project-say-they-have-been-harassed-put-under-surveillance-idUSKBN1FX0H0 [Accessed 01 July 2021].

20: Rahul Batia (13 February 2018), 'Critics of India's ID card project say they have been harassed, put under surveillance', *Reuters*, URL: https://www.reuters.com/article/us-india-aadhaar-breach/critics-of-indias-id-card-project-say-they-have-been-harassed-put-under-surveillance-idUSKBN1FX0H0 [Accessed 01 July 2021].

21: Electronic Frontier Foundation (25 October 2019), 'Street-level surveillance: Iris recognition', *Electronic Frontier Foundation*, URL: https://www.eff.org/pages/iris-recognition [Accessed 02 July 2021].

22: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021] p. 6.

23: Vindu Goel (26 September 2018), 'India's Top Court Limits Sweep of Biometric ID System', *New York Times*, URL: https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html [Accessed 05 July 2021].

24: John Freeman (17 June 2020), 'The great danger: A conversation with Arundhati Roy: Part II', *ZYZZYVA*, URL: https://www.zyzzyva.org/2020/06/17/the-great-danger-a-conversation-with-arundhati-roy-part-ii/ [Accessed 7 October 2021].

25: Reetika Khera (9 August 2018), 'These digital IDs have cost people their privacy – and their lives', *The Washington Post*, URL: https://www.washingtonpost.com/news/theworld-post/wp/2018/08/09/aadhaar/ [Accessed 05 July 2021].

26: Reetika Khera (9 August 2018), 'These digital IDs have cost people their privacy – and their lives', *The Washington Post*, URL: https://www.washingtonpost.com/news/theworld-post/wp/2018/08/09/aadhaar/ [Accessed 05 July 2021].

27: Child Poverty Action Group (2020), 'Computer says no! Access to justice and digitalisation in universal credit', *Child Poverty Action Group*, URL: https://cpag.org.uk/policy-and-campaigns/computer-says-no-access-justice-and-digitalisation-universal-credit [Accessed 05 July 2021].

28: Yeshimabeit Milner and Amy Traub (2021), 'Data capitalism and algorithmic racism', *Data for Black Lives and Demos*, https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf [Accessed 05 July 2021], p. 16.

29: Yeshimabeit Milner and Amy Traub (2021), 'Data capitalism and algorithmic racism', *Data for Black Lives and Demos*, https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf [Accessed 05 July 2021], p. 16.

30: Yeshimabeit Milner and Amy Traub (2021), 'Data capitalism and algorithmic racism', *Data for Black Lives and Demos*, https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf [Accessed 05 July 2021], p. 16.

31: Tebogo Sibidla (September 2019), 'South Africa: the use of biometric information', Data Guidance, URL: https://www.dataguidance.com/opinion/south-africa-use-biometric-information [Accessed 12 September 2021].

32: Kim Harrisberg (8 January 2021), 'Plan to record all babies' biometric raises privacy fears', *News24*, URL: https://www.news24.com/news24/SouthAfrica/News/plan-to-record-all-babies-biometrics-raises-privacy-fears-20210108 [Accessed 12 September 2021].

33: Kim Harrisberg (8 January 2021), 'Plan to record all babies' biometric raises privacy fears', *News24*, URL: https://www.news24.com/news24/SouthAfrica/News/plan-to-record-all-babies-biometrics-raises-privacy-fears-20210108 [Accessed 12 September 2021].

34: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 6.

35: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 6.

36: Paul Plantinga, Rachel Adams and Saahier Parker (2019), 'AI Technologies for Responsive Local Government in South Africa', in *Artificial Intelligence: Human rights, social justice and development*, Global Information Society Watch 2019, p 217.

37: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.

38: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021], p 10.

39: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 6.

40: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 7.

41: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 22.

42: Engenas Senona, Dr. Erin Torkelson and Dr. Wanga Zembe-Mkabile (July 2021), 'Social Protection in a Time of Covid-19: Lessons for Basic Income Support', Report Commissioned by Black Sash, URL: http://blacksash.org.za/images/0541_BS_-_Social_Protection_in_a_Time_of_Covid_Final_-_Web.pdf, p 22.

43: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.

44: Special Rapporteur on extreme poverty and human rights (2019), *Report to the United Nations General Assembly*, 11 October 2019, A/74/48037, URL: https://undocs.org/pdf?symbol=en/A/74/493 [Accessed 25 June 2021], p 18.

45: Section 71(3)(b) of the Protection of Personal Information Act 4 of 2013.

46: 46 Paul Plantinga, Rachel Adams and Saahier Parker (2019), 'AI Technologies for Responsive Local Government in South Africa', in *Artificial Intelligence: Human rights, social justice and development*, Global Information Society Watch 2019, p 218.

47: CK Prahalad (2004) *The fortune at the bottom of the pyramid,* (First. ed.) (Wharton School Publishing).

48: Presidential Commission on the 4th Industrial Revolution (23 October 2020), 'Summary and Recommendations Report', Government Gazette No. 48384, p 18.

49: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.

50: Eldrid Jordaan (2021). Interview with Open Secrets Investigators.

51: GovChat Privacy Policy (2 February 2021), Documents provided through COGTA PAIA Request p 3-6.

52: Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* 10, 3069 (2019).

53: Alex Hern (1 August 2017), 'Anonymous' browsing data can be easily exposed, researchers reveal' *The Guardian*, URL: https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers [Accessed 10 September 2021].

54: Wolfie Christl and Sarah Spiekermann (2016), 'Networks of Control: a report on corporate surveillance, digital tracking, big data, and privacy', (Facultas, Wien) URL: https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf [Accessed 10 September 2021].

55: Chenai Chair (July 2021), 'Does data protection safeguard against risks in Southern Africa?', published by Heinrich-Böll-Stiftung, p 6.

56: Chenai Chair (July 2021), 'Does data protection safeguard against risks in Southern Africa?', published by Heinrich-Böll-Stiftung, p 8.

57: Republic of South Africa (26 Novemeber 2013),'Personal Protection Information Act (2013)', Government Gazette, Vol. 581, no 37067.

58: Protection of Personal Information Act, 2013 Act 4 of 2013.

59: Philip de Wet (5 April 2021), 'SA's info regulator is activating long dormant powers – ahead of a possible Facebook fight', *Business Insider*, URL: https://www.businessinsider.co.za/the-information-regulator-is-activating-popia-powers-that-could-block-facebooks-whatsapp-plans-for-south-africans-2021-4 [Accessed 12 September 2021].

60: GovChat Privacy Policy (2 February 2021), Documents provided through COGTA PAIA Request. Pg 3-6.

61: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ [Accessed 6 September 2020].

62: Phillip De Wet, (30 March 2017), GovChat site for sale – but there are some strings attached, *Mail & Gaurdian*, Available: https://mg.co.za/article/2017-03-30-00-govchat-site-for-sale-but-there-are-some-strings-attached/ {Accessed 6 September 2020].

63: Heidi Swart (25 September 2021), 'Vumacam's "hundreds of thousands of cameras" will be watching you', *Daily Maverick*, URL: https://www.dailymaverick.co.za/article/2021-09-25-vumacams-hundreds-of-thousands-of-cameras-will-be-watching-you/ [Accessed 30 September 2021].

64: Privacy International (2021), 'Data and Elections', URL: https://privacyinternational.org/learn/data-and-elections [Accessed 30 September 2021].

65: Privacy International (2021), 'Data and Elections', URL: https://privacyinternational.org/learn/data-and-elections [Accessed 30 September 2021].

66: Bruna Martins dos Santos and Joana Varon (2018), "Analysis of the playing field for the influence industry in preparation for the Brazilian general elections" Research by *Coding Rights for Tactical Technology Collective*, published as country report of the project 'Personal Data and Political Influence', URL: https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-data-and-politics-brazil.pdf [Accessed 30 September 2021].

67: Bruna Martins dos Santos and Joana Varon (2018), "Analysis of the playing field for the influence industry in preparation for the Brazilian general elections" Research by *Coding Rights for Tactical Technology Collective*, published as country report of the project 'Personal Data and Political Influence', URL: https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-data-and-politics-brazil.pdf [Accessed 30 September 2021].

68: Eleonora Nestola (6 March 2019), 'Why it's too easy to manipulate voters – and steal the EU elections', *The Guardian*, URL: https://www.theguardian.com/commentisfree/2019/mar/06/digital-manipulation-eu-elections-personal-information [Accessed 30 September 2021].

RECOMMENDATIONS AND CONCLUSION

1: INKOTA-netzwerk (January 2019), 'The power of corporations in a digital world', Translated by Oxfam, URL: https://www.oxfam.de/system/files/diskussionspapier-konzern-macht-in-der-digitalen-welt.pdf [Accessed 12 September 2021], p 13.

2: INKOTA-netzwerk (January 2019), 'The power of corporations in a digital world', Translated by Oxfam, URL: https://www.oxfam.de/system/files/diskussionspapier-konzern-macht-in-der-digitalen-welt.pdf [Accessed 12 September 2021], p 13.

3: In their report on the nature of the digital welfare state and how it could be managed, Digital Freedom Fund laid out a visual map of the data processing system for social welfare applicants, that involve crucial steps in need of sound data security mechanisms. See the visualisation here: https://digitalfreedomfund.org/wp-content/uploads/2020/04/20200204-DFF-Digital-Welfare-State-Visualisation_FINAL.pdf; Nani Jansen Reventlow (10 February 2020), 'Tackling the Human Rights Impact of the "Digital Welfare State" ', Digital Freedom Fund Blog, URL: https://digitalfreedomfund.org/tackling-the-human-rights-impacts-of-the-digital-welfare-state/

4: Competition Commission South Africa (7 September 2020), 'Competition n the Digital Economy', URL: http://www.compcom.co.za/wp-content/uploads/2020/09/Competition-in-the-digital-economy_7-September-2020.pdf, pp 46-59.

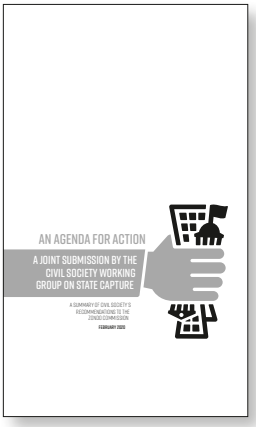
5: SASSA (2020-2025), '2020-2025 Strategic Plan', URL: https://static.pmg.org.za/SASSA_STRATEGIC_PLAN_2020-2025.pdf, pp 28- 32.

6: In their report in analysing the need for a Basic Income Grant, Black Sash, detailed the difficulties grantees encountered when trying to access the new digital platforms used during the Covid-19 Pandemic. Some of which include the lack of digital literacy, no access to airtime, data or good Internet connectivity. However, their analysis also showed that the digital platforms did provide positives which included grantees and applicants finding it easier to apply through these portals. See: Engenas Senona, Erin Torkelson and Wanga Zembe-Mkabile (2021), 'Social Protection in a time of Covid: Lessons for a Basic Income Support', Black Sash, URL: https://www.samrc.ac.za/sites/default/files/files/2021-07-28/SocialProtection%20in%20a%20Time%20of%20Covid.pdf, pp18-20.

OUR PUBLICATIONS

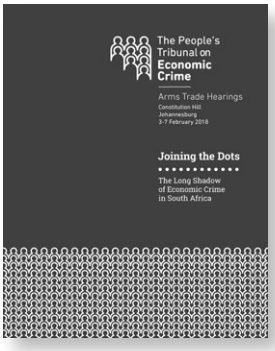
Most of our publications are available for free download on our website. Just visit: www.opensecrets.org.za/publications

OUR REPORTS:



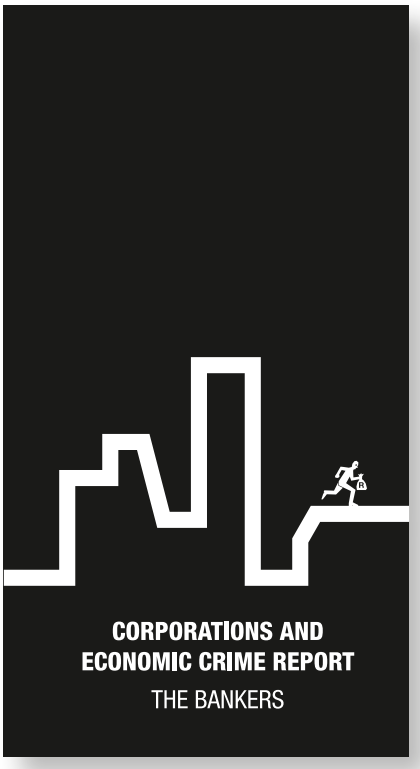
JOINT SUBMISSION TO THE ZONDO COMMISSION:
AN AGENDA FOR ACTION

This Agenda for Action is based on detailed submissions made to the Zondo Commission by organisations of the Civil Society Working Group on State Capture (CSWG) covering the widespread impact of state capture on lives of people in South Africa. Open Secrets acts as the secretariat of the CSWG. Editors: Naushina Rahim, Zen Mathe and Hennie van Vuuren.



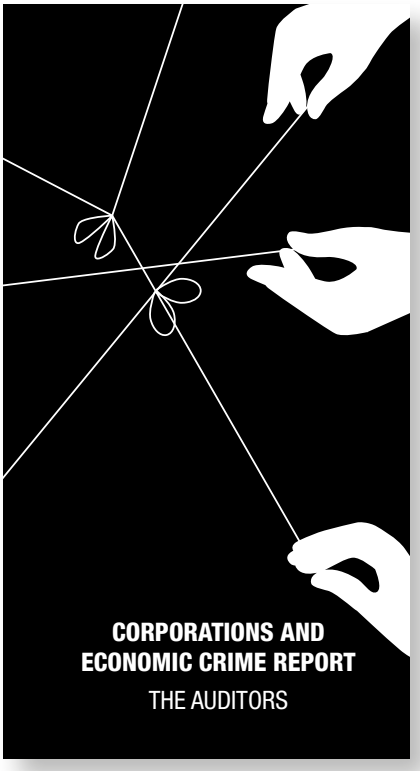
JOINING THE DOTS:
THE LONG SHADOW OF ECONOMIC CRIME IN SOUTH AFRICA

Prepared for the first People's Tribunal on Economic Crime, this report examined continuities in economic crime and corruption in South Africa related to the arms trade, from apartheid to contemporary state capture. In doing so it highlighted the powerful deep state networks that have facilitated these crimes.



CORPORATIONS AND ECONOMIC CRIME REPORT
VOLUME 1: THE BANKERS

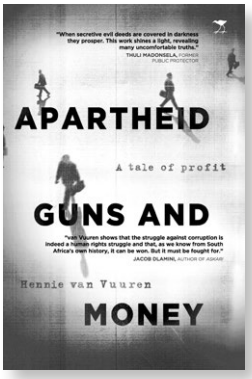
The Corporations and Economic Crime Reports (CECR) explores the most egregious cases of economic crimes and corruption by private financial institutions, from apartheid to the present day. In doing so, we aim to highlight the key themes that link corporate criminality across these periods of time, focusing on the role of the private sector, a critical blind spot in the discourse around economic crime. This first volume of the series focuses on the role of banks and other financial sector actors in corporate criminality.



CORPORATIONS AND ECONOMIC CRIME REPORT
VOLUME 2: THE AUDITORS

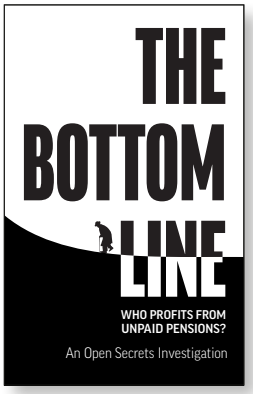
This second volume in our Corporations and Economic Crime Reports (CECR) series focusses on the big four auditing firms- PWC, KPMG, Deloitte and EY and their role in some of the most egregious examples of economic crime

OUR INVESTIGATIONS:



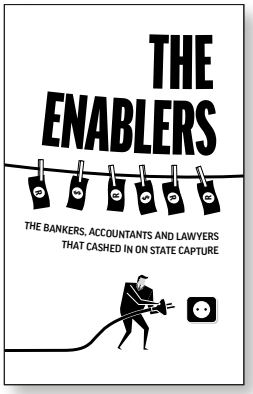
APARTHEID GUNS AND MONEY:
A TALE OF PROFIT

Published in 2017, this exposé drew on extensive archival research and interviews to reveal the global covert network of corporations, spies, banks and politicians in nearly 50 countries that operated in secret to counter sanctions against the apartheid regime, and profit in return.



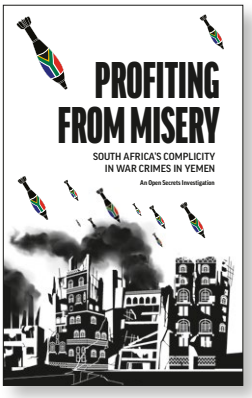
THE BOTTOM LINE :
WHO PROFITS FROM UNPAID PENSIONS?

This investigative report is the culmination of a year-long investigation by Open Secrets into role of corporations in the erroneous cancellation of pension funds between 2007-2013. The Bottom Line focusses on the role played by the big corporations who administer these funds, such as Liberty Corporate and Alexander Forbes. The report also looks into the role of the regulator in creating an enabling environment for the 'Cancellations Project'.



THE ENABLERS:
THE BANKERS, ACCOUNTANTS AND LAWYERS THAT CASHED IN ON STATE CAPTURE

This investigative report focuses on the role of banks, accounting firms, consultants and lawyers in facilitating criminal conduct that formed part of the state capture enterprise. The report shows that the systems that enable grand corruption and state capture are global in nature, and that private sector elites are central to the problem. It is intended to provide the evidence and analysis to assist Justice Zondo and the State Capture Inquiry with this pressing task in 2020.



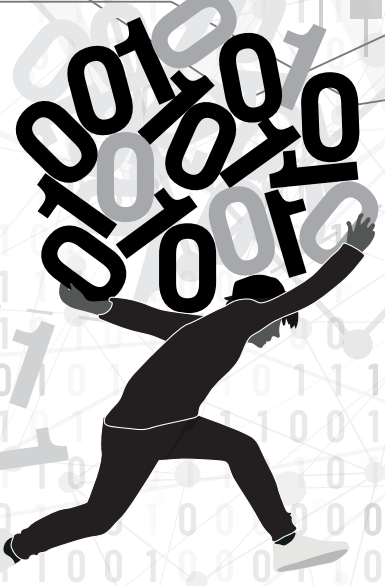
PROFITING FROM MISERY:
SOUTH AFRICA'S COMPLICITY IN WAR CRIMES IN YEMEN

This investigative report reveals the South African arms companies that have cashed in on the sale of weapons to Saudi Arabia and the United Arab Emirates (UAE), two central parties to the Yemeni conflict.

SUPPORT OPEN SECRETS

We are building a community that actively supports our work through small financial donations and pro-bono work. We investigate difficult issues, treading where it is hard to go, and challenge powerful banks, arms companies, and regulators who operate with impunity. We do so fearlessly and do not accept funds from governments and corporations, which ensures our independence. Your support means we can do more work to challenge the powerful.

JOIN US ON THIS JOURNEY, SHOW YOUR SOLIDARITY, SUPPORT OPEN SECRETS



open secrets

power & profit | truth & justice