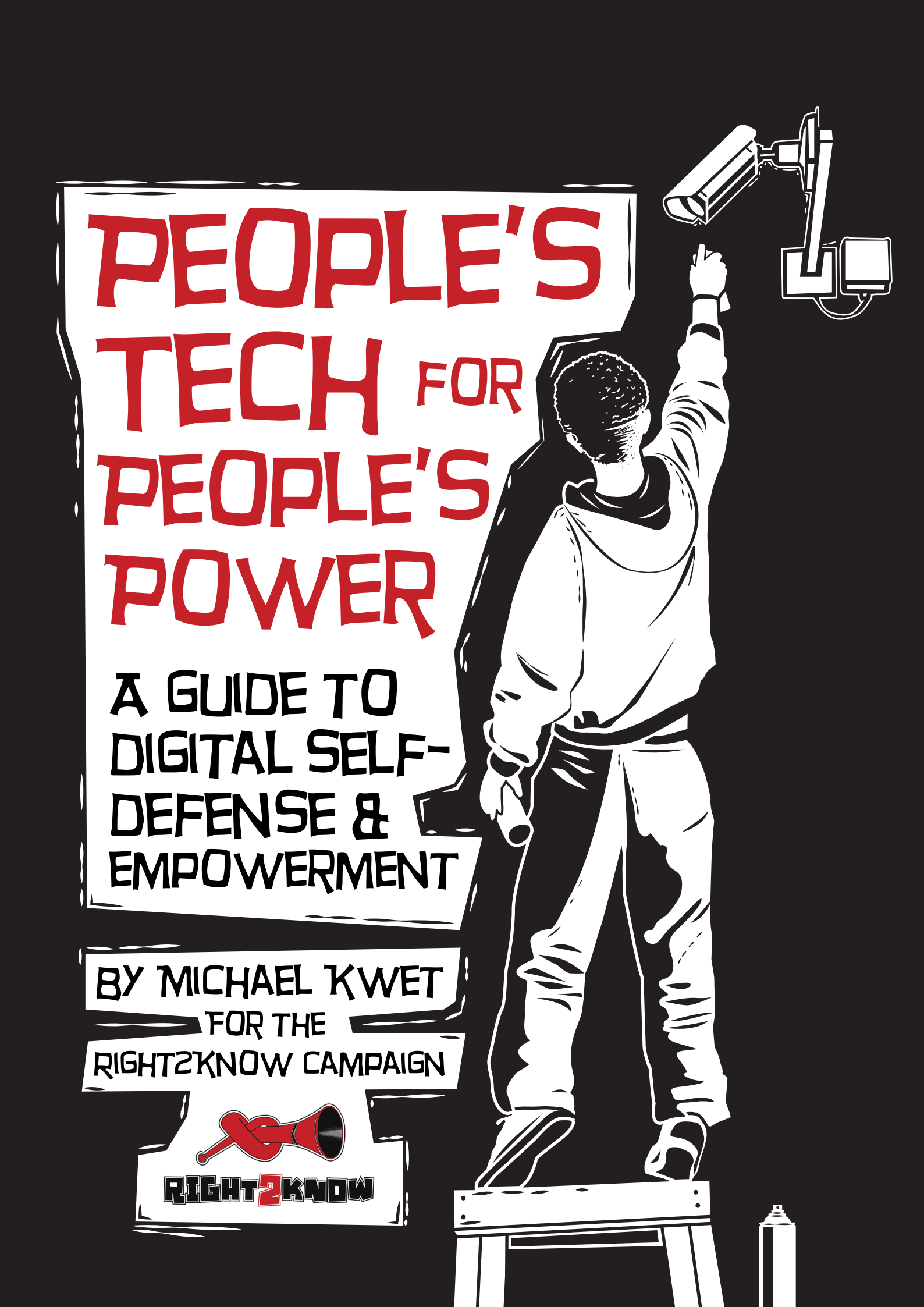
PEOPLE'S TECH FOR PEOPLE'S POWER

A GUIDE TO DIGITAL SELF-DEFENSE & EMPOWERMENT

BY MICHAEL KWET
FOR THE
RIGHT2KNOW CAMPAIGN



CONTENTS

Acknowledgments

I would like to thank Murray Hunter, Matt Mitchell of Crypto Harlem, Azhar Desai, Dale McKinley for reviewing the text. Thanks also to Stronghold Publishing for designing the guide and Wilna Combrinck for designing the cover, and Right2Know's Thami Nkosi, Busi Mtabane, and Ghalib Galant for working with me on getting this published. I am responsible for all final content.

License:

Text: Copyright 2020, Michael Kwet. Licensed under CC BY-ND 4.0 International.

Cover image: Copyright 2020, Wilna Combrinck. Licensed under CC BY-SA 4.0 International.

ACRONYMS

ALPR:	Automatic license plate reader
CBD:	Central Business District
CCTV:	Closed-circuit television
CSIR:	Council for Scientific and Industrial Research
Free Software:	Free and Open Source Software
GCHQ:	Government Communications Headquarters
NCC:	National Communications Centre
NSA:	National Security Agency
OIC:	Office for Interception Centre
OS:	Operating system
PGP:	Pretty Good Privacy
RICA:	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
SA:	South Africa
SAPS:	South African Police Service
US:	United States

1 Introduction: The Rise of Digital Colonialism and Surveillance Capitalism

As we progress into the 21st century, digital technology is changing every part of society. With the spread of computers and the internet, enormous amounts of information is being collected by governments and corporations.

This guide, which is tailored to the South African context – but applicable to other societies – will equip you with the info needed to protect yourself against government and corporate spying. It provides you with knowledge about **People's Tech for People's Power:** technologies which empower individuals and societies to control their own digital experiences.

This guide is different from others because it contextualises the issue of surveillance to its root causes. Problems of privacy, security, and surveillance connect to the broader themes of capitalism and authoritarianism. People's Tech is essential to creating a more prosperous society that replaces digital capitalism with **digital socialism**[1] – a society in which the people directly own and control the means of computation, and develop it for the well-being of humanity instead of profit and control.

This booklet is for both beginner and more experienced readers. It will explain some of the fundamentals of 21st century surveillance in South Africa, touch upon themes of **digital colonialism**, and suggest what people can do to protect themselves from surveillance and empower their society.[i]

Surveillance Technologies: An Overview

Activists, journalists, academics, judges, politicians, and the general public are subjected to constant digital surveillance. Intelligence agencies, police, and private security forces are using high-tech equipment that can target activists and pacify dissent. Corporations are profiting by tracking your every move when you use their products and services. Law enforcement agencies often work with companies to obtain your data, blurring the line between private and public surveillance.

Tools used by government and corporate spies include:

Cell phone surveillance

- **Network monitoring:** As a matter of law, telecommunications operators such as MTN, Vodacom, Cell C, and Telkom are required to monitor information about their users. South Africa's primary state surveillance law, The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), forces these companies to store metadata[ii] about electronic communications. This includes metadata about phone calls, SMS messages, emails, and internet activity (such as browsing information)[2] for up to three years. They are also required to have the facilities available to intercept the content of

i The kind of digital socialism I have in mind calls for a democratic, commons-based digital ecosystem directly owned and controlled by the people (see Chapter 19).

ii Metadata is data about data, such as who texts who, rather than what they say in the text (see Chapter 3).

what you say in real-time (i.e. they're able to monitor content, but restricted from doing so unless they receive a court order). At the time of writing, it appears the government had only passed the necessary regulations to apply these requirements to the telecommunications industry; the situation is less clear when it comes to metadata-logging and interception of information among internet service providers.

- **Grabbers** are suitcase-sized tracking devices that intercept mobile phone communications within a several kilometer radius. Grabbers pose as fake cell phone towers, tricking cell phones into connecting to them. Once connected, the phone's physical movements can be tracked, and data such as SIM card identification numbers, phone numbers, contact lists, and metadata can be swept up by the grabber, with no knowledge from the phone owner that the tracking is taking place. Grabbers can also "clone" a target's cell phone and make/receive calls and text messages that will appear as if they are coming from the target's number. Some grabbers can intercept and record the content of SMS messages and phone conversations,[3] and thousands of people could be spied on all at once, simply for being in that area. Grabbers are also known as "IMSI catchers", "cell-site simulators", or "stingrays".[4]

Social media surveillance

- South African law enforcement agencies may be using computer software to collect information posted publicly on social media websites like Facebook and Twitter. When users post messages on social media which are shared with the public, the data can be easily collected and evaluated by spies.[5]

Video surveillance

- **Closed-circuit television (CCTV)** networks are comprised of surveillance cameras mounted to physical structures like walls, buildings, ceilings, vehicles, bodies, or street poles. Surveillance cameras often form a network to cover a wide area, and they are multiplying in public space. The latest CCTV networks are capable of using **video analytics**, such as behavioral, object, and facial recognition, while **smart camera networks** can perform complex analysis of behavior across a network of cameras.[6] A corporation called Vumacam is attempting to build a 100,000+ smart camera network that will extend across Johannesburg and expand into other areas, including Ekurhuleni, Mogale City, Tshwane, KwaZulu-Natal, and the City of Cape Town.[7] Private debt collectors and repossession agents are also making use of CCTV surveillance.[8]
- **Traffic cameras**: Surveillance cameras, including automatic license plate readers (ALPRs), are being used to regulate traffic, enforce traffic violations, and manage road tolling systems.[9]
- **Mobile police cameras**: The South African Police Service (SAPS) has piloted small cameras on police officer uniforms that they say will be widely used in the future. These "body cams" can be used to record video of public spaces.[10] The Cape Town, Nelson Mandela Bay, and eThekwini municipalities also operate mobile surveillance vehicles, while the SAPS utilise on-vehicle ALRPs.[11] In October 2019, the Durban Metro Police Department announced Microsoft partnered with the City of Durban for "21st century" smart policing. This entails a rollout of the Microsoft Advanced Patrol Platform for police vehicles, a surveillance-based patrol solution which incorporates facial recognition, a 360-degree ALPR, and integration into Microsoft's Azure cloud for evidence gathering and Big Data analytics.[12]
- **Drones** are unmanned aerial vehicles (UAVs) often used for surveillance and crowd control. In 2014, it was reported that an undisclosed mining company had bought drones that can

dispense pepper spray on protesters.[13] The Council for Scientific and Industrial Research (CSIR) surveillance system, Cmore, uses drones for live video streaming and tracking,[14] and the City of Cape Town has recently announced the use of drone surveillance by law enforcement agencies.[15]

Biometric Surveillance

- **Fingerprinting, iris scans, and facial recognition**: Biometric measurements quantify physical body parts for identification and verification of persons. In May 2018, the Department of Home Affairs introduced the new Automated Biometric Identification System to integrate all biometric systems – inside and outside government – into a single source for biometric authentication of citizens and non-citizens. It is a multi-modal system that will use fingerprints, iris scans, and facial recognition for identification. Palm prints and infant footprints will also be included in the database.[16]

Centralised Intelligence systems

- **Cmore** is a comprehensive surveillance system created by the CSIR, which compares it to the movie "Jason Bourne", where police forces constantly follow targets with a totalitarian surveillance system.[17] Cmore offers a cloud-based distributed platform that merges multiple sources of information into a single command and control centre. Data sources featured in Cmore's promotional material include ground surveillance cams, drones, optronic sensors, radar, and mobile devices deployed in the field. Use cases include border patrol, and it has been piloted for policing crime at undisclosed locations. In 2014, the CSIR partnered with local intelligence centres to develop "smart" policing services.[18]
- **Local (municipal/provincial) intelligence centres:** The City of Johannesburg operates a "nerve centre" it calls the Integrated Intelligence Operations Centre (IIOC) to monitor surveillance cameras and integrate municipal data on a single platform. The City of Cape Town houses its own version at the Transport Management Centre (TMC), while AxxonSoft's Incident Management Centre, located in Pretoria, monitors independent CCTV cameras from around the country. In 2017, India-based Tech Mahindra was awarded a tender to build a "One Stop ICT Fusion Centre" for the Limpopo province. Mahindra Defence Systems's technologies include license plate and facial recognition, behavior analysis, video analytics, and real-time monitoring.[19]
- **National intelligence centres**: The South African government has two primary national surveillance centres: the National Communications Centre (NCC) and the Office for Interception Centres (OIC). RICA provides for the OIC to act as the intermediary between government security agencies and telecommunications and internet providers during "legal" interceptions. For years, the NCC was involved in mass and targeted surveillance as an effectively unregulated, extra-legal interception centre. In September 2019, the High Court of South Africa ruled bulk surveillance activities and foreign signals interceptions carried out by the NCC are unconstitutional,[20] but the judge stopped short of ruling that *mass surveillance itself* is necessarily unconstitutional.[21]
- **Foreign intelligence agencies**: During the 2000s, a series of whistleblowers revealed that the United States is conducting mass untargeted surveillance across the world. In 2013, the Edward Snowden leaks revealed much of the surveillance is obtained through cooperation with or by exploiting US-based tech corporations like Microsoft, Facebook, Google, and Apple – whose products and services are used by South African citizens. Non-US persons are not protected from surveillance under US law.[22] Many governments enter into intelligence sharing alliances,

such as the Five Eyes (US, Britain, Canada, Australia, New Zealand), the Nine Eyes (the Five Eyes plus Denmark, France, the Netherlands, and Norway), the Fourteen Eyes (the Nine Eyes plus Germany, Belgium, Italy, Spain, and Sweden), and the NSA partnership with Israel's Unit 8200 army intelligence unit.[23]

In 2013, Britain's Government Communications Headquarters (GCHQ), a top US intelligence ally, was caught spying on South Africa's foreign ministry.[24] Two years later, a tribunal found the GCHQ kept the Legal Resources Centre under unlawful surveillance.[25] Nevertheless, the world's people, including South Africans, remain targets of foreign dragnet surveillance programmes led by the United States.

Surveillance Capitalism

Throughout history, surveillance systems have undermined freedom and democracy. In South Africa, surveillance has been central to systems of oppression, from the identity passes issued to indigenous people under colonialism to the reference books (dompas) administered by the apartheid government. With digital technology, the capacity for surveillance has expanded, and is being used by those with power for political, economic, and social control.

South Africa is often deemed the "protest capital of the world", and many protesters are subjected to mass and targeted surveillance. This threatens freedom of expression. Civil society activists and the poor are the most vulnerable, and they face the most violent repercussions for their political activity. Journalists, judges, politicians, whistleblowers, unions, and academics are among the many surveillance targets in recent years.[26]

Today's surveillance is much more pervasive than in times past. A new, digitally-powered form of **surveillance capitalism**[27] – the economic exploitation of society through corporate and state mass surveillance – is spreading to South Africa from abroad. This threatens our civil rights and liberties by subjecting us to a life continuously watched and recorded by states and corporations.

Big Data refers to the drastic expansion of data collected about people and nature in today's digital world, and the use of computers to make sense of it by identifying patterns and correlations.[iii] Information about things such as what people like, what websites they visit, and who they are friends with has provided Big Tech corporations with data that can be used to manipulate people's behavior with targeted advertisements and addictive features. For instance, Silicon Valley corporations are capturing market share by using "brain hacking" – the systematic exploitation of psychological vulnerabilities to hook consumers into their products and services so they will view more ads.[28] Big Data underpins these practices, and is spreading fast across society.

US-based transnational corporations, led by "GAFAM" (Google, Amazon, Facebook, Apple, Microsoft), are the centre of this brave new world. They continuously collect every little detail about us from our computers, mobile phones, and internet activities. As technology advances, they are expanding their data fiefdoms by building surveillance into household gadgets like Amazon Echo and Google Nest. Through the Internet of Things, everyday appliances like "smart" refrigerators, thermostats, trash cans, toothbrushes, and even diapers are being manufactured to collect ever more consumer data.[29]

iii Big Data also extends to non-human data, such as images from outer space. In this guide "Big Data" is primarily concerned with data about people.

Digital Colonialism

At a broader level, **digital colonialism** – the use of digital technology for political, economic, and social control – is wreaking havoc on the Global South.[30] Digital colonialism is principally achieved through the ownership and control of the *digital ecosystem* – software, hardware, and network connectivity – which is then designed by its owners for profit and plunder. The term dates back a couple decades, and the issue has now become a crisis in global politics. Silicon Valley has created an exploitative model for the digital society, which is being replicated by many South African startups and corporations.

During the late nineteenth century, white colonizers seized the mineral-rich land in Kimberley and Johannesburg, owned and operated the heavy machinery necessary to drill deep underground, fashioned the chemicals required to exploit the minerals, recruited the engineers needed to produce all of these technologies for industrial-scale looting, and forced people of color into cheap and menial labour. US engineers swooped in for the bounty. European missionaries waged intellectual warfare on the population to compel obedience to brutal, racialised oppression. Similar patterns of colonisation were repeated throughout the world.

Today, the "open veins" of the Global South are the "digital veins" crossing the oceans, wiring up a tech ecosystem owned and controlled by a handful of mostly US-based corporations. The transoceanic cables are often fitted with strands of fibre owned by corporations like Google and Facebook, for the purpose of data extraction. The cloud centres are the heavy machinery owned by the likes of Amazon and Microsoft, proliferating like military bases for US empire, with Google, IBM, and Alibaba following behind. The engineers are the corporate armies of elite programmers numbering the hundreds of thousands, with generous salaries of R4 million ($250,000) or more as compensation.

The exploited labourers are the people of color producing the minerals in the Congo and Bolivia, the armies of cheap labour annotating artificial intelligence data in China and Africa, the East Asian workers enduring PTSD to cleanse Big Social Media of graphic content, and the vast majority of people asked to specialise in non-digital goods and services in a worldwide division of labour. The US is at the helm of advanced economic production, which it dominates through the ownership of intellectual property and core infrastructure, backed by imperial trade policies at the World Trade Organisation. The missionaries are the World Economic Forum elites, the CEOs of Big Tech corporations, and the mainstream "critics" in the US who dominate the "resistance" narrative, many of whom work for or take money from corporations like Microsoft and Google, and integrate with a network of US-Eurocentric intellectuals drawn from elite Western universities and media outlets.

Chinese corporations like Tencent, Huawei, and Hikvision could also have a neocolonial impact in South Africa. However, these companies currently have a marginal influence by comparison to US transnationals, though Chinese corporations have a substantial role in South African industries like CCTV surveillance and 5G. Some Chinese mobile devices are popular in South Africa (e.g. Huawei, HiSense, Xiaomi), but these typically come packed with US software.[iv]

E-education – the use of computers in education – is a key battleground in the fight for South Africa's digital future. Operation Phakisa in Education (OPE), launched by then-President Jacob

iv The United States banned Huawei phones from licensing core Google software products in 2019, which could eventually increase the presence of Chinese-developed software in the South African mobile phone market.

Zuma in 2015, aims to fast-track digital technology into all public schools – with Silicon Valley set to colonise the classroom and through it, South Africa's broad tech ecosystem.[31] The ANC plan to roll out paperless classrooms throughout the country was re-affirmed by President Ramaphosa in 2019 (see Chapter 18). The technologies chosen for public schools will have an enormous impact on the trajectory of digital development in South Africa.

The state-corporate domination of the digital ecosystem poses an emergency. If we are to have a free and humane society, we need to push back against digital colonialism, surveillance capitalism, and the state-corporate ruling class elites driving it forward.

People's Tech: The Fight for a New Digital Society

As you will see, freeing yourself from corporate products and surveillance is not as simple as installing a new app, nor is it simply an *individual* problem you can prevent all by yourself. We live in a digital society, and we are forced to interact with digital technology together.

Some people say, "I don't care about surveillance because I'm not doing anything wrong". In reality, we all value our privacy. We close the door and shut the blinds when we wish to be alone or spend time with someone else. Nobody wants to live in a glass house.

In addition to personal protection, privacy is also needed for the *social* good. Many *other* people need freedom to improve society. Nelson Mandela, Steve Biko, student activists, and countless other heroes were monitored by apartheid authorities. The struggle for a better society is not over, and the new generation is being targeted for its activism and whistleblowing.[32]

Studies show that Big Data surveillance is disproportionately harmful to people of colour, the poor, immigrants, women, and other vulnerable and marginalised groups.[33] Studies also show that we conform to the status quo when we know we are being watched.[34] Mass surveillance is bad for democracy, and in the digital era, we are subjected to surveillance at levels far beyond anything experienced in human history. We need to oppose state and corporate surveillance as seriously as the pass law systems of past, before it is too late.

Through the control of digital technology, Big Tech is re-colonising the Global South. The digital economy has concentrated wealth and power into the hands of transnational corporations mostly based in the United States. South Africans and other Global South countries cannot afford to let foreign companies extract wealth and exacerbate inequality, nor can they afford to let local elites replicate Silicon Valley's playbook to amass their own tech fiefdoms.

The time to fight back is now.

People's Tech incorporates the technologies, laws, and educational changes needed to make tech work for the people, not corporations and governments. This guide explains the set of tools needed to defend yourself and your communities against digital surveillance and corporate colonisation. It links these struggles to the broader context, digital colonialism, and provides some of the concepts needed to think critically about how to build a digital society by and for the people.

2 Threat Modeling

Spying on journalists

In 2017, journalist Sam Sole of the amaBhungane Centre for Investigative Journalism obtained evidence that the South African government had spied on him. Sole was investigating the Zuma Spy Tapes story in 2008 when government spies decided to tap his conversation with a prosecutor involved in the case.[35]

In 2018, it was revealed that *Mail & Guardian* journalist Athandiwe Saba was spied on by police, who obtained her records from MTN and Vodacom. Many other journalists have been targets of state surveillance in South Africa.[36]

Everyone should learn about modern surveillance and how to protect themselves the best they can. As this guide demonstrates, there are many simple steps you can take to drastically improve your privacy. Others are more complex. People should evaluate their privacy choices *in a way that makes sense for their own lives and those in their community.*

There are many reasons we all need privacy. For the *politically active*, surveillance could paralyse their activities and deprive them of the power to change the status quo. For *everyday technology users*, surveillance could induce conformist behavior. For the *marginalised and oppressed*, surveillance could lead to violence and exploitation.

Solutions to these problems include using privacy-oriented chat apps like Signal instead of WhatsApp, concealing your web browsing activity with the Tor Browser, and making educated choices about what you choose to share on social media networks.

How should *you* make use of your computer or phone in this brave new world? Privacy advocates recommend evaluating your "threat model" to determine your choices.

A **threat model** is a plan of action to handle threats you face from adversaries. The Electronic Frontier Foundation suggests each person ask the following questions:

1. *What* do you want to protect?
2. *Who* do you want to protect it from?
3. How *likely* is it that you will need to protect it?
4. How bad are the *consequences* if you fail?
5. How much trouble are you willing to go through to try to prevent those consequences?[37]

Privacy by design

Information collected and stored by someone else – be it a corporation, government, or personal acquaintance – may one day be used against you, even if it is illegal to use that information against you right now. If the law protects you today, it may not protect you tomorrow.

Because your personal information can be used against you and your community, you should use technology that is built for privacy by design. A technology engineered for privacy will keep third parties from being able to access your data altogether, or minimise how much data accessible to them if that is not possible. This guide provides an overview of technologies designed to safeguard your privacy.

Solutions for Threat Modeling

Different people face different risks from surveillance. The activist or journalist might face severe threats like jail time or assassination, while the average person might face other repercussions, such as consumer manipulation or cyber theft.

It's impossible to safeguard against every type of threat from every possible adversary. In the physical world, you may protect your home by closing your windows or locking your doors. You may also build a fence, which takes a little bit of effort to install. The same applies to your digital security. Some steps take a matter of minutes – like installing the Signal chat app to replace WhatsApp – whereas others require a little more effort – like replacing the operating system on your smartphone.

Coping with 21st century surveillance is similar to coping with security in the physical world. You need to decide your threat model and act accordingly. All of the software in this guide is simple enough for anyone to set up and use. I will assume you have little understanding of computers, and will explain each option so you can understand it in simple terms.

For those living under extremely repressive governments, it should be noted that your Internet Service Provider (ISP) can often detect *which* apps you use for internet services, even if those apps have features to protect your privacy. For example, the company you pay to access the internet may be able to detect *that* you are using Signal or the Tor network to keep them from spying on you (see Chapters 4 and 5). If certain privacy-oriented apps are only popular with privacy-seeking activists and not the broader population, an authoritarian government may obtain this information from your ISP and flag you as suspicious. The apps in this guide should be safe to use in South Africa and countries of similar character, but if you are living in a country under very severe government repression, you should consult with trusted experts familiar with your context about which privacy apps are safe to use.

Do a little at a time

We recommend you free yourself from surveillance one step at a time using the recommendations in this guide. You do not have to change all of your habits at once. Try a new app and see how it works. Share it with your friends. Get comfortable using it. Then try something else.

Remember that a threat model begins with you, but you should also apply it to the people you interact with. If you use Gmail, for example, then Google will know who you are emailing, even if those people do not want Google to know.

Ultimately, we need to think beyond individual threat models and transform the broader digital ecosystem. If enough people use Big Tech services provided by the likes of like Microsoft, Google, Apple, and Facebook, then those companies will continue to dominate the global society. We need to find collective ways to undermine their power and replace them with a socialist commons (see Chapter 19).

3 The Basics of Information Security and Software

Information security can seem complicated to the non-specialist. Encryption, networking, and computer science are complex subjects. But there are basic principles about computer privacy and security anyone can understand.

What do we mean by "privacy"?

First, it is important to clarify the concept of privacy. Columbia law professor Eben Moglen boils privacy down to three components: *secrecy*, *anonymity*, and *autonomy*.[38]

Secrecy ensures *what* you say in your messages is only known to those who you intend to receive them.

Anonymity is secrecy about *who* is sending and receiving a message, even if *what the message says* is not secret.

Autonomy gives you the ability to control your interactions without unwanted interference. It's achieved when you have both secrecy and anonymity in your actions and communications. Without secrecy and anonymity, someone else may be watching what you say, what you read, who you are talking to, when you communicate, and more. This threatens your autonomy to decide for yourself how to behave without someone else knowing about it. A person without secrecy and anonymity loses their autonomy. Privacy is therefore foundational to our freedom.

A lack of privacy often has a **chilling effect** on freedom of expression whereby the fear of surveillance discourages freedom of speech and association in conformity with the status quo.[39]

How does encryption work?

WATCH: The Internet: Encryption & Public Keys, by Code.org

What is "encryption"?

It is also essential to explain what is meant by encryption.

Encryption scrambles the content of your data to prevent other people from reading it. To read encrypted data, you need to use a digital "key" to **decrypt** (or "unlock") the scrambled data.

End-to-end encryption is a form of encryption whereby the message is encrypted by the sender so that a third party, such as a company providing a chat app or email service, does not have the means to decrypt it. The only person with a key to decrypt the message is the person you send it to.

Encryption in the anti-apartheid movement

In 1986, the ANC and its paramilitary wing, Umkhonto we Sizwe (MK), launched Operation Vula — an initiative to bring exiled leaders and military capacity back into South Africa in support of a potentially armed movement against the apartheid state. Participants in Vula relied on an encrypted communications system they created to communicate safely across borders.[40]

Content and Metadata

When you communicate, there are two main categories of information produced:

- **Content**: This is *what* you express in the communication, such as the words, pictures, or other things you communicate in a text message, document, or email; the audio of what you say to someone over the phone or app; or the image stream in your video chat.
- **Metadata**: This is information *about* your communication, such as who or when you called or texted, how long you spoke for, or the physical location of your communications device. For internet communications this includes which websites you visit, and when.

To make this clear, let's consider a case example. Pretend you call a friend at 19:00 from the number 011 222 3333, and say, "Hello, I will meet you outside." The *metadata* includes your cell phone number, your friend's number, when the call was made, how long it lasted, the physical location of the phone, and so on. But it does not include the content of what you say on the phone ("Hello, I will meet you outside.").

Metadata surveillance violates your privacy because your metadata can reveal sensitive information about you. For example, if you call an HIV/AIDS medical clinic, it may indicate your health status. Metadata can reveal who you are friends with, who you talk to and how often, your marital status, your physical location, your income level, what political party you prefer, and more.[41] In some cases, the metadata can reveal more information about you than the content. Taken by itself, the statement, "Hello, I will meet you outside" reveals less about you than metadata which reveals you called an HIV/AIDS clinic.

Many popular Big Tech apps offer *some* elements of privacy, but still spy on you. For example, WhatsApp and Skype currently encrypt the content (voice, text, and video) of your communications. However, they also exploit your metadata for profit, and many Big Tech providers are partnered to intelligence agencies.

Some apps and services designed for privacy also collect your metadata if it is necessary to run the service. However, truly privacy-oriented solutions, such as those recommended in this guide, will usually minimise the metadata they store, and they will not make money by sharing your metadata or using it for marketing purposes.

It is important to consider both the privacy of your content and how your metadata is handled when using privacy apps for talking, texting, and other internet services.

Why use Free and Open Source Software?

Many privacy experts hold that **Free Software** – also called "Free and Open Source Software" – is indispensable to privacy and security because it provides transparency about how computer software works. Free Software provides computer users with four essential freedoms:

- The freedom to run the app as you wish, for any purpose (freedom 0).
- The freedom to study how the app works, and change it so it does what you want (freedom 1). Access to the *source code* is a precondition for this.
- The freedom to redistribute copies so you can help others (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). This gives the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

Freedoms 0 and 1 give you the freedom to use, study, and modify software. Freedoms 2 and 3 allow you to share and collectively modify software; this enables community control over the software.[42]

Software is the main element which determines what your computer can and cannot do. The *source code* is the set of human-readable instructions that tells your computer how to operate, similar to a cooking recipe. Computer code therefore shapes your computer experience.

Proprietary software is authoritarian because it dictates how your computer works through the exclusive ownership and control of computer code. Most proprietary software does not release the source code to the public, so it is *black box* software: people cannot see how it works.

Free Software is designed to prevent proprietary/authoritarian ownership and control of software by granting people the freedom to understand and control their software. With the freedom to use, understand, modify, and share your software, individuals and communities can exercise direct control over their computer experiences.[43]

The power dynamics of Free Software also strengthens privacy and security. With proprietary software, the owner of the software is given the power to insert features that spy on users because the public cannot see or modify what is going on. Proprietary software also prevents computer experts from reviewing the code for flaws that make the software insecure. If your software is vulnerable, attackers can target your device and spy on you.

Unlike proprietary software, Free Software allows anyone to view and modify the code. As a result, researchers can peer review the code, fix its flaws and insecurities, and remove malicious features that spy on you. Free Software is therefore more trustworthy than proprietary software.[v]

As Bruce Schneier, a leading computer security expert, puts it: "In the cryptography world, we consider open source necessary for good security; we have for decades … For us, open source isn't just a business model; it's smart engineering practice."[44] Edward Snowden, the whistleblower who exposed US-based NSA surveillance programmes, said the leaking of NSA documents in 2013 "would not have been possible without Free Software. I did not use [proprietary Microsoft] Windows machines when I was in my operational phase because I couldn't trust them."[45]

v For more details, see Chapter 14.

It's important to note that while Free Software is critical to freedom, security, privacy, education, and equality, it does not *guarantee* that your software will deliver those values. All software, including Free Software, can (and sometimes does) have security vulnerabilities that can be exploited by adversaries, and Free Software can be (and sometimes is) used by powerful actors seeking to exploit users. However, Free Software provides a necessary foundation, or starting point, for building truly trustworthy and empowering software (see Chapter 19 for a deeper explanation).

Free Software terminology

The term "Free Software" – or "Free and Open Source Software", as some people call it – is really about the *freedom* to use, study, and modify the software, not the *price* you pay for it. The word "free" is shorthand for "freedom", not price. When you hear someone use the term "free software" or "free and open source software", you might as well think "*freedom* software" that is meant to protect your liberty, rather than how much it costs to use.

That said, Free Software has an added pro-poor bonus: because people are able to freely copy and share the software, they typically do not have to pay to use it! Thus Free Software not only enhances our freedom (liberty), it is accessible to those who cannot afford to pay for software out-of-pocket.

It's also worth emphasising that just because you didn't pay for a particular piece of software doesn't automatically mean it is Free Software. Apps like WhatsApp and Skype are "free" – you can use them without paying – but are still proprietary and under the authoritarian control of the software owner. Big Tech corporations often make money with "free" (as in zero price) apps by spying on you and force-feeding you personalised ads. Instead of looking at the price, check if an app is Free Software by searching online for the software's license.

Wikipedia lists the software license of many apps. For a list of Free Software licenses, see: https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses.

Solutions: Use Free and Open Source Software

Free Software is vital to privacy, security, education, technological development, and economic equality.

To improve security, community self-determination, education, and the local economy, the South African government has a **Free and Open Source Software policy preference** for use in the public sector.[46]

Yet in most cases, the government is not currently implementing Free Software. It is crucial that activists demand the government use Free Software in the public sector if South Africans are to secure their privacy and develop an economy that works for the people.

For all software choices, it is best to avoid Big Tech corporate software because they spy on their users, exploit people, and concentrate wealth. The Free Software products and services listed in this guide are some of the best choices for privacy, security, and empowerment.

4 Mobile Phones: Talking and Texting

Is your phone safe?

People often make calls or send text messages containing personal information they want to keep secret. When activists learn that app makers and governments spy on their communications, they usually begin to distrust their phones. They may power them off at meetings or stow them away in a container to ensure someone else is not somehow listening or recording them.

S'bu Zikode is a civil society activist of Abahlali baseMjondolo, a movement of shack-dwellers based around Durban. In 2011, he began receiving strange phone calls from various officers in the Crime Intelligence Division. He and many other activists contend their phones are bugged.[47]

In 2017, statistics obtained from MTN, Vodacom, Cell C, and Telkom revealed that cops are exploiting Section 205 of the Criminal Procedure Act to spy on the phone records of at least 70,000 mobile phones every year.[48] Civil society activists and journalists have serious concerns about cell phone surveillance.[49]

A Stellenbosch-based company called VASTech has developed powerful technology to intercept, record, and analyse the phone call, voice, fax, and SMS communications communications of entire populations. VASTech uses intercepted data, including chat data, to identify relationships between people based on their communications patterns. There is no evidence that VASTech is being used inside of South Africa, but it cannot be ruled out, as it is based in South Africa and the company's founder focuses on "developing countries ... hungry for advanced surveillance technology".[50]

Over 90% South Africans have a mobile phone. Sixty percent of South African adults owned a smartphone as of spring 2018, while 33% own a basic "feature phone".[vi] [51] Because smartphones are getting cheaper, most mobile phones will soon be smartphones.[52] However, data rates in South Africa are among the most expensive in the world, and much work needs to be done so that everyone can access a quality smartphone and afford to use the internet. Low income individuals should be given a free basic amount of airtime and data just as they should be provided free basic water and electricity.[53]

To obtain a cell phone number, RICA requires you to register your SIM card using your national identity document,

How does SA's surveillance law work?

READ: Stop the Surveillance – an activist guide to RICA in South Africa

vi Feature phones are older, inexpensive cell phones that usually have physical buttons, simple software, and very limited internet services. They do not include the advanced software functionality of a smartphone.

temporary ID, or passport, as well as proof of residential address. This means your phone number is fixed to your identity. RICA also requires telecommunications providers like MTN, Vodacom, Cell C, and Telkom to keep metadata records about their customers for up to three years. The state can request access to that information subject to RICA procedures.

Thus your phone communications – who you call, when you call, and if you are wiretapped, what you say – are surveilled by your mobile data provider and (potentially) government agencies. To stop this snooping, you must use smartphone apps that secure your privacy.

The two most popular Free Software chat apps available for smartphones are Signal and Wire. These apps protect your conversations with end-to-end encryption. Signal collects a minimum amount of metadata, but requires you to use your phone number to use the app. Wire keeps a lot of metadata about you on their servers, but does not require you to use your phone number to use the service. Signal and Wire apps do not display ads or make money by sharing or exploiting your data.

Some Big Tech apps like Facebook's WhatsApp offer end-to-end encryption, but they are problematic because they are owned by companies that also exploit your metadata for profit, are likely or known to be partnered to intelligence agencies, and dominate markets in the digital economy.

Solutions for Talking and Texting on Mobile Phones

To protect your phone conversations, you should use apps designed for privacy such as Signal and Wire. This can only be done on smartphones, as feature phones will not be able to install special privacy apps to encrypt your calls and text messages.

Chat Apps

Signal is a privacy chat app for your smartphone and desktop/laptop that protects all communications – text messaging, voice messages, phone calls, and video calls – with strong end-to-end encryption via the Signal Protocol. You can be very confident that your communications in Signal are private. Signal is Free Software, though there are some proprietary elements in the backend.[vii]

Signal pledges not to store metadata about who you talk to. At present, the only data it keeps is what number you use, when you registered with Signal, and when you last used it.[54] In the near future, Signal will be adding a feature that will force you to upload your contact list to Signal's servers, in order to make it easier to move your profile across devices. This feature has been criticized by some cybersecurity experts.[55]

Signal has been audited by independent security experts to help ensure it is safe and secure.

Like many chat services, Signal provides a two-check indicator about the delivery of its text messages to phones. The first check indicates your text message was sent to the Signal server, and the second message indicates it was delivered to your friend. Be wary that if you send a message to someone and they don't respond, it may be that their phone did not notify them. The message will show up when they open the Signal app.

Drawbacks: At present, Signal requires requires you to register an account with your phone number. Because RICA compels you to register your phone number with your real-life identity, your Signal account will be linked to your real-life identity. Communication with other Signal users requires you to reveal your phone number, which can then be used to identify who you are when using Signal.[56] In the near future, Signal has indicated it will be allowing you to form an account without using your phone number. However, this move has been criticized by some cybersecurity experts, because it also requires you to upload your contact list to Signal's servers using a method some experts believe can compromised by well-resourced adversaries.[57]

To install Signal, download the APK installation file from https://signal.org/download and open it on your phone, or install the app from Google Play or Apple App Store. Once you register an account on your phone, Signal can also be used as a standalone app on your desktop or laptop (see Chapter 9).

Wire is a privacy chat app for your smartphone and desktop/laptop/tablet that secures all app features – text messaging, voice messages, phone calls, and video calls – with strong end-to-end encryption. You can be very confident the content of your communications in Wire are private. Wire does *not* force you to register with your phone number (you can register with an email address), so you can use a fake name (such as *Cat12345*) without having to link your account to your real-life identity. With this feature, people can talk to you without having to know your actual phone number. That is a significant benefit to your privacy because, as noted above, your mobile phone number is tied to your real identity in South Africa (and in many other countries). For this reason, Wire is endorsed as the preferred chat app by privacy experts like Matt Mitchell of Crypto Harlem.[58]

Wire has been audited by independent security experts to help ensure it is safe and secure.

Wire is Free Software, including the Wire server code.[59] When a message is received by the other phone, Wire will display "'Sent", "Delivered", or "Unsent" under your message.

Drawbacks: Wire keeps a lot of metadata about you (in plaintext[viii] on their servers) until you delete your account, including your contact list, who you speak to, when you speak to them, when you last logged in, and more. This means that substantial metadata may be obtained by intelligence agencies without your knowledge.

To install Wire, download the APK installation file from https://wire.com/download and open it on your phone, or install the Wire app from Google Play or Apple App Store. Wire can also be used as a standalone app on your desktop, laptop, or tablet, and it can be accessed via your web browser (see Chapter 9).

Basic / Feature phone

If you do not use software to protect your privacy, your telephone conversation and SMS text messages can be easily snooped on by companies providing you the service or by third parties. Under RICA, your phone call and SMS metadata will be stored by your mobile phone provider for up to three years.

vii In this instance, the *backend* is the infrastructure Signal uses to connect users and transmit their encrypted messages.

Avoid Big Tech products and services

Apps and services provided by Big Tech corporations exploit your data for profit and often share your data with intelligence agencies. Instead of using Big Tech products, try using privacy apps and services as your top choice, and use Big Tech products as little as possible.

WhatsApp is the most popular smartphone app in the world and the most popular chat app in South Africa. It can be used on your phone and on your desktop, laptop, or tablet. WhatsApp uses the Signal Protocol, which protects the *content* of your communications with end-to-end encryption.

However, WhatsApp is owned by Facebook, a surveillance capitalism corporation that is partnered to the NSA and violates user privacy for commercial profit.[60]

WhatsApp users have the option to create a non-encrypted backup of their messages and store them in an Apple iCloud (iOS) or Google Drive (Android) account. While this feature does not have to be turned on, both you and the people you communicate with will have to turn the feature off to avoid one party storing a plaintext (unencrypted) log of your conversation with Google or Apple.

WhatsApp also collects your metadata. This means WhatsApp and its parent company, Facebook, can learn a lot about you: who you talk to and how often, your friend networks, and even your dating or health status. WhatsApp also retains a copy of your contact list, which can be handed over to governments.

While Wire collects your metadata, it at least allows you to register under an anonymous name via an email account, and it is not owned by Facebook or aspiring to become a surveillance-based corporation.[61]

I recommend avoiding WhatsApp because it collects and exploits user metadata for advertisements, there is no way to reliably prove backups are turned off for both parties in a conversation, and because they are owned by Facebook, a surveillance capitalism corporation partnered to the NSA.[62] *Twitter* direct messages, Facebook's Instagram messaging, and WeChat (owned by China's Tencent) do not provide end-to-end encryption, and they exploit your metadata.

Facebook Messenger does not protect your content (messages, voice, audio) with end-to-end encryption unless you turn on "Secret Conversations" each time. Secret Conversations is available in the Facebook Messenger mobile app. Your metadata is exploited by Facebook.[63]

Apple iMessage provides end-to-end encryption of your content for iMessage users only. Apple keeps your metadata for 30 days and may share your iMessage contacts with law enforcement agencies.[64] *Snapchat* does not use end-to-end encryption for text messages and group chats, conducts location surveillance, and exploits your data to serve targeted ads.[65]

Telegram uses a proprietary encryption protocol criticised by cybersecurity experts like Edward Snowden.[66] It offers end-to-end encryption only through its "Secret Chats" option, which is only available when messaging one other person. Telegram groups are not encrypted nor are Telegram channels, and the company collects your metadata.

viii "Plaintext" means in plain, readable format, without protection like encryption. Wire cannot encrypt its metadata because it keeps the metadata in order to offer ease of use across devices.

5 Web Browsing

Digital colonialism online

The online advertising industry is currently monopolised by Google and Facebook.[67] In 2017, online news outlet GroundUp dropped Google Ads from its website because they were making almost no money from it. "Why let Google profit off our ads when we hardly make a single Rand back?" they reasoned.[68]

Nevertheless, Google and Facebook follow people across the internet to profile their browsing habits for targeted advertising. In some cases, targeted ads have led to racial profiling in social media experiences.[69]

You are being watched by advertisers and data brokers while you browse the web. They follow you around to target you with personalised ads and track consumer behavior. This creates a commercial surveillance society where you are profiled by corporations looking to manipulate you into purchasing products.

When you surf the web, your browser is considered a client that requests information from websites. The request is received by the website's *server*, which sends the requested information to your unique computer address (called an *IP address*) that can be used to identify who you are.

Most websites use software to track you for marketing purposes. To do this in web browsers, they often place web cookies on your hard drive. Cookies are small files that create a data trail about you. They can track you around the web and record where you go, what you click on, as well as other activity. Websites also use *web beacons* – invisible pixels which load in your browser (or email) that record data about you. *JavaScript* can be used within websites to track information about you as well, such as where you move your mouse and for how long.

On many websites, Big Tech corporations like Facebook and Twitter display "like" buttons and "share" buttons that spy on you, even if you don't click the button. Website spying is so pervasive that Facebook uses tracking technology to snoop on your browsing habits even if you do not have a Facebook account.[70]

Foreign intelligence agencies (and possibly South African ones) also spy on your internet browsing activity.[71]

There are a few ways to protect your privacy when browsing the web. One is to use the Tor Browser. "Tor" is short for "The Onion Router". It is a network of computers which combines encryption and *onion routing* to provide people with anonymous communications over the internet.

With Tor, you can visit websites anonymously. This means third parties like your Internet Service Provider or government spy agency cannot see which websites you are visiting. However, they can

determine *that* you are using the Tor network, and some repressive governments might flag Tor users as suspicious.

A second option is to use a Free and Open Source web browser, such as Mozilla Firefox or Chromium, that you customise for privacy by tweaking the settings and installing extensions (add-ons) designed to block surveillance and ads. Firefox and Chromium don't provide you the same degree of protection that Tor provides, but they are a little more convenient to use.

Some people install a *Virtual Private Network (VPN)* to circumvent censorship, access geo-blocked content, and secure privacy and security against third parties like websites and or public WiFi providers. VPNs are private networks that essentially transmit data for you directly over an encrypted connection. This cuts out your Internet Service Provider's (e.g. Vodacom, MTN, Telkom, etc.) ability to snoop on your internet traffic, and it can provide a degree of obscurity from the service you request data from (such as a website), who will see the VPN as the one requesting information instead of your network IP address. This latter obfuscation, of course, does not work if you log into an account that is tied to your real-life identity, such as a Facebook account, because it's likely that it's you who is logging in.

Many VPNs pledge not to keep logs of the data you request while using their service, and they promise to respect your privacy. However, you can never *verify* that they are doing what they say they do.[72] You have to trust your VPN provider is telling the truth and not, say, selling your data or sharing it with an intelligence agency. You cannot trust *free* VPN services to protect your privacy because they need to make money are are likely to exploit your data in exchange for the "free" service.[73] If you use a VPN, make sure to look into a which paid services are deemed trustworthy by independent researchers.

Solutions for Web Browsing

There are easy-to-use ways to reduce corporate and state surveillance when browsing the web. You may want to protect your privacy by:

- Hiding which websites you visit from outsiders
- Blocking ads, cookies, and other tracking technologies

Hiding which websites you visit can be complex because there are a variety of ways to track you. Your ISP (e.g. MTN or Vodacom) can see which websites you visit unless you use special software like Tor to block them.

To moderately protect your privacy, you can use Mozilla Firefox or Chromium with special extensions (add-ons) that block advertisements, cookies, and other tracking technologies.

Note that many web browsers have "privacy mode" or "incognito mode" options. These typically do things like delete your browser history or cookies, *but they do not provide features like anonymity.*

Some apps seem to run faster than others, depending on what hardware you are using. If one app seems slow, trying testing another.

For true privacy you should use the Tor Browser. I recommend installing Tor, Mozilla Firefox with with plugins, and Chromium with plugins.

Web Browsers

Tor Browser offers the most private and secure web browser. A Free and Open Source web browser, it uses the Tor network to secure your anonymity.

You shouldn't install add-ons like extensions inside your Tor Browser because they may be used to reveal your identity.

When using the Tor Browser, be aware that if you enter your personal information into a web page – for example, if you log into your bank account using Tor – it will still be obvious that it is you who is the visitor. In other words, *Tor does not help you if you are logging into a personal account that can easily be linked to your real-life identity.*

Tor features a *dark web* of websites you can only visit using web browser software for the Tor network, such as the Tor Browser. Dark web websites can host important and useful services, but some of them host illegal or offensive content. You can find your way around the dark web without coming across illegal or offensive content by using a dark web directory (such as http://zqktlwi4fecvo6ri.onion).[ix]

It is worth reading The Tor Project's overview for a visual explanation of how Tor works (https://www.torproject.org/about/overview.html.en) and their FAQ about how to use Tor wisely (https://support.torproject.org/faq).

To download the Tor Browser, visit: https://www.torproject.org. On the phone, install the APK from https://www.torproject.org/download, Google Play, or Apple App Store.

Mozilla Firefox (with add-ons) is a Free and Open Source web browser. It allows you to install extensions that will block advertising services.

To install add-ons, when Firefox is open, go to Tools > > Add-ons or visit https://addons.mozilla.org.

I recommend the following extensions:

- *uBlock Origin* will block advertisements. Get it at: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin.[x]
- *HTTPS Everywhere* forces Firefox to use the secure version (https) of a webpage if it is available. Get it at: https://www.eff.org/https-everywhere.
- *Privacy Badger* helps you avoid trackers and cookies. Some websites don't work properly without them so Privacy Badger lets you disable it for any site you want. Get it at: https://www.eff.org/privacybadger.
- *Facebook Container* makes it harder for Facebook to track you around the web. Get it at: https://addons.mozilla.org/en-US/firefox/addon/facebook-container.

I also recommend you review your browser settings and make changes to suit your privacy preferences.

ix .onion addresses can only be opened inside of Tor.

x Do *not* use AdBlock Plus, which, despite its name, still shows ads. See Jacob Kastrenakes (13 Sep 2016). "Adblock Plus now sells ads," The Verge, at: https://www.theverge.com/2016/9/13/12890050/adblock-plus-now-sells-ads.

I recommend some of the following settings:

Menu > > Edit > > Preferences > > Privacy & Security > > Firefox Data Collection and Use

- Turn off "Allow Firefox to send technical and interaction data to Mozilla"
- Turn off "Allow Firefox to send crash reports to Mozilla"

Menu > > Edit > > Preferences > > Privacy & Security > > Tracking Protection

- Click "Always" under "Use Tracking Protection to block known trackers"

Menu > > Edit > > Preferences > > Search

- Set DuckDuckGo to default search engine

For additional privacy and security recommendations in Firefox, see: https://riseup.net/en/security/network-security/better-web-browsing.

To install Firefox, go to: https://www.mozilla.org. On the phone, install Firefox Focus: The Privacy Browser from APKmirror.com, Google Play, or Apple App Store. You can also try IceCatMobile, a Free Software rebranding of Firefox, from F-Droid.

Chromium (with add-ons) is the (mostly) Free Software version of Google Chrome, which can be used as a replacement to Google Chrome.

To install extensions, when Chromium is open, go to Menu > > More tools > > Extensions or visit the Chrome web store at https://chrome.google.com/webstore.

If you are using Chromium on a desktop I recommend the following extensions:

- *uBlock Origin* will block advertisements. Get it at: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm.
- *HTTPS Everywhere* forces Chromium to use the secure version (https) of a webpage if it is offered there. Get it at: https://www.eff.org/https-everywhere.
- *Privacy Badger* helps you avoid trackers and cookies. Some websites don't work properly without them so Privacy Badger lets you disable it for any site you want. Get it at: https://www.eff.org/privacybadger.
- *Chrome password alert* lets you know if you enter your Google password on a suspicious website. Get it at: https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep.

I also recommend you review the settings and make changes to suit your privacy preferences.

I recommend some of the following settings:

Menu > > Settings > > Search engine > > Search engine used …

- Set DuckDuckGo to default search engine

Menu > > Settings > > You and Google > > Other Google Services

- Turn off options to send information to Google

For additional privacy and security recommendations in Chromium, see: https://riseup.net/en/security/network-security/better-web-browsing.

To install Chromium, go to: https://www.chromium.org/Home. On the phone, you can install the Chromium APK from https://download-chromium.appspot.com or getChromium from F-Droid.

VPNs

I only recommend using paid VPNs. You should assume that they may keep records of your data. Consult a guide authored by an independent researcher if you are interested in using a VPN.[74] Do not use free VPNs because they need to make money and will likely exploit your data to do it.

That One Privacy Site (https://thatoneprivacysite.net) offers a good overview of the VPN market. For additional guidelines on VPNs, see the Electroncic Frontier Foundation's overview at: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

Avoid Big Tech products and services

Brave is a Free and Open Source privacy-oriented web browser based on the Chromium browser. It comes prepackaged with tools to block ads and website trackers.

However, Brave offers an optional advertising service that pays users small amounts of money – paid out in Brave's cryptocurrency – in exchange for viewing ads. This puts pressure on low income people to view advertisements, which are often deceptive and push a consumerist lifestyle on the public. It also perpetuates an ad-supported media model which is corrosive to democracy and media independence.

For these reasons, I do not recommend the Brave web browser.

Google Chrome is based on the Free and Open Source Chromium browser, with proprietary Google features. It should be avoided at all costs. The Chrome browser generates profit for the surveillance giant Google, and it subjects its users to massive amounts surveillance-based advertising.[75]

Apple Safari only works on Apple devices, which keeps you locked into Apple's neocolonial, surveillance-infested software ecosystem. There is no reason to use Apple Safari instead of Mozilla Firefox or Chromium.

Microsoft Edge is based on the Free and Open Source Chromium browser, with proprietary Microsoft features. Like Google, Microsoft is partnered to the NSA, and is a neocolonial force in the Global South. There is no reason to use Microsoft Edge instead of Mozilla Firefox or Chromium.

6 Searching the Web

How fear leads to censorship

In 2013, an American whistleblower named Edward Snowden leaked classified documents about the US National Security Agency spy operations to the press.[76] In 2017, a legal scholar named Jon Penney released a landmark study on censorship, which found a drastic and sustained drop in the number of people who searched for terrorism-related terms on Wikipedia immediately after the Snowden leaks. Awareness of government surveillance had substantial chilling effects on Wikipedia users, who self-censored their searches for fear of being watched.[77]

Data from search engines can reveal a lot about your personality. People should be free to search the web without disclosing information about themselves. Yet whenever you use Google's search engine, you are feeding Google information about what you are interested in knowing, what you desire, and much more. The same is true for any search engine that collects data about you.

Research has shown that in addition to profiling people with surveillance, search engines can reinforce socioeconomic biases against marginalised communities. For example, Google's search results have been shown to discriminate against black women in its autosuggestions for answers to questions about what is beautiful or what a professor may look like.[78]

Search engines like DuckDuckGo and Qwant pledge not to track or profile their users based on the searches they make. However, this does not mean their search results are not also biased. As a user, be wary of potential search engine biases in any search engine that you use.

Solutions for Searching the Web

You can secure your privacy by making searches within Tor, and by using search engines which pledge not to keep track of your search history as part of their service.

If you have a Google account, you should check all the searches you made on Google and delete them by going to My Activity: https://myactivity.google.com.

DuckDuckGo is the most popular search engine that offers privacy protection. It features a search bar just like Google and Bing, but pledges not to track or store personal information about its users as a matter of policy.[79] Try using DuckDuckGo instead of Google or Bing.

To search with DuckDuckGo, go to: https://duckduckgo.com. On the phone, install DuckDuckGo from https://apkmirror.com or install DuckDuckGo in F-Droid, Google Play, or Apple iTunes.

Qwant also searches the web for you without collecting your data as a matter of policy.[80]

To search with Qwant, go to: https://www.qwant.com. On the phone, install Qwant from https://help.qwant.com/help/qwant-mobile/download-android-apk, Google Play, or Apple App Store.

Searching in Tor: You can search for information anonymously when using the Tor Browser, so if you want truly strong privacy when searching online, use Tor. By default the searches typed into Tor Browsers are made via the privacy protecting search engine, DuckDuckGo, but Google Search is also available within Tor.

At the moment of writing, when you search Google and many other services inside Tor, the website periodically asks you to fill out a *CAPTCHA,* which is a short image identification quiz to make sure your computer is not a robot. This can take as long as a minute to complete. Unfortunately, the most popular captcha system, called reCAPTCHA, is run by Google, and it trains Google's artificial intelligence. Thus, when the reCAPTCHA system pops up in Tor, it perversely makes Google image recognition more powerful.[81]

Searching on Firefox or Chromium: You can change your default search engine in your web browser so that a privacy-respecting search engine is your first option.

In the Firefox Menu, go to:

Edit > > Preferences > > Search

- Select something new, such as DuckDuckGo

In the Chromium Menu, go to:

Settings > > Search Engine

- Select something new, such as DuckDuckGo

Avoid Big Tech products and services

Services like *Google Search* and *Bing* spy on their users and profile them. I recommend avoiding these search engines wherever possible.

7 Sharing Data Safely

When data protection safeguards lives

In 2017, journalists from *Daily Maverick, amaBhungane,* and *News24* began publishing a series of major stories after receiving the #GuptaLeaks. The #GuptaLeaks contain hundreds of thousands of emails detailing alleged state and private sector corruption pertaining to the mass theft of public resources.[82] The #GuptaLeaks whistleblowers have yet to reveal their identities for fear of retaliation.

Journalists keep the names of leakers secret to protect them from repercussions. The ability to share data privately is essential to whistleblowers and journalists.

It is critical that the public is able to share information with others safely. Whether you are blowing the whistle on corruption or sharing personal information with a friend, you should have ways to transfer your information across the internet privately.

There are a variety of privacy tools for sharing files like pictures, videos, documents, or audio files. Apps like OnionShare require that you and your friend both use the Tor browser, and that one of you share the file through the OnionShare app. OnionShare encrypts the file and allows the sender and receiver of the information to share it anonymously.

Online sharing services like Firefox Send and Riseup Share offer an easy-to-use service that does not require a special app. Just go to their website and upload your file, and then send the unique link they generate for you with the person you want to share the file with. The file transmission is end-to-end encrypted, meaning the hosts (Firefox and Riseup) cannot access the file you upload to their servers. These services limit the size of the file you can upload, however, and will be automatically removed within a set amount of time.

Privacy solutions for personal cloud-based storage drives are still being developed by the Free Software community (for more on the cloud, see Chapter 16). Services like NextCloud require you to pay for a storage solution in the cloud or host your own server. However, it is currently complex to use, and end-to-end encryption is still in a testing phase. Big Tech providers offer free file storage in their clouds, but they do not use end-to-end encryption and hold the encryption keys, so they can access your files.

Prominent news organisations use SecureDrop as a state-of-the-art solution for secure communications and the sharing of top-secret information. SecureDrop is a complex solution built for whistleblowers and professional use cases.

Solutions for Sharing Data Safely

The privacy-respecting file sharing services I recommend involve downloading an app or using a website. Both options are easy to use.

OnionShare is a Free and Open Source app that utilises the Tor network for file sharing. If you install OnionShare, you can safely share files securely and anonymously with your friend over the Tor network. The person whom you want to share the file with has to use Tor browser to visit a hidden service/dark web site that OnionShare creates on your machine. OnionShare will provide you with this web address. By default, once the file is downloaded the address stops working so no one else can use it. However, you can disable the setting to "stop sharing after first download" to allow multiple users to download the file.[83]

You can download Onionshare from: https://onionshare.org. For instructions on how to use Onionshare, see: https://github.com/micahflee/onionshare/wiki.

Mozilla's Firefox Send offers a Free and Open Source, browser-based end-to-end encrypted file sharing service[84] so you can send files to friends without having to use a special app like OnionShare. To use the service, visit https://share.firefox.com in your web browser and upload your file.

You can upload a file up to 1GB in size at the time of writing. After the file is uploaded, the Mozilla website generates a unique link (URL) that you can copy and send to your friend. Your friend can then visit the URL and download the file. The file will remain on the Mozilla server until someone downloads it. If nobody downloads the file, Mozilla automatically deletes it after 24 hours. **Note:** As of August 2020, the service is offline to be improved, but will re-launch soon. Keep checking the website for its return.

Riseup Share offers a Free and Open Source, browser-based end-to-end encrypted file sharing service[85] similar to Firefox Send. The file uploaded can only be deleted by the person who uploads it, and files are stored no longer than 12 hours. Currently, files cannot exceed 50MB in size. To use Riseup Share, visit https://share.riseup.net and upload your file.

Sharing files through services like Firefox Send and Riseup is convenient, but use caution: do not provide the link to anyone you do not want to download to your file. I recommended that you use secure, private chat apps (like Wire or Signal) or encrypted email to share links if the file contains sensitive information.

If you have a file to share that is very sensitive, you might want to use OnionShare. However, for most use cases, Firefox Send and Riseup Share is a safe enough way to share files.

In-Person: Another option is to share files using USB sticks or hard drives in-person. This cuts out the process of sending files over the internet.

SecureDrop is a Free and Open Source file-sharing solution that is used by professionals to share top-secret information. Prominent news agencies use SecureDrop to offer whistleblowers a safe way to send top-secret information, such as confidential documents, to their news agency.

- For more information about SecureDrop, visit: https://securedrop.org.

NextCloud is a Free and Open Source solution for backing up personal files and sharing files in a personal cloud. It uses multiple layers of encryption (e.g. in-transit, server-to-server, on-storage, and end-to-end in the clients), but its end-to-end encryption is in a testing phase. To use NextCloud, you must pay for storage, either by purchasing access to a third party cloud provider or by hosting your own personal server device (see Chapter 16).

Be on the lookout for new, easy-to-use Free Software services like 3NWeb for storing and sharing personal data.

Avoid Big Tech products and services

Dropbox, *Microsoft OneDrive*, *Google Drive*, and *Apple iCloud*: These services do not end-to-end encrypt the files you store on their servers. The service providers hold the encryption keys, which means they can decrypt and access your files, and if government agencies come calling, they can hand your data over to them.[86] Moreover, Microsoft, Google, and Apple provide these services as a means to lock users into their software suites and entrench their dominance in the market.

8 Email Encryption

Protecting your email from outsiders

In October 2017, Economic Freedom Fighters leader Julius Malema posted a screenshot from his Google email account on Twitter: "government-backed attackers may be trying to steal your password." While the actor has not been confirmed, it suggests that a government targeted Malema's account.[87]

Some companies, like Google, scan the contents of your emails for targeted advertising. Many of the Big Tech companies that provide email services, such as Yahoo, Microsoft, and Google, are partners with the National Security Agency in the United States. In 2013, Edward Snowden disclosed that when he was a contractor for the intelligence community, he could search through the email of anyone.[88] In 2016, it was reported that Yahoo secretly scanned customer emails for US intelligence.[89]

Many people rely on email for written communications. If you use email provided by Big Tech firms, your messages are spied on by them and the intelligence agencies they share information with.

The *content* of email can be protected from spies by using encryption. However, email *metadata* – the data about who your email address is exchanging messages with, among other metadata – is not protected by current email privacy solutions.

Thus, if you don't want someone to access metadata such as *who* you are talking to and *when*, email encryption *cannot* protect you. This means if you are emailing an activist or an HIV/AIDS health clinic, a spy can potentially determine you are speaking with that activist or clinic. It is also important to be aware that the email *subject line* is *not* protected by email encryption. If you send something revealing in the subject line, such as "call my phone at 011 222 3333", that information could be intercepted.

Email encryption is valuable, however, because it can protect what you say *inside the email*. This keeps spies from accessing the *content* of the conversations you have over email. If you type, "my phone number is 011 222 3333" inside the email, it cannot be read by spies.

It is essential to remember that *both* people in an email exchange must have encryption set up in order to protect the content of the emails. This cannot be overemphasised: if someone emails you from a Gmail account that is not using email encryption, or if you email a Gmail user without using encryption, then the content of the email will be known to Google, and ostensibly spy agencies like the NSA in the United States, which could be shared with other governments (including the South African government).[xi]

xi While Big Tech services like Gmail may allow you to set up encryption to protect your emails, you must set the encryption up using other software.

There are two ways to use encryption over email: the easy (but limited) way, and the more advanced way.

Easy email encryption

The simple way to encrypt your email content is to sign up for a free service that encrypts your emails automatically. Two popular services are ProtonMail and Tutanota. But there is a limitation: these services automatically encrypt your email *only if you use the same service provider*. So if you use ProtonMail, all messages sent to other ProtonMail users will be encrypted. The same is true for Tutanota.

This method has a drawback: a user *cannot automatically* encrypt emails sent to users *outside of* their service provider. For instance, an email from ProtonMail to a Gmail account is not automatically encrypted. There is a fix for this: in order to keep the privacy of your email content secret, if you select an option to protect your email's content, ProtonMail will send the Gmail user a *link to the content* along with a password you create. The Gmail user then clicks on the link, enters the password after reading a password hint, and reads the message in a separate web page. This is a cumbersome way to send encrypted emails.

So let's say you're using ProtonMail:

- Your emails to other ProtonMail users are automatically secret/encrypted.
- Your emails to non-ProtonMail users can be secret/encrypted if you choose to use a link and password.
- However, the emails you receive from non-ProtonMail users are *not* encrypted. Any *content* in the messages coming into your inbox is not secret.

In short, it is simple to encrypt emails with ProtonMail only when you are emailing other ProtonMail users. When you email non-ProtonMail users, you have to use a clunky "link-with-password" option. The same is true for Tutanota or any other email service using this method of encryption.[90]

Advanced email encryption

Email apps like Mozilla Thunderbird offer a smoother option through an encryption technology called Pretty Good Privacy (PGP). PGP can be used with many different email services. However, you have to set it up yourself – which requires first-time users to consult a guide that walks you through the settings – and other users have to also set up PGP for it to work. Moreover, this option will require you to store a private decryption key on your own computer. If you ever lose that key, you will never be able to open those encrypted emails again. You can make extra copies of your decryption key, but if anyone ever gets a copy of that key and discovers your password, they will have the means to decrypt your emails.

How does encryption and key exchanges work?

SEE THIS VIDEO:
https://www.youtube.com/watch?v=ZghMPWGXexs/

There are a couple of advantages to using an email app like Thunderbird. First, if you already have an email account, you may be able to access it using Thunderbird, so you don't have to set up a new email account from scratch. Second, the key exchange allows users to conduct end-to-end encrypted email exchanges with users of other email service providers.

Remember: if you lose your private decryption key, you will NEVER be able to read your encrypted emails again.

Solutions for Encrypted Email

With email, you have two options. One is quick-and-easy: just create a new email account with a service like ProtonMail or Tutanota. This means you have to start using a new email account, and it works best when your friends use the same email service provider as you. The other option is to set up your own PGP encrypted email using an app like Thunderbird and the Enigmail extension. You can usually add PGP to your already-existing email account. Using Thunderbird with Enigmail works with anyone also using PGP.

ProtonMail & Tutanota: Sign up for these email services at https://protonmail.com and https://tutanota.com. Mobile phone apps can be downloaded directly from the ProtonMail and Tutanota websites, the Tutanota mobile app can be downloaded from F-Droid. Both apps can also be dowloaded from Google Play and the Apple App Store. If you are not using those app stores, download the APK file from the ProtonMail and Tutanota websites.

Mozilla Thunderbird with Enigmail are Free and Open Source solutions for accessing and PGP encrypting your email. Download Thunderbird from: https://www.mozilla.org/en-US/thunderbird. Follow the guide at https://emailselfdefense.fsf.org for step-by-step instructions on how to get your setup working, including how to install the Enigmail extension.

FairEmail and K-9 Mail: Thunderbird is not available on phones. The popular Free Software clients on Android are FairEmail and K-9 Mail. These apps let you access most email services from a single app. Install FairEmail or K-9 Mail from Apkmirror.com, F-Droid, or Google Play.

9 Video Chat

Are your video chats private?

In early 2020, the coronavirus disease 2019 (Covid-19) outbreak forced people with access to computers and internet data to rely upon popular video conferencing software like Skype, Zoom, Microsoft Teams, and Google's G Suite services. Unfortunately, these options have privacy and trust issues.

In 2013, leaked documents revealed that Skype incorporated a backdoor which lets US intelligence agencies monitor the video and audio calls of Skype users. Five years before this was reported, Skype initiated an internal program called "Project Chess" to explore how they could make Skype calls available to the government.[91]

Leaked documents also revealed that between 2008 and 2010 alone, the NSA and the GCHQ spied on millions of Yahoo video chats through a program called "Optic Nerve". This included people not suspected of any crime, as well as millions of still images from users' chats.[92]

Use of the popular video conferencing software Zoom spiked amid the Covid-19 pandemic. Yet Zoom has abused its power as a proprietary software provider to exploit information about users. In 2020, the media exposed shady data sharing practices by Zoom, which they were forced to stop in response to bad press.[93] Zoom had also claimed it was using end-to-end encryption, but the press revealed it was untrue. In response to popular pressure, Zoom will be adding end-to-end encryption in the near future.[94] Given its litany of deceptive practices, trust issues remain.

There are easy-to-use Free Software solutions for safe and secure video chats on your smartphone, laptop, and desktop computers.

For video chat, you can use privacy-oriented apps like Wire and Signal. Wire uses end-to-end encryption for video chats on the desktop/laptop, tablet, and smartphone, and is free to use for one-to-one (two-person) chats. Signal offers end-to-end video chats, but only for use on your smartphone at the moment.

You can also use your web browser (like Firefox or Chromium) to create your own video chat room online for free. To do this, simply go to the website offering the service (for example, https://meet.jit.si), enter in your own title, and push the "Go" button to generate the video chat room (for example, https://meet.jit.si/Cats12345). Then send that link to your friend(s), who can join by visiting the URL. When all participants exit the website, the room goes away.

Jitsi's chat rooms can be password protected to prevent outsider access, and you can see if another person joins the room. While Jitsi chat rooms are *not* end-to-end encrypted at the moment, developers will be adding this feature very shortly.[95]

While Jitsi offers a nice solution for video chats, it does not offer a full set of video conferencing features. For online web conferences, BigBlueButton offers a Free and Open Source web conferencing system that runs within your web browser. Features include real-time sharing of audio, video, presentation, and screen – along with collaboration tools such as whiteboard, shared notes, polling, and breakout rooms, as well as recording sessions for later playback. BigBlueButton requires you to set up its software on a server your own or rent, and is not end-to-end encrypted.

Some Big Tech providers offer end-to-end encrypted chats, but they also may exploit metadata surveillance for profit, share data with intelligence agencies, or offer "free" video chat services to lock users into their corporate software suites.

Solutions for Video Chat

Online "create-your-own-room" video chat solutions are good for casual interactions over the web. Services like Jitsi are easy to use for video chats in the web browser. Wire is excellent for the phone, desktop/laptop, and tablet, and Signal is excellent for the phone.

Jitsi Meet is a Free and Open Source service that provides a browser-based video chat, with the option to set a password to your room. Jitsi Meet chats are not end-to-end encrypted, but the developers are working on an end-to-end encryption solution that will be available soon. Until then, other services, such as Wire and Signal, should be your top choice if you need strong privacy.

One way to use Jitsi is to create your own Jitsi chat room by directly entering your own room name at the end of https://meet.jit.si/ or by visiting their website. You can also download the Jitsi Meet mobile app from https://jitsi.org/downloads, Google Play, or Apple App Store.

Wire offers an end-to-end encrypted video chat option for the desktop/laptop, tablet, and smartphone. The service is free for video chats between two people. At the time of writing, users have to pay for group video chats.

- To download Wire for GNU/Linux, Windows, or macOS, visit: https://wire.com/en/download.
- To use Wire in a web browser, visit: https://app.wire.com.
- To install Wire on your phone, download the APK installation file from https://wire.com download or install the Wire app from Google Play or Apple App Store.

Signal offers a standalone app that works on your desktop or laptop computer, in addition to your smartphone. However, unlike Wire, Signal only offers video calls on smartphones at the moment. At the time of writing, Signal does not offer an option for group video chats.

- To download Signal for GNU/Linux, Windows, or macOS, visit: https://signal.org/download.
- To install Signal on your phone, download the APK installation file from https://signal.org download or install the Signal app from Google Play or Apple App Store.

Big Blue Button offers a Free and Open Source web conferencing system. To set it up, you have to own or rent a server to facilitate your conferencing sessions. It is free for participants to use once the server is taken care of.

- For step-by-step instructions on how to install BigBlueButton, visit: https://docs.bigbluebutton.org/2.2/install.html.
- For more on how BigBlueButton works, visit: https://docs.bigbluebutton.org.

Avoid Big Tech products and services

Big Tech corporations offer proprietary products and services that typically spy on users. Even when their products offer something like end-to-end encryption (e.g. Apple's Facetime), they channel users into their surveillance-infested software ecosystems and tighten the stranglehold of digital colonialism.

Skype collects your metadata, and is partnered to the National Security Agency.[96] While Skype offers an option for end-to-end encryption, it is only enabled when users select "Private Conversations", and their metadata is accessible to the company.

Zoom is problematic for a number of reasons. It is proprietary software, so we cannot verify exactly how it works. Zoom's iOS app was sharing users' personal data with Facebook until *VICE News* exposed it to the public, at which point they stopped.[97] Zoom was also secretly sharing the LinkedIn profile data of some users with other Zoom users without disclosing it – a practice that they also stopped after it was exposed to the public.[98] The company emphasises that it does not sell user data to third parties, but Zoom has not made crystal clear which data is (or can be) shared with which third parties, and for what purpose.[99] Zoom had previously included an attendance tracking feature which allowed the host of a Zoom conference to see if a user clicked away from Zoom for more than thirty seconds. They removed this feature after bad publicity.[100]

For the time being, Zoom is still widely used for video conferencing because it offers the most smooth and feature-rich group video chat software available. The company is currently redesigning its approach to privacy. If you must use it, search the web for ways to secure your privacy on Zoom.

Apple's *Facetime*, Facebook's *WhatsApp*, and *Google Duo* offer end-to-end encrypted video chats, but their companies collect your metadata, exploit surveillance for profit, and are partnered to the NSA. Facebook Messenger, Google Meet, and Microsoft Teams do not offer end-to-end encrypted video chat.

10 Online Document Collaboration

Is somone watching you work?

Many people want to collaborate on documents together online in real-time. To do this, people often use services like Google Docs.

In October 2017, it was revealed that Google scans your Google Docs to flag "abusive" files. This demonstrated that Google spies on Google Docs. In 2019, a former Google staffer, Martin Shelton, who now works for the Freedom of the Press Foundation, published a blog post detailing how Google can scan the documents within Google's G Suite of applications, which do not use end-to-end encryption. Shelton notes that Google may be "compelled to share relevant user data as part of law enforcement investigations".[101] Microsoft Office 365 features similar problems.[102]

By using Big Tech online document services, you feed personal data to product providers and ostensibly their partners in intelligence agencies.

For online collaborative document editors, you can instead use services like Etherpad or CryptPad. Etherpads services work similarly to Jitsi and Firefox Send: go to the website (e.g. Riseup's Etherpad at https://pad.riseup.net), enter in your own title, and push the "Go" button. A new "room" is created. Next, send your friends the link to the room so you can edit a document together.

Etherpads use **security through obscurity** as a method to protect your privacy. Once you create the link, anyone can visit the room, *but only if they know the address of the link you created (the URL).* If the URL is obscure is difficult to guess, your conversation will be difficult to discover. Security by obscurity is similar to hiding something under your bed – it's a pragmatic solution ideal for some circumstances, but not others.

Here's an example: pretend you create your own room at an Etherpad website, https://pad.riseup.net/p/SiphosChatRoom. If an outsider discovers the website URL, or by chance visits that URL, they can see the contents of what you wrote in there. For this reason, if you pick a relatively long phrase, it is highly unlikely an adversary or stranger will guess the name of the URL.

→ Here's an example of a well-chosen URL: https://pad.riseup.net/p/SiphosChatGalaxy-2019

→ Here's an example of a poorly chosen URL: https://pad.riseup.net/p/Right2Know

The second example is a poor choice because spies may want to monitor Right2Know and could easily guess that name. Picking a password is much like hiding a key in a secret spot: if you a pick a bad spot (e.g. under the doormat) then it's easy to find.

CryptPad (available at https://cryptpad.fr) is like Riseup Pad but offers encryption that prevents the service provider (CryptPad) from being able to read what users type into the pad.[103] It offers a wider variety of fonts, formatting, and document types than a Riseup Pad.

CryptPad automatically generates a random string to name the room (e.g. CWBMLPQneFYWwe560e2j22Ng). This makes it highly unlikely someone guesses your room name, but it also makes it less convenient to remember by name if you are collaborating with a friend. If you use a CryptPad, you will have to bookmark or write down the room name. CryptPad also allows you to set a password to protect your room.

Solutions for Online Document Collaboration

Etherpad solutions are good for casual collaborations over the web. The Free Software community offers two excellent solutions, Riseup Pad and CryptPad.

Riseup Pad is better for simple text and easy-to-remember collaborative pads. CryptPad has better security and richer features, but the room names are harder to remember.

Riseup Pad offers a Free and Open Source online collaborative text editing service based that uses security through obscurity. It is hosted by Riseup, an activist organisation dedicated to user privacy.

- To use Riseup Pad, visit https://pad.riseup.net and create a new pad.

CryptPad offers a Free and Open Source online collaborative document editing service. It uses end-to-end encryption and offers you the option to password protect your collaborative document. CryptPad document URLs are difficult to remember by name, however.

Document types include rich text (akin to Microsoft Word), presentation (akin to Power Point), Sheet (akin to Excel), as well as services for coding, polls, whiteboard, to-do list, and file storage.

- To use CryptPad, visit https://cryptpad.fr and create a new pad.

Avoid Big Tech products and services

I do not recommend using Google Docs because it spies on users and supports Google, a neocolonial surveillance corporation. To create a Google Doc, you must be a Google user. Thus Google Docs draws users into the Google suite of software products, further entrenching their dominance in the digital economy.

11 Protecting Your Data

The physical theft of computer data

In February 2014, two researchers at the University of Johannesburg – Professor Kate Alexander[xii] and researcher Dr Carin Runciman – had their laptops stolen. In the course of investigating service delivery protests, the scholars found that, contrary to government claims, the protesters were not part of a mysterious "third force" aimed at destabilising the government. Details surrounding the incident suggest the laptop theft was a political operation.[104]

Many other intellectuals and public figures have had their laptops stolen. Examples include: journalists at the SABC, the laptop of advocate Dumisa Ntsebeza (who was investigating the Marikana massacre), two laptops belonging to the prosecutors at the offices of the National Prosecuting Authority, computers stolen at the Directorate for Priority Crime Investigation (aka the Hawks), fifteen computers stolen from the offices of Chief Justice Mogoeng Mogoeng in Midrand, a hard drive stolen from the office of Hennie van Vuuren (who was investigating the arms deal), an armed robbery of a member of the board of inquiry investigating then national police commissioner Bheki Cele, and computers stolen from the Helen Suzman Foundation.[105]

The information stored on your devices can be physically stolen by a thief – unless you protect yourself using encryption. Even if you are not a political person, you probably have sensitive data stored on your devices, and it is worth knowing how to protect it.

Each computer has a "drive" inside that saves your information in "files". The *hard disk* is the physical unit that stores your information – your documents, the pictures you take, and so on. The files on your computer and phone can be protected from other people if you use software to encrypt your storage drive.

There are two kinds of drives you might want to encrypt. The first is the *internal* drive that comes inside your laptop, desktop, tablet, or cell phone. The second is an *external* storage drive, such as a USB drive. Let's consider each in turn.

Setting up encryption on internal storage drives is relatively easy in GNU/Linux, Microsoft, and Apple operating systems. When you set this up, make sure to pick a safe password (see Chapter 12).

When you encrypt your drive, the software generates a *key* to unlock the drive. In most cases you will pick a password for that key. Whenever you start your computer, you enter in your password, and your computer uses the key to unlock the drive. When you power down your device, the ability to access the information is once again protected by encryption. Each time you turn your device back on, you unlock the encrypted information with your password.

xii At the time, Kate went by Peter Alexander.

This type of encryption, called *full disk encryption*, is needed to fully secure your device. If you use a password to log into your computer but do not also encrypt your data, your information will not be safe. A full disk encryption solution with a password is needed to protect your data, but it only does so when your computer is powered off. Once you have turned on your computer and successfully logged in with your password, the full disk encryption is turned off so you can use the machine. In other words, full disk encryption helps secure your device against someone who steals it, as long as the device is turned off. It is therefore a good idea to shut your device off if it will be left alone at home or in an office space.

Be sure to remember your password

Remember that if you ever forget your password used to encrypt your files – you can NEVER access that data again.

It is important to understand that files which are copied to third-party services – such as pictures stored in the "cloud" – are not protected by the full disk encryption of your phone or computer. If you would like to protect files before you put them in the cloud, you have to use file encryption software. You should do research to figure out if the app or operating system you are using is configured to copy your files to a third-party cloud service. Generally speaking, GNU/Linux operating systems like Ubuntu, LineageOS on the phone, and apps from the F-Droid app store can be trusted not to copy your data to a third-party cloud by default (see Chapter 14).

Setting up encryption on *external* storage drives can be done using an app like VeraCrypt. External storage devices include flash drives (such as USB memory sticks or small SD cards people typically use for their phones) or external hard disk drives (larger storage units that you can plug into your computer). Encrypting your external devices, such as your USB drive, is typically recommended for more advanced users.

As a potential compromise, you can use software to encrypt *individual folders* on your drive instead of everything. A program called Cryptomator allows you to create password-protected encrypted "vaults" for data storage on a drive already in use. Search the web for to get help about how to use VeraCrypt and Cryptomator.

Solutions for Protecting Your Data

If you are concerned about getting your device stolen, or losing it, I recommend setting up encryption on your *internal* drive through your operating system settings. Make sure you remember the password to unlock your device!

If more advanced users want to try external drive encryption, I recommend VeraCrypt. For an easy way to encrypt folders on a drive, I recommend Cryptomator.

On GNU/Linux: You should set up hard disk encryption when you first install your operating system. For GNU/Linux operating systems such as Xubuntu or Ubuntu (see Chapter 14), there is usually an option to set up hard disk encryption with a password of your choice. This is simple: just check the box and create a password. If you already installed GNU/Linux and want to encrypt your

files without reinstalling the operating system, you can encrypt some of your folders. Search online for help with this process.

For more information, see: https://www.maketecheasier.com/encrypt-hard-disk-in-ubuntu. As always, you can search online for help. Try searching for: "how to encrypt hard drive in Ubuntu" – or if you're using a different operating system, such as Trisquel, search for "how to encrypt hard drive in Trisquel", and so on.

VeraCrypt is Free Software that can encrypt your hard drive or individual files and folders. A somewhat knowledgeable computer user will be comfortable using VeraCrypt. You can use VeraCrypt on GNU/Linux, Microsoft Windows, and Apple MacOS. VeraCrypt can be downloaded from: https://veracrypt.fr. There is no VeraCrypt mobile app.

Cryptomator is Free Software that can be installed to created encrypted data vaults. It can be used on GNU/Linux, Microsoft Windows, or Apple MacOS. You can download Cryptomator from: https://cryptomator.org. Unfortunately, Cryptomator's mobile apps are not Free and Open Source.

Smartphones: Recent versions of LineageOS (which is Android-based; see Chaper 14), Google Android, and iOS are automatically encrypted if you set a passcode. On older Android devices, you may have to manually set up encryption. This is easy to do through the phone settings (see https://www.androidcentral.com/how-enable-encryption-android).

Avoid Big Tech products and services

On Apple MacOS: VeraCrypt should be used on macOS. Apple's own product, called FileVault, is proprietary and should be avoided.

On Windows: VeraCrypt should be used if you are on Microsoft Windows. Microsoft's own product, BitLocker, is proprietary and should be avoided.

Additional Reading:

A technical explanation of hard disk encryption:
https://wiki.archlinux.org/index.php/disk_encryption

Comparison of encryption software:
https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

How encryption works in Ubuntu:
https://security.stackexchange.com/questions/39306/how-secure-is-ubuntus-default-full-disk-encryption

12 Creating and Managing Passwords

When passwords are compromised

During the 2016 US election, documents and emails from the Democratic National Committee (DNC) were leaked to Wikileaks, who published them for the world to read. Some of the passwords used by the DNC included "Obama-Biden-2012" and "obamain08". These are weak passwords because they are too easy to guess.

In 2017, South Africa's largest data breach in history occurred when a giant file containing 27 gigabytes of data about each citizen was found openly available on the internet. The dataset included over 60 million people and contained the full name of each person, their national identity number, income, employment history, phone address, age, marital status, ethnicity, gender, and more. It also contained 2.2 million email addresses.[106]

Security researcher Troy Hunt uploaded those email addresses at https://haveibeenpwned.com, a database he maintains to help people discover if their email password has been compromised in a data breach. At that website, you can search for any email address to see if its password has been compromised in a known data breach.

When creating a password, you should do two things:

→ Pick a *strong password*

→ Decide *how to manage* the many accounts you have

In this guide, I use fictional passwords for case examples. DO NOT use the example passwords in this guide – make up your own passwords!

Creating Strong Passwords

There are different opinions about the best strategy for creating and managing strong passwords. Passwords like "123456" or "p@ssw0rd" are easy to guess and should never be used. Passwords that are short like "cat" or "Mpho" are also easy to guess and should never be used.

Experts used to suggest picking a sufficiently long password (at least 8-12 characters) that uses at least one upper-case letter, one lower-case letter, one number, and one special character (e.g. % or *). This method protects users against brute force guessing: even the fastest computer cannot guess every possible combination of a lengthy password, because there are far too many combinations to guess, even for a computer.

Researchers recently discovered that because humans have many accounts, they tend to pick a handful of passwords and re-use them across accounts. It is not practical to select a password like "yARnKitten9^" for your bank, "sHIRtMovie4$" for your Twitter account, and so on – for, say, 30 accounts. You'll never remember them all.

Many cybersecurity experts concluded that you should pick passwords which are easy for you to remember, but hard enough for someone else to guess. To do this, they recommend passphrases which are at least 5 words long. This might be something like *KittensPlayYarnFunSummer* – maybe based on a memory you have of a kitten playing with yarn in the summer. Perhaps you will add in a number and special character to make it stronger.

The length of the phrase helps to prevent computers from brute force guessing the password. However, normal sentences are easier to predict, so you may want to be clever by creating a broken sentence, such as KittensYarnFun4Ever. The most secure password might include five unrelated words with a number and special character (such as *Box*Cloud6FurballSkyChicken*), but that is less memorable than a pass phrase. It is typically recommend that you pick a pass phrase you can remember.

Managing Passwords

Once you select a passphrase, you need to figure out how to keep track of all of your passwords. Let's say you have 30 accounts, including accounts for your banks, email, social media, and so on. What do you do?

First, it is important to have a unique password for every account and to not reuse passwords. For 30 accounts, however, this becomes burdensome. **Password managers** offer a solution: they can securely store all your passwords, and they can create strong ones if you don't want to pick your own.

With a password manager, the only password you need to remember is the password to the password manager. The password manager software is protected by a password you choose: once you enter the manager's password, the password manager will automatically fill in the passwords for all of your accounts.

You can use a Free and Open Source password manager like KeePassXC to keep track of your passwords. This will keep a secure record of your passwords in a database stored on your device, and it will auto-fill in your passwords as you log into your accounts on your device.

For websites, you can set your web browser to remember your website passwords using options like Firefox Password Manager.

A password manager is generally safe, but it has a drawback: it creates a single point of failure. If someone can access your device and knows the password to your password manager, then they can then get access to all of the usernames and passwords you stored in the password manager. Moreover, if you forget or lose your master password, then you will lose access to the database of passwords.

Some people use password managers to sync their passwords across their devices. This is done by storing your password information encrypted on a third-party cloud-based server. Your password manager then receives your encrypted password data and decrypts it on your local device. Hosting your encrypted password data on a third party cloud opens up a degree of vulnerability. If you are not comfortable with that process, then you cannot currently sync your password management across devices, and have to manage your passwords separately on each device. A Free and Open

Source password manager called Bitwarden stores your passwords using end-to-end encryption online.

Multi-factor Authentication

Some services use multi-factor authentication to improve your security. Multi-factor authentication means you must perform more than one separate authentication sequence in order to access your account. This might be done by entering a short numerical code sent to your phone for Step One, and the entering of your account password for Step Two. An email account log-in would then be as follows:

- Enter a one-time generated code sent to your phone (for example, 1a3iu6)
- Enter your password (for example, KittensWithYarnCute4Ever)

Security Questions

Some services ask you to provide answers to security questions in case your forget your password. The service provider (say, ProtonMail) will then send a way for you to recover your password to another account you provided when you signed up – so long as you can answer the security questions correctly.

Security questions typically have a weakness: they are usually related to something someone might know about you, or can discover on the internet. For example, a security question may ask "What is your favorite musician?" or "Where did you go to high school?" If someone else knows the answer to these questions, then they might guess your security questions and obtain access to your account.

Some cybersecurity researchers suggest you pick an unrelated answer you will remember. Instead of answering something with "Beyonce" you should pick something a little harder to guess, like "KittyCat" or even "BeyonceCat".

Remember: Do not use the fictional passwords in this guide – make up your own passwords!

Solutions for Managing Passwords

When you pick your password, try to use a pass phrase that you will remember. If you have a lot of accounts, it will be difficult to manage your passwords efficiently. Try using a password manager to maintain your collection of passwords.

KeePassXC is a Free and Open Source password manager that can be installed on all devices and operating systems at: https://keepassXC.org. On Android, try KeepPassDX from F-Droid or Google Play. For information on how to use KeyPassXC, see: https://keepassxc.org/project.

Firefox and Chromium have their own password manager built in. If you use the password manager included, you should go to "Settings" and enable a Master Password for the password manager. If the password manager has no password, then anyone who can access your browser can see your saved passwords.

Bitwarden is a Free and Open Source password manager for cloud-based solutions that sync across devices. Download Bitwarden at: https://bitwarden.com. On the phone, install the APK from https://github.com/bitwarden/mobile/releases, Google Play, or Apple App store. Remember that if you forget your master password, you will lose access to your database of passwords.

Check the Have I Been Pwned website: You should periodically visit https://haveibeenpwned.com to see if your email address has been compromised. If your email address shows up in the search results, you should change your password. Be sure to note the date of the breach, which is listed at the Haveibeenpwned.com website. If you don't see a new breach listed, then there is no evidence of a new breach prompting you to change your password. However, remember that the website says that it only lists a small portion of the breaches which have occurred. It's always possible that your email address was breached but not listed at Haveibeenpwned.com.

Options to avoid: Other popular password managers include *1Password* and *LastPass*. These are proprietary services that also charge for the product (1Password) or premium features (LastPass). I do not recommend these options.

13 Phishing and Getting Hacked

The many harms of hacking

In October 2019, the City of Johannesburg shut down its website and billing systems after a hacker group, Shadow Kill Hackers, hacked their computer systems and demanded payment of four Bitcoins (about $30,000 or R530,000). The breach was "at the user level, not at the application level", suggesting the hackers breached the City's security through an employee.[107]

According to one estimate in the banking sector, South Africa has the third-highest number of cybercrime victims in the world, losing an estimated R2.2 billion a year to cyber attacks.[108] Individuals; small, medium, and micro-sized enterprises (SMMEs); and large corporations like banks are all targets of cybercriminals, the extent of which is underreported in South Africa.[109] According to IBM, South African companies lose an average of R36 million for every data breach.[110]

Spying software can be extremely invasive. Spyware called Pegasus, created by the Israeli hacker organisation, the NSO Group, exploited a security flaw in WhatsApp that gave it full access to targeted smartphones, including users' text messages, camera, and microphone. Pegasus has been discovered in over 45 countries, including South Africa.[111] An investigation spanning 100 sources in 15 countries found local authorities are using Pegasus to target human rights organisations, journalists, lawyers, politicians, researchers, and activists. Members of marginalised and vulnerable groups, such as members of LGBTQ+ communities, have also been targets of local authorities using Pegasus.[112]

Reading about spyware like Pegasus may scare you into thinking you can never protect your privacy. Why even bother trying to protect yourself if someone can come along and hack you?

In reality, protecting your privacy is not hopeless. Joan Scott-Railton, a senior cybersecurity researcher at Citizen Lab credited as the first research group to identify Pegasus, reiterated that encrypted messaging is valuable and the public should not lose confidence in encryption just because Pegasus exploited a WhatsApp vulnerability. There is a spectrum of methods used by **hackers**[xiii] that correspond to a wide range of vulnerabilities, and in most cases, you can protect yourself if you make good choices.[113]

One easy way to hack a phone or laptop is called **phishing**. A phishing attack occurs when someone sends you an email or text message designed to compromise your data. It is a method of **social engineering**, whereby a person masquerades as a trusted party, but is really trying to get your information.

xiii In the computer world, the word *hacker* has multiple meanings. Its original meaning simply referred to a person who plays around with their computer to change how it works. However, for most people, the word has since taken on a different meaning: a bad person who tries to breach your security to spy on your or steal your information. This kind of behavior is also called "black hat hacking".

Phishing attacks have been successfully used to steal information from everyone, from high-level politicians to the common person.

A phishing attack might be an email sent to you from someone who appears to be a reputable company, such as First National Bank, but is really someone else. The email address of the sender might look something like "support@fnbb.co.za" – a fake website that is misspelled, but resembles the real First National Bank website, "fnb.co.za". If you don't look closely and recognise that the website is misspelled as "fnbb.co.za", you might behave as if it is a genuine email. The fake emailer might say something like, "your account has been hacked, please click on this link to get help!" If you click on the link, it might prompt you to enter your name, national identity, or credit card information. The scammer might then use that information to purchase something with your money.

This could also happen by phone. Someone trying to steal your information might call your cell phone and pretend to be from a bank, claim that your account is in danger (or that you won some money, etc.), and try to trick you into giving your personal details away.

Other hacks are more sophisticated. The NSO Group's Pegasus software traditionally sent a Trojan horse attack – malicious software that is disguised as something legitimate – through a bogus link disguised as a real one. But in a recent case, NSO Group discovered a vulnerability in WhatsApp's Voice over IP stack (software for phone calls) that could infect their smartphones simply if they missed a WhatsApp phone call. In this case, the surveillance targets were helpless: they didn't have to pick up the call, and the records of the phone call could be remotely deleted, so they wouldn't know the call happened in the first place.[114]

While extreme vulnerabilities like this are always possible, cybersecurity experts maintain that a single security flaw of this type is rare and does not mean users should lose confidence in encryption and digital self-defense. Moreover, WhatsApp is suing the NSO Group for exploiting their software, which could discourage the use of such aggressive hacking software by some companies.[115]

It's virtually impossible to live in society with zero risk of a data breach. Even if you stop using computer devices, data about you can be placed into data repositories by other people (such as friend uploading a picture of you to Facebook) or businesses (such as purchases made with a bank card). In reality, the best that can be done is to use the best software and common sense privacy strategies, understand how to avoid phishing attacks, and put pressure on lawmakers to punish those who fail to protect our data, including those like the NSO Group who exploit software vulnerabilities.

Solutions for Phishing and Hacking

To safeguard against phishing attacks, you should be wary of suspicious emails and text messages asking you to click on links, files, or divulge sensitive information like your bank account details or national identity number to them.

Phishing scams tend to revolve around carrots and sticks. The carrots are free stuff – coupons, free money, and so on – which are too good to be true. The sticks are emails designed to make you panic, such as, "your account has been hacked or compromised, click on this link immediately!"

If you ever receive a suspicious message, you can look up the company through a trustworthy channel by calling or emailing their help services directly from their official website or phone listing and asking them if they tried to contact you.

Suspicious things to look out for include:

- Messages from people or companies that you do not know personally.
- Messages that that are misspelled.
- Links that do not match official websites (e.g. fnb-bank.co.za instead of the official website, fnb.co.za). These may be mixed in with legitimate links.
- Unsolicited attachments the sender wants you to open.
- Messages that begin with generic greetings (such as "Dear valued customer" instead of "Dear Mpho Dlamini"). It is possible that a phishing scam address you by name, but many do not. Most legitimate companies address you by your name.
- Comments like "urgent action required" or "we've noticed some suspicious activity or log-in attempts". Note that a company like Facebook or Twitter might send a message like this, however. If you get these messages, make sure the sender originates from the correct email domain. And remember, when in doubt, you should contact customer support directly, instead of opening the link provided in the email or text message.
- Messages asking you to confirm personal details.
- Messages offering you coupons for free stuff, free money, or a refund.

Good software security practices include:

- Keeping your software up to date by setting it to update automatically.
- Using an antivirus program. A good Free and Open Source antivirus program is ClamAV (available at: https://www.clamav.net).
- Backing up your important data to a USB stick or extra hard drive.
- Using multi-factor authentication for your passwords (see Chapter 12).

14 Choosing an Operating System and App Store

Proprietary software has a spying problem

In July 2019, the German state of Hesse announced they would ban several Big Tech products from schools because they violate German privacy laws. The Germans reasoned that these products are sending data about their school children to servers in the United States, which are subject to NSA surveillance. Microsoft Windows 10 was among the products listed because of the opaque data collection practices of its telemetry program.[xiv 116] The ban follows growing concerns that the popular operating systems of Microsoft Windows, Google Android, and iOS spy on their users.[117]

Equally important, researchers have revealed that Google Play and Apple iOS apps are infested with hidden trackers that spy on their users.[118] In order to create a lucrative app economy, Google and Apple allow apps to siphon your data out while you do things like check the weather or play video games. The app makers profit by collecting your data and sharing it with marketers for things like targeted advertising.

Smartphone software uses GPS, cell towers, WiFi, and Bluetooth to track your physical location for targeted advertising and app services. Knowledge of your physical whereabouts can reveal sensitive details about you, such as your political affiliations, health, and income. Location data is used to manipulate your behavior, and it creates a data trail that may be accessed by law enforcement agencies now or in the future.[xv 119]

A Free Software app store called F-Droid actively screens out apps with hidden trackers, and only offers Free Software apps.[120] The absence of spying software included in GNU/Linux and F-Droid demonstrates how the Free Software community is dedicated to protecting your privacy.

Operating Systems

Your *operating system (OS)* is the most important software in your device. If you have a poorly functioning OS, your device will will not work well. If you have an insecure operating system, your device will be highly vulnerable to hackers and malware like viruses and spyware. Operating systems can also constrain your choices. For example, Apple will not let users install apps without using the Apple App Store, so iPhone users are stuck with apps that Apple allows them to use. Your OS is therefore essential to your privacy, security, and freedom.

xiv Other products banned include cloud-based productivity suites from Microsoft, Google and Apple. See Danny Bradbury (17 Jul 2019). "Microsoft, Google and Apple clouds banned in Germany's schools", *Naked Security*, at: https://nakedsecurity.sophos.com/2019/07/17/germany-bans-schools-from-using-tech-giants-clouds.

xv In order to prevent location surveillance by cell tower providers, you have to turn your phone off or block the signal, which stops your ability to make telephone calls or transmit internet data over mobile provider networks.

On desktops and laptops, there are three common operating systems: Microsoft Windows, Apple macOS, and GNU/Linux. Windows is a proprietary operating system, while macOS is proprietary with some open source elements. **GNU/Linux** is a Free and Open Source operating system.

Free Software helps protect you against surveillance because it empowers users to remove malicious features like advertising surveillance built into the software. It also allows a broad set of communities with different political interests to audit the code for security vulnerabilities and malicious features.

The GNU/Linux operating system has many different versions. Popular, easy-to-use versions include Ubuntu (developed by Mark Shuttleworth's foundation, Canonical), Xubuntu (which is based on Ubuntu but has a Windows-like interface), and Linux Mint.

On the smartphone and tablet, there are two dominant options: Android and Apple iOS. Apple iPhones and iPads only allow you to install Apple iOS on them, and you cannot run Apple software on non-Apple hardware. Android includes an open source version called the Android Open Source Project (AOSP). All Android operating systems versions are built on the Linux kernel.

The typical Android smartphone is a Google-dominated version of AOSP that includes proprietary Google apps. Most smartphones use Google Android.

There are Free and Open Source versions of Android, however, such as LineageOS and Replicant, which are based on AOSP and without Google components. If you want to escape a great deal of Google's surveillance, I recommend installing the LineageOS operating system on your smartphone, and either LineageOS or some form of GNU/Linux (e.g. Ubuntu Touch) on your tablet.

App Stores

Your *app store* – a platform used to install apps on your device – is also very important to your software freedom, privacy, and security. GNU/Linux offers a *package manager* – which is akin to an app store – containing Free Software apps. (On the Ubuntu version of the GNU/Linux operating system, the popular version of this is called the Software Center.)

For Android smartphones, the F-Droid app store offers a repository of 100% Free Software apps free of any surveillance *anti-features* – features like surveillance that people don't want. Apple iOS users are forced to use Apple's App Store, so their ability to escape surveillance is constrained to whatever apps Apple allows its users to download.

Solutions for your Operating System

Switching your operating system might seem like a big change. However, people get used to a new system fast. The best way to switch is to back up all of your important files on a separate drive and install the new operating system on your main device. (Note: to be extra-safe, it is ideal to make two copies of your important files by placing them on two separate drives.)

In some instances, you need to have the correct hardware model to install GNU/Linux on your desktop, laptop, or tablet, or an operating system like LineageOS on your phone. Most desktops support GNU/Linux, and so do many other devices.

For a list of laptops, tablets, and other hardware that supports GNU/Linux, see: https://h-node.org/hardware/catalogue/en.

A GNU/Linux OS is often installed using a USB memory stick, also called a *flash drive*. Using the USB stick, you can either try GNU/Linux for a temporary session to see how you like it, or you can install it on your device.

To install or try GNU/Linux from a USB stick, download the .ISO file from a website like Ubuntu (https://www.ubuntu.com/download) or Xubuntu (https://xubuntu.org/download).

If you're on Windows, use an app like UNetbootin (https://unetbootin.github.io) to make your USB stick into a stick to install or try GNU/Linux. (Rufus https://rufus.akeo.ie is also an option on Windows.)

For help with installation, see this guide: https://www.howtogeek.com/howto/linux/create-a-bootable-ubuntu-usb-flash-drive-the-easy-way. (If needed, search the web for additional help.)

For a list of smartphones that support LineageOS, see: https://wiki.lineageos.org/devices.

GNU/Linux: I highly recommend using the GNU/Linux operating system. Xubuntu, Ubuntu, and Linux Mint are quite similar and provide a Windows and Apple-like experience. GNU/Linux is safe, secure, easy-to-use, and is Free and Open Source Software.

Some of the best versions of GNU/Linux are Ubuntu and Xubuntu. Ubuntu is produced by Canonical, a company founded by Mark Shuttleworth. Xubuntu is derived from Ubuntu, and is best for people who want a Microsoft Windows-like interface. Linux Mint is also a fantastic choice. Trisquel offers another other version of Ubuntu a little less easy to use but fully free of proprietary software.[xvi]

To download Xubuntu, visit https://xubuntu.org/download. To download Ubuntu, visit https://ubuntu.com/download.

LineageOS (smartphone and tablet): Your phone's operating system is critical to your security and privacy. LineageOS offers a secure, privacy-respecting, Free and Open Source alternative to Google's version of Android and Apple iOS.

I recommend LineageOS on smartphones for users who feel comfortable with their computer skills and are happy to experiment with their phones. LineageOS is supported by almost 200 phones and used by about 2 million people. However, to install LineageOS, your phone needs to be unlocked, and there are sometimes difficulties in getting many apps to work if they require Google Play services. Nevertheless, it is rewarding to install a user-respecting operating system on your phone.

Before installing LineageOS, search the web to help you determine if your smartphone is unlocked, and if it is not, how to unlock the model that you own.

To download LineageOS, visit https://download.lineageos.org and select your device by make and model. For a guide on how to install LineageOS, see: https://www.lineageosrom.com/2016/12/how-to-install-lineage-os-rom.html.

xvi Trisquel is 100% Free Software but other versions of GNU/Linux, such as Ubuntu, usually package in a few proprietary elements to make sure all compatible hardware and commonly run software works out of the box.

F-Droid: I recommend F-Droid for your Android app store. Because F-Droid apps are inspected for spyware, you can trust Android apps in the F-Droid app store. There are less F-Droid apps than there are in Google Play or Apple's App Store, but the majority of apps hosted by Google and Apple spy on you. A smartphone using LineageOS and F-Droid eliminates most spying software.

If you are not willing to go without certain apps that require Google Services, such as Google Maps or Tinder, then you will pay the price of being under surveillance. By tying some of the most popular apps to Google Services, companies perpetuate spying. In some cases, you can use your web browser to visit websites for the apps that require Google Services on your smartphone.

To install F-Droid, download the APK from: https://f-droid.org/en/packages/org.fdroid.fdroid.

Avoid Big Tech products and services

I highly recommend using Free Software solutions instead of Microsoft Windows, Apple macOS and iOS, and Google Android – especially if you want to protect yourself against commercial and government surveillance.[121] By using Big Tech's core products and services, the forces of digital colonialism and surveillance will tighten their stranglehold on South Africa and other societies.

15 Video Surveillance and Intelligence Centres

The return of apartheid surveillance

Surveillance of people's physical movements is expanding rapidly. Closed-circuit television (CCTV) networks and other surveillance devices are popping up all across the world. South Africa is no exception.

In early 2017, I reported that South African cities and suburbs are expanding the scope and sophistication of CCTV surveillance.[122] Cities like Johannesburg and Cape Town have been adding new cameras to their city surveillance grids. Law enforcement agencies in Johannesburg and Cape Town each operate several hundred surveillance cameras covering various areas of the city, such as the Central Business Districts. Braamfontein has at least one CCTV camera installed at half of the street intersections. Private businesses are also expanding camera coverage in public spaces, as are private citizens. Suburban neighborhoods are pooling their own resources to install new smart camera networks to be maintained by private security forces.[123] Surveillance cameras are also being utilised by police on patrol. Police in Cape Town and Durban are rolling out a Microsoft patrol car solution that features cameras which can integrate with the Microsoft Azure cloud.[124]

In early 2019, many South Africans were caught off-guard by the announcement a private CCTV surveillance provider called Vumacam would "blanket Johannesburg" with 15,000 cameras. Vumacam has since announced it aims to expand the network to 100,000+ cameras.

In November 2019, I authored a *VICE News* article, "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa" that detailed Vumacam's rollout. The piece exposed racist dynamics linked to the AI-based video analytics, private security forces, and residential segregation.[125]

In the Johannesburg Central Business District (CBD), there are at least 450 CCTV cameras; in Nelson Mandela Bay, there are around 350; and in Cape Town, there are more than 1,500 cameras. The City of Johannesburg is presently piloting facial recognition for use on CCTV networks. Universities have installed new surveillance cameras in reaction to protests, and surveillance has been used against #FeesMustFall protesters in conjunction with police and private security forces.[126] Video data provides "eyes on the street" to law enforcement agencies and city authorities, who are building centralised "nerve centres" for surveillance-driven policing and "smart" city management.

CCTV networks now utilise sophisticated **Video Management Software** and **video analytics** to automate and manage video surveillance.[127] Very often, this includes license plate readers, behavior recognition, and object recognition. Facial recognition is also beginning to be used, especially in areas ideal for detecting faces, such as airports and the entry/exits points of train stations.

By harnessing the power of artificial intelligence, video analytics can sift through hours of video surveillance data to track persons or objects of interest, identify people by name, compile a record of their movements, and even flag "unusual behavior" that video analytics software deems "suspect" or "dangerous".

For surveillance centres to record and analyse what thousands of CCTV cameras are "seeing", they must utilise video analytics. Without video analytics, most CCTV footage is of minimal value, because there is too much footage for a staff of humans to watch. The City of Johannesburg is now implementing video analytics – including experimentation with facial recognition – in its CCTV camera network. Meanwhile, private security companies use Vumacam's smart camera network to spy on citizens across neighborhoods with video analytics. Use cases are spreading to retail and "smart" cities applications.

Cities across the world are also starting to offer **plug-in surveillance networks** – camera networks that allow individual residents or businesses to plug their cameras into a larger network of cameras to increase the scope of the camera networks. Some major cities outside of South Africa have already started the trend. The use of plug-in surveillance networks in South Africa would drastically expand the coverage of CCTV networks.[128]

Connecting surveillance cameras to the internet threatens public security. Vumacam and city authorities make use of cameras manufactured by China-based Hikvision, which has a history of poorly securing its cameras.[129] Yet Chinese cameras aren't the only ones vulnerable to attackers,[xvii] in part because it is generally difficult to secure software against all possible attacks. The expansion of networked CCTV cameras itself spreads the likelihood that public surveillance devices will be hacked by nation-states or other actors.

Surveillance data is frequently fed into *fusion centres* or *Real Time Crime Centres* that aggregate various repositories of surveillance data into a single intelligence station. In 2017, the Free State bid for a contract with India-based Tech Mahindra to build its own fusion centre, and it remains to be seen what data will be available to the law enforcement agencies in charge.

South Africa's Council for Scientific and Industrial Research (CSIR) has built its own complex surveillance platform called "Cmore" for policing rhino poaching and border patrol. Cmore has also been piloted for use by the South African Police Services (SAPS). The CSIR previously collaborated with the apartheid government to police the anti-apartheid movement.[130]

Within the surveillance industry, corporate giants like Axon (formally known as Taser) are developing video analytics for use on police body cameras. In 2015, the SAPS piloted the use of body cams in Cape Town. Recent research suggests that body cams do not reduce police violence.[131] In October 2019, the Durban Metro Police announced it partnered with Microsoft for "21st century" policing. Using the Microsoft Advanced Patrol Platform (MAPP) – an IoT platform for police cars that integrates surveillance sensors and database records on the Azure cloud – the Durban police will surveil their surroundings on the prowl in an effort to enforce "zero tolerance" policing. A facial recognition camera can be set up when the vehicle is stationary, and a 360-degree ALPR can scan up to 5,000 license plates per minute. A spokesperson for Microsoft SA said the solution is

xvii In 2018, for example, it was revealed that a major US-based camera manufacturer, Axis Communications, had critical security vulnerabilities in about 400 of its IP camera models. See Lindsey O'Donnell (18 Jun 2018). "Axis Cameras Riddled With Vulnerabilities Enabling "Full Control"," *Threatpost*, at: https://threatpost.com/axis-cameras-riddled-with-vulnerabilities-enabling-full-control/132888.

already rolled out in Cape Town. Microsoft recently opened Azure cloud centres in Cape Town and Johannesburg.[132]

South Africa also uses *grabbers* to collect cell phone data located within several kilometres of the grabber surveillance device. Grabbers can pinpoint a cellphone's precise location with no knowledge from the owner of the phone that the tracking is taking place.[133]

Diverse sources of physical, behavioral, demographic, and environmental data may be pooled into South Africa's emerging regional "nerve centres", such as Joburg's "Integrated Intelligence Operations Centre" (IIOC). The data repositories could then be used for predictive analytics and surveillance purposes by police and city administrators as a part of "safe" and "smart" city initiatives.

The spread of physical surveillance is justified in the name of fighting crime, private property rights, and managerial efficiency. Yet the drastic expansion of physical surveillance in publicly accessible spaces threatens civil rights and liberties.

Aside from Vumacam, there has been little public discussion of contemporary physical surveillance in the South African press or university publications.[134] There is no opting out of CCTV surveillance. Many human rights advocates believe that a society under constant surveillance is not a free society at all.

Solutions for Video Surveillance and Intelligence Centres

There aren't many ways to stop video surveillance with technology. People sometimes cover their faces and bodies in public, but you could face harsh penalties for covering your face at a protest gathering (see section 8.7 of the Regulation of Gatherings Act). Even if people were allowed to cover their faces as they please, it would be a poor solution to an undesirable problem.

Public discussion and activism are key to this issue. Civil society, lawyers, and policymakers should discuss the rapid spread of cameras in public settings and how the right to privacy in public should work in light of new technologies. (Laws covering other tracking devices, such as grabbers and Bluetooth beacons, should also be addressed.)

Some believe that South Africa's new data protection law, the Protection of Personal Information Act (POPIA), will fix the issue once it goes into effect. There is little reason to trust this. POPIA is already being interpreted to allow mass CCTV surveillance in public spaces, and it is loaded with weak provisions and exemptions (see Chapter 19).[135]

New legislation is needed to rein in CCTV surveillance and centralized surveillance centres. Some options include:

- Banning video analytics in publicly accessible spaces (perhaps with exceptions for rare cases, such as bodies on train tracks or safety in dangerous workplace scenarios).
- Banning plug-in surveillance networks and restricting the scope of networked cameras beyond the premise of a single site.
- Limiting the density of camera and other surveillance sensors in public.
- Banning centralised city intelligence centres and restricting the pooling of information for intelligence purposes.

16 Internet Decentralisation

Big Tech centralisation in the global internet

Over the past two decades, the structure of the internet changed. What began as a decentralised information system which allowed people to communicate without easy government and corporate censorship was quickly captured by state-corporate power. A handful of US-based transnational corporations, led by GAFAM (Google/Alphabet, Amazon, Facebook, Microsoft, and Apple), became the five richest corporations in the world, with a combined market value topping $5 trillion (R90 trillion).[136]

How did Big Tech corporations get so powerful?

The short answer is that US transnationals took over the *digital ecosystem* – software, hardware, and network connectivity.

Because US-based corporations own and control the technical architecture of the digital ecosystem, they can design it to exploit the global society. They use their power as infrastructure owners to shape the flow of information, extract rent, and monetise Big Data surveillance. They also use their resources to influence the law, control new innovations, and set the ideological frame for how a digital society should work. This process has led to a new, insidious phenomenon called **digital colonialism.**[137]

Internet Centralisation and the Rise of the Cloud

In the late 1970s and 1980s, personal computers spread to the general public in the middle and upper classes. Corporations like Microsoft built a business model to control technology for profit by licensing computer code as proprietary software. Software activist Richard Stallman began a movement to counter the power of proprietary software vendors with the invention of the GNU General Public License (GPL) and the founding of the Free Software Foundation. Free Software hit its first major milestone with the release of the GNU/Linux operating system in 1991. However, around the mid-2000s, Big Tech corporations began to change how the digital ecosystem works. A shift was made to host software services in "the cloud", which provided a foundation for Big Data surveillance and advances in artificial intelligence to emerge.

In simplified terms, clouds function as a collection of servers that provide products and services over the internet. Facebook, for example, operates via Facebook's cloud. When you use Google Search, Gmail, Instagram, Facebook, Twitter, or similar internet-based platforms, you are being fed data and services from their corporate clouds. These companies often utilise Free Software to run those services. However, if the product you are using is run off their cloud, they exercise authoritarian control over your experience – even if it is using Free Software – because you cannot

access or modify the software running on their physical servers. The public is subjected to how the corporation designs the user experience. For this reason, critics of the cloud say, "there is no cloud, just someone else's computer". Because you cannot control someone else's computer, using Free Software alone is not enough to protect our freedom.

Cloud services are typically used to centralise data collection. Facebook, for example, hosts your data in the Facebook cloud. To "share" your pictures, you upload them to the Facebook cloud, and your friends can only see the photographs after downloading them from the Facebook cloud. Facebook is a middleman between you and your friends.

As a result of this centralised social networking design, Facebook gets a copy of everyone's data. Moreover, when you access a Facebook service, it records everything you do: what you "like", what you click on, how long you look at a photograph, which ads you click on, and more. Facebook and other Big Tech services hosted on internet clouds now conduct 24/7 surveillance on all of us, and make money off of our data.

Centralisation of services on the internet is enormously threatening because the internet has a universal and open architecture that people across the world are free to access. The internet knows no borders, and preventing corporate services from operating inside your country typically requires draconian measures, such as China's "Great Firewall", to control which websites and services people inside the country can access. Centralised control of software and internet services has led to the authoritarian control of the "open" internet by US corporations and intelligence agencies. Internet centralisation is therefore inextricably connected to digital colonialism.

The Movement for Internet Decentralisation

In recent years, the Free Software community has developed a number of decentralised internet services that are growing in popularity. A decentralised internet service does not have one centralised authority – such as the company running it – that determines how the service works and spies on everyone. Instead, decentralised services rely on the federation of interoperable services. Data can either be stored and transmitted through a set of federated servers with no privileged, centralised service provider, or through peer-to-peer technologies by which users simultaneously host and transmit data on the network. Using Free Software to provide the services helps ensure the public can exercise control over how the services work. For the user, the services will provide the kind of experiences they are accustomed to for things like social networking, email, chatting, online calendaring, and more – but they will no longer be owned and controlled by "someone else's computer" in the cloud.

Decentralised internet services thus aim to transform centralised, cloud-based services into a democratic digital commons owned and controlled directly by the world's people.[138]

Solutions for Internet Decentralisation

Technologies that decentralise internet services and distribute ownership and control to users at the edge are necessary to abolish digital colonialism. While solutions are in development, I recommend that you begin using decentralised social networking services like Mastodon. More advanced users

can also experiment with technologies like FreedomBox. South African programmers and engineers can contribute to the development of these technologies, because they are based on Free and Open Source Software, or they can be funded to develop new solutions.

Decentralised social media: I recommend trying Mastodon because it is the most popular and polished decentralised social network available. It resembles Twitter, but does not centralise data or control into a single surveillance intermediary or serve ads.[139] Mastodon is part of the Fediverse, a collection of "interoperable" social networks that allow users to interact with and follow each other without signing up for multiple accounts. PixelFed (akin to Instagram), PeerTube (akin to YouTube), Pleroma (similar to Twitter and Mastodon), and diaspora* (similar to Facebook) offer additional alternatives.

- To join the most popular Mastodon server, visit: https://mastodon.social.
- To pick a different server with Mastodon, visit: https://instances.social.
- To join PeerTube, visit: https://joinpeertube.org.
- To join PixelFed, visit: https://pixelfed.org/join.
- To join Pleroma, visit: https://www.pleroma.com.
- To join diaspora*, visit: https://diasporafoundation.org.
- For a directory of Fediverse social networks, visit: https://fediverse.party. For statistics, visit: https://the-federation.info.

At present, Fediverse platforms are structured to allow those who own and operate various networks to surveil activity on their networks. This means that you have to trust the people who administer the network with your data. It would be better if there were even more decentralised ways to host and transmit data, so that there is no ability for others to see your data other than those who you explicitly intend to see it. One project, LibreSocial, is developing a social networking solution that provides a more private and secure peer-to-peer architecture. However, it is in a testing phase, and is not yet ready for use by the public.

Keep an eye out for the public launch of LibreSocial by visiting: https://libresocial.com.

While decentralised social networks are still in development, they are improving quickly. But unless most people start using them, many users will remain fixed to Big Tech platforms, because it's too hard to convince all your friends to leave Facebook, Instagram, and Twitter, and instead use something like Mastodon, PixelFed, or LibreSocial. It will take a global activist campaign against digital colonialism and internet centralisation to counter Big Social Media and other Big Tech services.

Grassroots activism: To decentralise internet services, activists and lawmakers need to press for commons-based solutions embodying principles of self-governance, decentralisation, and federation. The provision of internet services would be transformed from a profit-seeking enterprise into a global democratic commons. To make this reality, we also need to press governments to fund the development of public interest technology and provide the infrastructure needed to lower-income households. Funds for implementing social networks can be raised by taxing the rich and Big Tech. Resources for infrastructure and development should be extended to people in the Global South as reparations for colonialism, including recent revenue extraction through digital colonialism.

FreedomBox: To counter the general centralisation of internet services into corporate clouds, Columbia law professor Eben Moglen – a central lawyer for the Free Software Movement – proposed a "FreedomBox" solution in 2010. FreedomBox is Free Software designed to power a "personal cloud" server that would run in each household, as well as places like schools and work. You can install FreedomBox on a small, increasingly inexpensive device (~R450 at present) that stays inside your home. It can store your data as a personal cloud that you can access from any device using a safe username and password, even when you leave your home. It can also block ads and provide some of the infrastructure needed to decentralise internet services.

Initiatives like FreedomBox aim to "re-decentralise" the internet. A Free Software-based decentralised ecosystem would help slam the breaks on Big Data surveillance.

To be effective, technologies like FreedomBox will have to be used by millions of people. This means the technology must be user-friendly and available to everyone. FreedomBox is already equipped to run in developing world contexts: in 2019, FreedomBox developers worked with NGO Swecha to successfully implement FreedomBoxes in twelve Indian villages.[140]

Policymakers could subsidise research and development and implement decentralisation technology – along with education about how to use it – in public institutions like schools and universities.

While you can purchase a pre-loaded FreedomBox device, you can also install the FreedomBox software on your own device, such as a Raspberry Pi, desktop, or laptop computer.

- To download FreedomBox, go to: https://freedombox.org/download. Video instructions on how to install FreedomBox within five minutes is available on the website.
- For more detailed instructions, see: https://wiki.debian.org/FreedomBox/Download.
- To try a FreedomBox demo, go to: https://freedombox.org/demo.
- For a description of FreedomBox features, see: https://wiki.debian.org/FreedomBox/Features.
- For a list of supported hardware, see: https://wiki.debian.org/FreedomBox/Hardware.
- FreedomBone is a popular home server system based on FreedomBox that offers some of its own features. You can download FreedomBone at https://freedombone.net.

Riot offers a diverse, decentralised communications service that can be used as a standalone app or in your web browser. Riot looks and feels a lot like Slack. You can use the Matrix.org website's servers for data hosting, or you can host your own server to power the service. Riot is in the beta stage of development, and its audio and video chat do not run smoothly for the time being. Keep an eye out for progress in the future.

- To download the Riot app, visit: https://riot.im/download/desktop. To launch Riot in a browser, visit: https://riot.im/app. Riot is also available to install on your smartphone through F-Droid, APKpure.com, Google Play, and the Apple App Store.

17 Free and Open Source Software for Everyday Use

Proprietary software as digital colonialism

In 2008, *The Wall Street Journal* reported that Microsoft attempted to persuade (and pay) the Nigerian government to replace GNU/Linux with Microsoft Windows on thousands of school laptops.[141] The tactic is consistent with a broader strategy to ensure Microsoft's proprietary software is used on devices throughout the Global South. In 2007, it was reported that Microsoft "tolerated" the pirating of Microsoft Windows in China, a poor country with a per capita income similar to South Africa, to ensure Chinese computer users will become addicted to Microsoft products.[142]

Other corporations selling proprietary software sometimes offer "free" versions that limit the features people can use unless they buy the "full" version. This restricts the ability for people without disposable income to enjoy the full set of features because they cannot afford to pay for the software.

In the winter of 2013, I helped students with computer basics at Nombulelo Secondary School in Makhanda, Eastern Cape. Learners were using old hardware to run Microsoft Windows XP and low-quality proprietary software. The students had a blast drawing pictures, but they were using the basic, feature-poor Microsoft Paint software. They could have instead used feature-rich Free Software, such as the GIMP photo editor and a lightweight GNU/Linux operating system built to run efficiently on slow hardware. The teachers and students were not aware that high quality Free Software solutions are available.

Because Free Software grants people the freedom to share copies of the software without charging a price, it is freely available to the poor. The Free Software app, GNU Image Manipulation Program (GIMP), for example, is free to use, and has features similar to Adobe Photoshop, which costs $240 (R4,300) per year. GIMP is many times more interesting, powerful, and fun to use than the low-quality Microsoft Paint software students were stuck with at Nombulelo. Yet many people are not aware of Free Software alternatives to proprietary software, so they "pirate" proprietary software or use "free" versions that limit the features you can access without paying.

Free Software apps are often as good as or better than proprietary software. Moreover, Free Software provides communities with the power to control the software, which empowers them to remove malicious anti-features like surveillance, but also to customise the products (e.g. to their own language), modify them to incorporate new features (without having the reinvent the wheel), and develop them for the benefit of local communities instead of foreign corporations.

Thus, Free Software is valuable not only because it is critical to privacy and digital self-defense, but also because it provides equitable access to software and is well-suited to local economic development. The South African government has long recognised these benefits,[143] and they should be using Free Software in the public sector and cultivating its development (see Chapters 18 and 19).

Solutions for Everyday Applications

A wide variety of high-quality Free Software apps are available so that you can replace Big Tech's authoritarian, expensive, and surveillance-oriented software with empowering alternatives.

Free Software apps are usually just as good or better than proprietary alternatives. For example, you may find interesting features in the GNU/Linux OS that are not available in Microsoft Windows or Apple MacOS.

There are too many Free Software apps to list in this guide, but you can always search the web for '"Free and Open Source Software" or "Linux" and the kind of app you are seeking out. For example, if you search for "Linux video editing software" you will find a website recommending apps to try. When installing an app on Linux, you may want to search for "how install *xyz* on Linux", where "*xyz*" is the specific app you are looking for.

On GNU/Linux, apps can often be installed easily from the app store (e.g. apps like "Software Store" or "Synaptic") or from the shell (terminal). Search the web to learn how to use these features so that installing your apps is quick and easy.

For a large catalog of Free Software alternatives to proprietary software, visit the Switching.software website: https://switching.software.

Here are some Free Software apps that meet your everyday needs:

LibreOffice is an office productivity suite. It offers an alternative to Microsoft Office 365. Files can be saved in open document format (.odt) or in other formats, such as Microsoft Word DOC (.docx).

- To download LibreOffice on the desktop/laptop, go to: https://libreoffice.org. On the phone, install LibreOffice Viewer from F-Droid or Google Play.

Video Games: Gamers in the Free Software community typically use Steam to download and play video games.

- For a guide on gaming, see: https://itsFreeSoftware.com/linux-gaming-guide.

GIMP is used for photo editing. It offers an alternative to Adobe Photoshop. (If you like the Photoshop interface, be sure to "dock" the windows the first time you use the application, under Windows > > Single-Window Mode.)

- To download GIMP on the desktop/laptop, go to: https://www.gimp.org/downloads.

Inkscape is for professionals looking to draw and sketch for use cases like website design. It offers an alternative to Adobe Illustrator.

- To download Inkscape, go to: https://inkscape.org/release.

Okular is used to read and highlight PDFs. It offers an alternative to Adobe Acrobat, though it is not as feature-rich as Acrobat Pro.

- To download Okular, go to: https://okular.kde.org/download.php.

MuPDF is used to read PDFs on the desktop/laptop and smartphone.

- To download MuPDF, go to: https://mupdf.com/downloads/index.html. On the phone, install from F-Droid, Google Play, or Apple App Store.

Audacity is used to record and edit audio files. It offers an alternative to Sony Soundforge.

- To download Audacity, go to: https://www.audacityteam.org/download.

OBS Studio is used to live stream media, such as a music performance or talk show.

- To download OBS Studio, go to: https://obsproject.com/download.

Kdenlive is used to edit videos.

- To download Kdenlive, go to: https://kdenlive.org/en/download.

VLC Media Player is used to play media files and is especially good for video.

- To download VLC Media Player, go to: https://www.videolan.org/vlc/index.html. On the phone, install from F-Droid, Google Play, or Apple App Store.

Clementine is used to play audio files like MP3s.

- To download Clementine, go to: https://www.clementine-player.org/downloads. On Android, Clementine Remote allows you to control the desktop/laptop app from your phone. You can install Clementine Remote from F-Droid or Google Play.

Kazam is used to capture the video and audio of your computer screen.

- To download Kazam, go to: https://launchpad.net/kazam.

Deluge is used to download torrent files used for file sharing. To learn about file sharing, search the web for "how to download files using torrents" in DuckDuckGo.

- To download Deluge, go to: https://dev.deluge-torrent.org/wiki/Download.

Calibre is used to open ebooks, and is especially good for .epub and .mobi file formats.

- To download Calibre, go to: https://calibre-ebook.com/download.

Book Reader is an ebook reader.

- On the phone, install Book Reader from https://apkpure.com, F-Droid, or Google Play.

18 Public Education: A Key Battleground

Surveillance and product placement in schools

In 2015, then-President Jacob Zuma announced Operation Phakisa for Education (OPE) – an initiative to fast-track digital technology into all public schools. A two-week "scoping lab" was hosted by the World Bank that June, followed by a four-week "main lab" hosted by Deloitte in September. The main lab featured 120 participants, including members of government, teachers, Big Tech corporations, labor, and nonprofits, among others. Participants were bounded by non-disclosure agreements. My doctoral dissertation, *Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley*, published in 2019, provides the only thoroughgoing account of the programme on record.[144]

By 2019, Basic Education Minister Angie Mothshekga stated that the experimental phase of tech rollouts to schools was completed, and the government plans to deliver one computer device to each learner in all public schools. In his 2019 State of the Union speech, President Ramaphosa said the government aims to complete the rollout to all public schools within six years.[145]

By using computers for learning and administration, the government plans to "transform" public education. The Department of Basic Education (DBE) has built a DBE Cloud (http://www.dbecloud.org.za), and seeks to conduct "longitudinal" analytics in education. In the most expansive version of this, learner behavior would by tracked by the government and corporations from childhood into adulthood. Using mass surveillance, performance could be evaluated at each stage of development in granular detail to determine how to manage the education system across generations. When doing research on OPE in Pretoria, one government official at the then-Department of Telecommunications and Postal Services told me the government would like to include learners' web browsing cookies in their analytics. Teachers will likely be assessed by education analytics, either directly or by proxy through accounts of learner behavior.

Government cloud surveillance will almost certainly be developed in partnership with Big Tech corporations like Microsoft, Google, and Pearson.

Education technology programmes aim to radically alter the norms of "brick and mortar" education. Popular e-education initiatives include blended learning (the mixing of computer technology with traditional learning), flipped classrooms (the "flipping" of expository learning to after-school and homework to in-school class time, often mediated through technology), and adaptive learning (artificial intelligence software powered by Big Data surveillance).

Under apartheid, teachers were "inspected" by outside observers to enforce compliance with the apartheid agenda. Today, teacher surveillance may return with a vengeance through cloud-based surveillance services.

To this end, the Michael & Susan Dell Foundation has launched the Data Driven Districts Dashboard – an educational dashboard system with the eventual capacity for detailed surveillance of teachers and learners in the classroom.[146] (Visit http://www.datadrivendistricts.co.za to see how the system works.)

Discussions about e-education is usually limited to education-specific software, such as the DDD Dashboard or the Canvas learner management system. However, there is much more to the story of tech in education. Even if education-specific software were not used, the use of Big Tech products like Microsoft Windows and Google Android on learner devices is deeply problematic, for a number of reasons.

First, product placement in schools will deepen the stranglehold of corporations like Microsoft and Google over South African society. Students will become accustomed to their software, and will likely prefer to keep using Big Tech products throughout lives.

Second, the future generation of software developers will likely seek to build products for the software ecosystems they grow up using. If they are using Microsoft and Google, then the future of software development will be biased towards products built for software platforms offered by Microsoft and Google.

Third, Big Tech software forcefully subjects students and teachers to corporate and state spying. If schools provide students with devices pre-loaded with Microsoft Windows or Google Android, then South African students will have lifelong profiles archived by Microsoft and Google, with access available to US intelligence. This violates the autonomy of children and teachers, and normalises the idea that being spied on all the time is acceptable. Moreover, once children become aware of the corporate and state surveillance infecting their devices, many will become more conformist due to chilling effects.

It is critical that People's Tech is used in the education system instead of Big Tech products and services. Around the world, there are pockets of Free Software deployments in the public education system. In August 2008, the State of Kerala, India, instructed all institutions under the General Education Department to strictly use Free Software alone in all future teaching and training activities. The Kerala Infrastructure and Technology for Education (KITE) has developed several Free Software applications, including a customisation of BigBlueButton for e-learning and online classes.[147]

South Africa is well-positioned to commit to implement Free Software now, because most public schools have yet to deploy computers in the classroom. If contracts are doled out to Big Tech corporations and school participants trained on Big Tech software, it will be more difficult to reverse course.

Solutions for Public Schools and Universities

Schools are a key battleground for South Africa's digital society. In the 21st century, there can be no decolonisation of education, economy, or society without the decolonisation of technology.

People's Tech should be pre-installed on learner and teacher devices. Schools should be free of corporate and state surveillance. Children need the freedom to develop their thinking without fear of reprisal or judgment. A free people are not herded along paths predetermined by bureaucrats conducting longitudinal data analytics. Commercial, government, and educational software should not continuously collect data about learners or teachers, even if it is strictly used for educational purposes.

Because the source code in Free Software can be read, studied, and modified, it is ideal for education: anyone can use it without paying, anyone can learn how the software works, and anyone can experiment with modifying the software. The South African government adopted a Free and Open Source Software policy preference in 2007, yet it has not put it into practice. Civil society and activists should pressure the government to ensure Free Software is used in schools.

Personal clouds like FreedomBox could be installed in schools. These could be used to protect privacy and to teach children the basics of networking and privacy software. Students and schools could also make use of decentralised social networks in the Fediverse.

A quality education technology programme will do more than provide devices to education participants and teach learners to code. It will also teach learners about the politics of Free Software and digital colonialism. It will teach them the value of privacy and the need to develop technologies of freedom.

Most of the South African population lives below the poverty line of about 33 Rand per person per day.[148] The state is currently needed to subsidise devices like laptops and tablets to the masses. The software that comes pre-loaded on devices will have a powerful influence on South Africa's political, economic, social, and technological trajectory.

It is essential to provide empowering technology to the youth, together with education about technology and freedom.

19 Digital Socialism: The Antidote to Digital Colonialism

Who rules digital South Africa?

With each passing day, South African authorities in government, business, and higher education trumpet the so-called "Fourth Industrial Revolution", which promotes the latest technologies produced by Big Tech. These authorities also advocate the use of Big Data and artificial intelligence to profile, evaluate, and manage human interactions. They are endorsing a surveillance society.

In 2013, the government enacted South Africa's data protection law, the Protection of Personal Information Act (POPIA). The law is said to protect South Africans from harms committed by those processing their data. POPIA will commence (i.e. come into effect incrementally), beginning in July 2020.

In 2019, one of the information regulators responsible for interpreting and enforcing POPIA, Collen Weapond, opined that Vumacam's all-seeing smart camera network should be permissible under POPIA. While the interpretation is not final, if it stands over time, it would mean that POPIA is so weak that it cannot even prevent a company from filming you everywhere you go in public space.

Yet leadership has done more than simply endorse surveillance technology. They are embracing and advocating digital capitalism – a digital economy based on private ownership and control over the means of computation – led by Silicon Valley corporations, who are colonising the tech ecosystem. In most parts of the world, US-based transnational corporations dominate the digital ecosystem, including search engines (Google); web browsers (Google Chrome); smartphone and tablet operating systems (Google Android, Apple iOS); desktop and laptop operating systems (Microsoft Windows, macOS); office software (Microsoft Office, Google G Suite); cloud infrastructure and services (Amazon, Microsoft, Google, IBM); social networking platforms (Facebook, Twitter); transportation (Uber, Lyft); business networking (Microsoft LinkedIn); streaming video (Google YouTube, Netflix, Hulu); and online advertising (Google, Facebook) – among other products and services.

In 2016, the City of Johannesburg announced a partnership with Microsoft South Africa to train one million residents in digital literacy skills. Computer skills taught include how to use Microsoft software like Office 365. This violates the Free and Open Source Software policy preference passed in 2007, and demonstrates that its stipulations for a mere "preference" were too weak to stop the march of digital colonialism.

Let us begin this chapter with a simple observation: no country will ever become wealthy when the critical infrastructure powering its economy is owned and controlled by foreign corporations. South Africa's modern history arises from a European-led invasion by the Dutch East India Company, who stole the land and brutally exploited the indigenous people for profit. Critical infrastructure and resources – railroads, mines, industrial equipment, housing, and land – were dominated by white settlers at the expense of the African people.

White authorities also waged psychological and conceptual warfare on the population through the imposition of colonial interpretations of religion, culture, and political economy. Bantu education sought to instill passivity and acceptance of race and class-based inequality.

Today, US-based corporations are colonising digital technology. Instead of taking over the land, they are colonising critical digital infrastructure and human knowledge. They seek to own the world's knowledge and culture (intellectual property), the material infrastructure (cloud server farms, transoceanic cables, and other hardware), the code powering computers (software), and information about people and nature (data). Converting knowledge into private property is foundational to their system of domination.

When Big Tech corporations do share knowledge, it is done in ways beneficial to themselves. Google and Facebook, for example, are happy to "open source" some of their artificial intelligence software (e.g. Tensor Flow and PyTorch) because they use it to monetise Big Data surveillance.[xviii] Yet if their access to surveillance data were shut out by new technologies and privacy laws, they would close off much of their "open source" technology and increase the share of proprietary code in the software market. The problem we face today is digital capitalism and authoritarianism, not simply surveillance capitalism.

As I previously wrote in the *Mail & Guardian*, the Fourth Industrial Revolution (4IR) narrative claims Big Data, intellectual property, centralised clouds, the Internet of Things, "smart" cities littered with surveillance, automation, algorithmic decision-making, Big Tech corporations, and surveillance capitalism are the way of the future. A creation of the ultra-capitalist World Economic Forum (WEF), the 4IR concept is an elite construct which serves a useful purpose at the periphery of empire by steering inquiry about tech into the WEF agenda. Like the colonial missionaries of past, they preach a new religion, the 4IR, as the saviour of society.

Not surprisingly, the tools they promote are the tools of the masters: corporate ownership, intellectual property, centralised clouds, Big Data surveillance, the profit incentive, and private production for the market. This will not work for the common person. As Audrey Lorde put it, "the master's tools will never dismantle the master's house".[149]

The threat of proprietary technology – and the selective sharing of knowledge by corporations – was captured by Archbishop Desmond Tutu, who stated in 2007:

> *Freedom is an ongoing process, and not an end in itself … We are not shy to use the word freedom, and do so in contexts where its importance is not always recognised. In a digital world, there are many threads to a hard-won liberty. There are those who take our ideas and lock them up for*

xviii Tellingly, Google and Facebook will not license the software under a copyleft license, which would ensure that the software remains free and open to the public. See Keith Curtis (17 Feb 2018). "PyTorch Should Be Copyleft," at: http://keithcu.com/wordpress/?p=3847.

business gain. There are those who will take the fruits of the human mind and lock them up, dishing them out to us in meted amounts for a fee that locks most of our people out. And there are laws that are reserved for business reasons and changed to rob society of its own rights ...

To paraphrase Edmund Burke, who said, 'the only thing necessary for the triumph of those who take away our freedom in the digital world is for organisations [like universities] to do nothing.' But there are people, like our keynote speakers … who are not content to do nothing. Indeed, there is a whole movement that is rapidly gaining momentum worldwide arising out of the work of people like Free Software Foundation founder Richard Stallman, creating socially responsible businesses out of the very freedoms that we are talking about. Free Software and Open Source, Free and Open Resources for Education, new ways to create and share cultural artifacts such as music, writing, and art – all of these are changing the world for the better.[150]

Unfortunately, intellectuals who believe themselves to be "critical" of Big Tech have formulated a liberal imperialist narrative called the "techlash" that fails to address digital colonialism. These US-Eurocentric "critics", drawn from elite Western university and media outlets, ignore the centrality of property and the Free Software Movement. Much like the Sullivan Principles during apartheid,[xix] their solutions offer minor reforms that maintain US interests, such as weak privacy laws, "competitive markets" created through antitrust, and corporate ownership of the digital ecosystem. The "techlash" extends Francis Fukuyama's "end of history" to tech, where nothing fundamentally different can occur other than what we have seen in the West.[151]

If we are going to create a society that prioritises freedom and equality, we will have to develop a new framework to restructure the digital ecosystem. This requires more than the array of Free Software technologies outlined in this guide. We must also have supportive laws, critical education, and a grassroots movement to counter digital colonialism and replace it with a democratic digital commons owned and controlled directly by the people. There is no way around this.

Laws like POPIA are designed to safeguard surveillance capitalism. This can be seen in its provisions that allow Big Data surveillance to flourish with mild restrictions said to "protect" your privacy. Under POPIA, exemptions include data processed for national security, such as "defense or public safety", instances in which "the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject", and instances where the processing provides "a clear benefit to the data subject or third party that outweighs … interference with [their] privacy". The "public interest" includes "national security", "the prevention, detection and prosecution of offences", "important economic and financial interests of a public body", and "historical, statistical or research activity" (as well as the "special importance of the interest in freedom of expression").[152]

POPIA also allows people to "consent" to Big Data surveillance through terms and conditions, defined as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information." Yet we know that nobody can read these terms and conditions, even if they wanted to. One study showed that the average person would have to spend about 76 working days per year to read the Terms and Conditions of the websites they visit.[153]

xix The Sullivan Principles were introduced in 1977 by Reverend Leon Sullivan, a board member of General Motors, as a set of "corporate social responsibility" principles forming a "code of conduct" for US corporations operating in apartheid South Africa. Activists opposed the Sullivan Principles as corporate propaganda that perpetuated the apartheid system. Sullivan abandoned the principles in 1987 and joined those calling for total divestment.

Google South Africa sent me about 20,000 words of "terms and conditions" covering the Google technologies used in South African schools. Users can either "consent" to Google's data processing, or they can't use its technologies at all.

Forcing people to endure surveillance just to visit a website, join a social network, or use a weather app, on the basis that they "consent" is unjust. Yet POPIA does not appear to prohibit this "take it or leave it" surveillance society.

Digital capitalism has a business model crisis. It concentrates and extracts wealth, cedes authoritarian control over digital experiences to transnational corporations unaccountable to the public, and subjects users to surveillance, advertising, and manipulation. If it moves to a "pay-for-ethical-treatment" model, it will generate class inequality, especially for the poor who have no disposable income.

In a commons-based system of digital socialism, knowledge is free and open for all to consume, modify, and share. Free Software, interoperability, federated services, and decentralisation tools provide the public with the means to own and control their experiences. To support the global commons, production and maintenance of digital technology and culture could be paid for by the rich through progressive taxation and heavy taxes on Big Tech corporations. This requires a Tech New Deal that transforms the digital ecosystem from a profit-seeking enterprise into a publicly funded global commons. A movement for digital socialism dovetails with efforts to build an environmentally sustainable global economy based on wealth redistribution and equality, not limitless growth.[154]

Many of the core technologies powering the digital revolution were funded by the state, including computers, the internet, and GPS. The state also supports the education of computer scientists and engineers. Research and development institutions like the CSIR could help develop decentralisation technologies like FreedomBox instead of surveillance systems like Cmore. University researchers could work on voice assistants like Almond, which does not spy on its users, as they are doing at Stanford University. With enough funds from taxes, talented developers could be awarded comfortable middle-class salaries to work on public interest technologies, instead of joining exploitative institutions like Google and Microsoft, who pay researchers a few million rand per year.

As noted in previous chapters, government policy can require the use of People's Tech in schools, universities, and the public sector; protect user privacy; and teach people about tech freedom.

But none of this will occur without you. Technology corporations have concentrated enormous sums of wealth into the hands of a few, and they will not give it up without a serious fight. It doesn't help that elected representatives are tempted to exploit corporate tech for their own surveillance and control.

Nhlanhla Mabaso, a champion of Free Software, headed the Open Source Centre – since renamed the Meraka Institute – at the CSIR. ("Meraka" is Sotho for "open grazing land".) In a research interview, Mabaso told me some of his colleagues argue the government's Free and Open Source Software policy preference means "open source is law" in South Africa. Efforts by Mabaso and his peers once aimed to undermine the power of corporations like Microsoft from colonising the South African tech ecosystem.

Decades earlier, anti-apartheid activists protested against the use of computers from tech corporations like IBM to facilitate the apartheid system. They eventually forced IBM to withdraw its business operations from South Africa.[155]

During the struggle against apartheid education, Zwelakhe Sisulu asserted:

> *We are not prepared to accept any 'alternative' to Bantu Education which is imposed from above. This includes American or any other imperialist alternatives designed to safeguard their selfish interests in the country, by promoting elitist and divisive ideas and values which will ensure foreign monopoly exploitation continues.*[156]

Only through democratic institutions and committees could students, parents, and teachers take control of their own education. "We are fighting for the right to self-determination in the education sphere as in all other spheres … It has become a struggle of the whole community with the involvement of all sections of the community", Sisulu said.

In the neoapartheid era, a new wave of US tech transnationals are pushing oppressive products into the country once again. A People's Tech movement to kick Big Tech out of Africa could form a critical part of the global protests against the enduring legacy of racism and colonialism. Activists across the world could unite to form a targeted boycott, divestment, and sanctions (BDS) movement centered on Big Tech corporations and their supporters in the United States.

South African communities are tasked to build a digital ecosystem that the people own and control, so they are not subjects of American or any other imperialist powers. People's Tech for People's Power, a holistic solution based on a Free and Open Source technology commons, socialist legal solutions, people's education, subsidies for public interest technology, and a vigorous grassroots movement, is urgently needed to avert disaster and build a truly democratic and egalitarian society.

20 Conclusion: People's Tech for People's Power

In order to defend our privacy and ensure that technology serves our best interests, we must have a critical understanding of tech and privacy, a willingness to try new things, and collective solutions for our digital future. Digital colonialism – the use of technology for political, economic, and social domination – is a new force spreading across the Global South. Surveillance capitalism is a core pillar, but as we saw in this guide, there are things you can do to protect yourself.

Ultimately, the digital society must be restructured to into a global commons, based on principles of equality, self-governance, decentralisation, and federation. This kind of digital society is a form of digital socialism based on libertarian socialist principles that reject ownership and control of the digital ecosystem by *both* government and the private sector in favor of direct ownership and control by the people.[157]

This guide focused a great deal on privacy. In each chapter, it provided examples of how corporations and governments are exploiting surveillance and colonising the digital economy, and what you can do to counter them. These solutions prove that a different world is possible.

In the 1980s, anti-apartheid activists created a movement called "People's Education for People's Power". In the digital age, *People's Tech for People's Power* is absolutely essential to a future where technology serves the people, not those with power.

Most of the software in this guide can be used by a beginner. Signal, Wire, and Jitsi are just as easy to use as WhatsApp and Skype, for example. Some options take more effort, but they enhance our individual and collective freedom.

Rather than trying to use the apps in this guide all at once, I recommend you pick a few and try them out. Ask your friends to try them with you. Take it one step at a time. Search online for help when something doesn't work as expected. Join an online discussion forum like Reddit or Ubuntu Forums (https://ubuntuforums.org) if you cannot find an answer. Often times, people will help you out. Tech-savvy individuals looking to construct an independent South Africa can build their own internet forums in African languages to help communities learn in their native languages.

A new world is possible, and it will have to include technologies that feature *freedom by design*. This world will not be gifted by policymakers or enlightened corporations. It will be built by a movement. The people of the world must unite and seize the means of computation if they are to have true democracy and equality.

I hope that you found this guide useful. For feedback or questions, please reach out to:

Right2Know: http://www.r2k.org.za/contact-us
Michael Kwet: r2kguide@protonmail.com

Appendix A: Software Recommendations

Texting and Chatting

- Signal
- Wire

Web Browsing

- Tor
- Firefox (with extensions)
- Chromium (with extensions)

Searching the Web

- DuckDuckGo
- Qwant
- Search in Tor

Sharing Files

- OnionShare
- Firefox Send
- Riseup Share
- SecureDrop
- NextCloud

Email

- ProtonMail
- Tutanota
- Mozilla Thunderbird with Enigmail
- FairMail
- K-9 Email

Video Chat

- Jitsi
- Signal
- Wire
- BigBlueButton

Online Document Collaboration

- Riseup Pad
- CryptPad

Personal Data Encryption

- Full Disk encryption (usually through the operating system)
- VeraCrypt
- Cryptomator

Passwords

- Wisely chosen password strategy
- KeyPassXC
- Firefox and Chromium password managers
- Bitwarden

Phishing

- Awareness of common phishing scams
- Be cautious: Call or email someone directly when in doubt
- ClamAV antivirus

Operating Systems

- GNU/Linux (e.g. Ubuntu, Xubuntu, Mint) (desktop/laptop/tablet)
- LineageOS (smartphone/tablet)

App Stores

- Software Center (GNU/Linux)
- Synaptic Package Manager (GNU/Linux)
- F-Droid (Android)

Internet Decentralisation

- Mastodon
- PeerTube
- PixelFed
- Pleroma
- diaspora*
- LibreSocial
- FreedomBox
- FreedomBone
- Riot

Everyday Use

- LibreOffice
- GIMP
- Inkscape
- Okular
- MuPDF
- Audacity
- OBS Studio
- Kdenlive
- VLC Media Player
- Clementine
- Kazam
- Deluge
- Calibre
- Book Reader

Public Education

- People's Tech
- Moodle
- BigBlueButton

Appendix B: Glossary of Terms

A **definition** is that which is individually necessary and jointly sufficient. Most terms cannot be so easily defined. The definitions below provide rough approximations of terms that refer to complex underlying realities.

Anonymity: This refers to secrecy about who is sending and receiving messages, even when what is said in those messages is not secret.

Autonomy: The ability to control your interactions without unwanted interference. Autonomy is achieved when you have both secrecy and anonymity.

Big Data: The use of enormous amounts of data to assess, predict, and manipulate behavior. In this guide, Big Data refers to data about humans.

Chilling effects: When the fear of surveillance discourages freedom of expression.

Cloud: A cloud is a utility computing model that can remotely store data, scale, and perform computations for a client on-demand, independent of their location.

Content: The information expressed in a communication, such as the text messages, pictures, words spoken over the phone, and image stream in a video chat.

Decryption: A method of de-scrambling encrypted data so you can read it.

Digital capitalism: A digital economy based on proprietary technology and private ownership and control over the means of computation. Corporations dominate digital capitalism.

Digital colonialism: The use of digital technology for political, economic, and social control of a foreign territory. Digital colonialism is principally achieved through the ownership and control of the digital ecosystem, which allows owners to design the technology for domination. Other factors include the resources to hire lobbyists to influence the laws according to imperial interests, the financial capital to marshal economies of scale, the exploitation of cheap labor, and the capacity to hire many of the most talented developers and acquire competitors.

Digital socialism: A commons-based digital economy powered by Free and Open Source technologies and data repositories directly owned and controlled by the global public. Under digital socialism, the people own and control the means of computation.

E-Education: The use of computers in education. In South Africa former President Jacob Zuma launched Operation Phakisa in Education, a secretive plan to fast-track computer technology to all R-12 public schools. The current government aims to reach all students within the next six years.

Encryption: A method of scrambling the content of your data to prevent other people from accessing it.

End-to-end encryption: A method of encryption in which the message is encrypted by the sender so that a third party, such as a spy or a company providing an app or communications service, does not have the means to decrypt the message. The only people who can read the message are the people communicating.

Fediverse: A collection of interoperable, decentralised social networks developed by the Free Software community that allows users to interact with and follow each other without signing up for multiple accounts.

Free Software (also called Free and Open Source Software): Software licensed to provide users with the freedom to use, study, modify, and share copies of the software. Access to the source code – the human-readable computer code that determines what a computer does – is a necessary precondition.

Free and Open Source Software policy preference: Passed in 2007, the South African Cabinet stated the government is obligated to give preference to Free and Open Source Software for use and development in the public sector.

Full disk encryption: The application of encryption to an entire hard drive including the data files and software.

GNU/Linux: A Free and Open Source operating system based on the GNU software tools developed by Richard Stallman and the Linux kernel developed by Linus Torvalds. Many people call this Linux for short.

Hacker: A savvy computer programmer that uses technical knowledge to solve a problem. In popular usage, the term refers to a person who uses their computer skills to break into computer systems. White hat hackers do this for benevolent purposes, black hat hackers do this for nefarious purposes, and gray hat hackers may violate ethical standards, but do not have the malicious intent of black hat hackers.

Metadata: Information about a person's communication, such as who is called, when the call was made, how long the conversation lasted, a person's physical location, or a website visited.

Multi-factor authentication: When two or more authentication procedures are used to grant access to an account or service.

Passphrase: The sequence of words used to bolster your password by lengthening the amount of characters used.

Password manager: Software that manages your set of passwords for you.

People's Tech for People's Power: A digital ecosystem based on a Free Software and internet decentralisation, supported by socialist legal solutions, critical education, grassroots movements, and bottom-up democracy.

Phishing: The use of fraudulent practices to induce individuals to reveal person information, such as passwords or credit card numbers.

Plug-in Surveillance Networks: Surveillance networks that allow various entities to pool their surveillance devices into a broader network. Devices such as CCTV cameras are often provided by private sector actors, such as businesses and households, to public networks which may be operated by police or city administrators for "safe" and "smart" city initiatives.

Privacy: This has three components: secrecy, anonymity, and autonomy. Privacy is essential to liberty because people conform to the status quo and the expectations of others when they know they are being watched.

Secrecy: A situation where what you say in messages is only known to those who intend to receive them.

Security through obscurity: The use of security design to maintain secrecy by obscuring the ease of discovering your secret. This is akin to hiding your money under your bed. The strategy does not provide strong privacy protection, but it may be good enough for a relatively low-risk use case.

Smart camera network: The use of video analytics and Video Management Software to perform complex analytical tasks on data provided by CCTV networks, potentially in combination with data from other sources and sensors.

Social engineering: The use of deception to trick individuals into divulging personal information. Social engineering is often used for phishing attacks.

Surveillance capitalism: The use of Big Data to assess people and predict their behavior, in order to manipulate them for profit, exploitation, and control. Surveillance capitalism can be conducted by corporations for profit, but it is also carried out by the state for population control. The term was coined in 2014 by a collection of intellectuals writing for the Marxist magazine *Monthly Review*.

Threat model: The process of identifying and modeling how to approach surveillance and security threats. This helps individuals make choices about how to protect themselves against surveillance.

Video analytics: Computer software that detects motion, behavior, faces, or objects. It may also detect anomalous behavior in a scene watched by a camera for a fixed period of time.

Video Management Software: The software typically used to manage large networks of surveillance cameras.

Appendix C: Additional Resources

Discussions about privacy and digital colonialism should be made mandatory in schools and universities, and given greater coverage in the media. The material covered in this guide offers a great starting point.

This guide was designed with fundamental privacy and security principles in mind, which will keep it relevant for some time. That said, technology moves fast. New software is created, old apps become outdated, and new services take off. Metadata policies, the discovery of security vulnerabilities, and other features can change quickly. Be wary of the dates that recommendations or news stories are written.

Searching the internet can help you answer questions. Searching for things like "how Signal stores your conversations" or "criticisms of BitLocker" will help you build a greater understanding of the technologies available.

Here are some additional resources worth checking out:

- **Switching.software** has a top-notch guide to alternatives to for commonly used apps and services, based on Free Software and good ethics: https://switching.software
- **PrivacyTools.io** offers a website with a wide variety of software recommendations: https://www.privacytools.io
- **CryptoHarlem** offers a list of several high-quality security training guides: https://medium.com/cryptofriends/digital-security-training-resources-for-security-trainers-spring-2017-edition-e95d9e50065e
- **Security in a Box** has excellent how-to instructions on privacy software: https://securityinabox.org
- **The Electronic Frontier Foundation** has a popular guide on digital self-defense: https://ssd.eff.org/en/module-categories/basics
- They also offer a guide on self-defense for border crossing to and from the United States, from 2017: https://www.eff.org/wp/digital-privacy-us-border-2017
- Here is their **Security Education Project**, with free training materials: https://sec.eff.org
- **The Freedom of the Press Foundation** has several useful guides on its website: https://freedom.press/training
- See also a list of guides and resources compiled by Freedom of the Press Foundation's Martin Shelton: https://medium.com/@mshelton/current-digital-security-resources-5c88ba40ce5c

Endnotes

Note: Wherever possible, the links in this guide were backed up at https://archive.org and https://archive.is. If you click on a link and the page is no longer online, enter the URL (web address) at one of those two websites and the web page should be available there. If some websites limit how many articles you can view, try clearing your browser cookies or installing the "Bypass Firewalls" browser extension for Firefox or Chrome at: https://github.com/iamadamdev/bypass-paywalls-chrome.

1 For an overview of digital socialism, see Michael Kwet (2019). "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley," PhD Dissertation, Rhodes University, Chapter 3, at: https://ssrn.com/abstract=3496049.

2 See *BusinessTech* (7 Aug 2018). "Here's how the South African government could be using your phone to spy on you," at: https://businesstech.co.za/news/telecommunications/263691/heres-how-the-south-african-government-could-be-using-your-phone-to-spy-on-you.

3 See Simnikiwe Mzekandaba (8 Sep 2015). "Grabber used for National Security," *ITWeb*, at: https://www.itweb.co.za/content/gxnklOvzZ1Jv4Ymz; Shaun Swingler (1 Sep 2016). "Meet the Grabber: How government and criminals can spy on you," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2016-09-01-meet-the-grabber-how-government-and-criminals-can-spy-on-you-and-how-to-protect-yourself.

4 For a visual explanation, see *Electronic Frontier Foundation* (no date). "Cell-Site Simulators/IMSI Catchers," at: https://www.eff.org/pages/cell-site-simulatorsimsi-catchers. See also, Kim Zetter (31 Jul 2020). "How Cops Can Secretly Track Your Phone," *The Intercept*, at: https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking.

5 See Heidi Swart (11 Oct 2017). "Social Media: Big Brother, and his brother, are watching you via data mining," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2017-10-11-social-media-big-brother-and-his-brother-is-watching-you-via-data-mining; Heidi Swart (20 Oct 2017). "Social media surveillance may not just be urban legend," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2017-10-20-op-ed-social-media-surveillance-may-not-just-be-urban-legend; Heidi Swart (25 April 2018). "Government surveillance of social media is rife. Guess who's selling your data," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2018-04-25-government-surveillance-of-social-media-is-rife-guess-whos-selling-your-data.

6 See Michael Kwet (27 Jan 2020). "The Rise of Smart Camera Networks, and Why We Should Ban Them," *The Intercept*, at: https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks.

7 See, among others, Michael Kwet (22 Nov 2019). "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa," *VICE News (Motherboard)*, at: https://www.vice.com/en_us/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa; Michael Kwet (3 May 2017). "Apartheid in the Shadows: the USA, IBM and South Africa's Digital Police State," *Counterpunch*, at: https://www.counterpunch.org/2017/05/03/apartheid-in-the-shadows-the-usa-ibm-and-south-africas-digital-police-state; Dale T. McKinley (2016). "New Terrains of Privacy," *Right2Know*, at: http://www.r2k.org.za/wp-content/uploads/Monograph_New_Terrains_of_Privacy_in_South_Africa_2016.pdf; Nóra Loideain (2017), "Cape Town as a Smart and Safe City: Implications for Governance and Data Privacy," *Legal Studies Research Paper Series*, Paper No. 41/2017, p. 13, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035336; Jane Duncan (25 Feb 2018). "Op-Ed: What Ramaphosa needs to do to fix state spying, Part 4 – 'smart' policing

and CCTV surveillance," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2018-02-25-op-ed-what-ramaphosa-needs-to-do-to-fix-state-spying-part-4-smart-policing-and-cctv-surveillance; Heidi Swart (5 Oct 2018). "Controlling Cape Town: The real costs of CCTV cameras, and what you need to know," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2018-10-05-controlling-cape-town-the-real-costs-of-cctv-cameras-and-what-you-need-to-know; Duncan McLeod (23 Jun 2020). "Interview: Vumacam CEO Ricky Croock," *TechCentral*, at: https://techcentral.co.za/interview-vumacam-ceo-ricky-croock/99029.

8 See Dale McKinley, "New Terrains of Privacy" [note 7]; *BusinessTech* (9 Jul 2019). "Watch: South African highway cameras used to track hijackers," at: https://businesstech.co.za/news/technology/328221/watch-south-african-highway-cameras-used-to-track-hijackers; Murray Williams (16 Feb 2012). "CCTV eye turns traffic spy," *IOL*, at: https://www.iol.co.za/capeargus/cctv-eye-turns-traffic-spy-1235903; Arthi Gopi (12 May 2018). "'Big Brother' watching – cameras monitor highways," *IOL*, at: https://www.iol.co.za/ios/news/big-brother-watching-cameras-monitor-highways-14939633; *BusinessTech* (24 Feb 2019). "Here is the new smart technology the Western Cape is using to tackle bad driving," at: https://businesstech.co.za/news/motoring/300408/here-is-the-new-smart-technology-the-western-cape-is-using-to-tackle-bad-driving.

9 See Dale McKinley, "New Terrains of Privacy" [note 7].

10 See David Bruce and Sean Tait (2015). "A 'Third Umpire' for Policing in South Africa: Applying Body Cameras in the Western Cape," *Igarapé Institute*, Strategic Paper 14, at: https://igarape.org.br/wp-content/uploads/2015/02/AE-14_SMART-POLICING1.pdf; *BusinessTech* (24 Jun 2019). "South African police officers to wear body cameras," at: https://businesstech.co.za/news/technology/324999/south-african-police-officers-to-wear-body-cameras.

11 See *BusinessTech* (24 Feb 2019). "Here is the new smart technology the Western Cape is using to tackle bad driving," at: https://businesstech.co.za/news/motoring/300408/here-is-the-new-smart-technology-the-western-cape-is-using-to-tackle-bad-driving; Slindo Mbuyisa and Leon Engelbrecht (16 Jul 2010). "Mandela Bay purchases mobile surveillance vehicle worth R6 million," *defenceWeb*, at: https://www.defenceweb.co.za/security/civil-security/mandela-bay-purchases-mobile-surveillance-vehicle-worth-r6-million; *eThekwini's Municipality* (25 Jan 2012). "eThekwini's Mobile CCTV a First," at: http://www.durban.gov.za/Resource_Centre/new2/Pages/eThekwini's-Mobile-CCTV-a-First.aspx; *Visec* (8 Oct 2018). "South African Police (Saps) Use License Plate Recognition (LPR) to Help Catch Criminals," at: https://www.visec.com/index.php?route=extras/blog/getblog&blog_id=23.

12 See Michael Kwet (14 July 2020). "The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud," *The Intercept*, at: https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition.

13 Daneel Knoetze (11 Sep 2014). "City of Cape Town plan to acquire drones," *GroundUp*, at: https://www.groundup.org.za/article/city-cape-town-plan-acquire-drones_2226.

14 Michael Kwet (27 Jan 2017). "Cmore: South Africa's New Smart Policing Surveillance Engine," *Counterpunch*, at: https://www.counterpunch.org/2017/01/27/cmore-south-africas-new-smart-policing-surveillance-engine.

15 See Jay Caboz (6 Aug 2019). "Cape Town wants to use drones to combat crime – here's how it would work," *Business Insider*, at: https://www.businessinsider.co.za/city-of-cape-town-wants-to-use-drones-to-combat-crime-2019-8.

16 See Kavitha Pillay (16 May 2018). "Home Affairs launches new automated biometric ID system," *News24 (traveller24)*, at: https://www.traveller24.com/TravelPlanning/dha-launches-new-id-system-to-benefit-south-africans-while-improving-tourism-20180516.

17 As the CSIR put it: "Ever watched a crime drama or spy film…where a team of technicians are sitting in a darkened room full of big, fancy monitors that enable them to constantly track and follow a Jason Bourne-like assailant with great precision, in real-time, while being in constant communication with a team of operatives and controlling traffic lights and surveillance cameras seemingly at will? That is the

kind of advanced shared situational awareness that the Cmore system can enable." *CSIR* (Sep 2016). "The *CSIR* Dossier of Science and Technology for Defence and Security," 1, p. 42, at: https://www.csir.co.za/sites/default/files/Documents/Dossier_Aug2016_Draft8_final%20lowres%20file.pdf.

18 See Michael Kwet, "Cmore" [note 14].

19 See Michael Kwet, "Apartheid in the Shadows" [note 7].

20 See ruling by Roland Sutherland (16 Sep 2019). "Judgment – CASE NO: 25978/2017, amaBhungane Centre for Investigative Journalism v Minister of Justice and Others," at: https://amabhungane.org/wp-content/uploads/2019/09/Judgment-AMABHUNGANE-v-MIN-JUSTICE-OTH.pdf. For context, see Sam Sole (18 Sep 2019). "Analysis: Inside amaBhungane's landmark ruling on surveillance," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2019-09-18-analysis-inside-amabhunganes-landmark-ruling-on-surveillance.

21 See Jane Duncan (30 Sep 2019). "Bulk communication surveillance in South Africa – fix it or nix it," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2019-09-30-bulk-communication-surveillance-in-south-africa-fix-it-or-nix-it.

22 See Jennifer Granick (2017). *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It*. New York, NY: Cambridge University Press.

23 See Ewen MacAskill (2 Nov 2013). "Portrait of the NSA: no detail too small in quest for total surveillance," *The Guardian*, at: https://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance; Ryan Gallagher (1 Mar 2018). "The Powerful Global Spy Alliance You Never Knew Existed," *The Intercept*, at: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors; *Wikipedia* (1 May 2020). "UKUSA Agreement," at: https://en.wikipedia.org/wiki/UKUSA_Agreement.

24 *The Guardian* (16 Jun 2013). "How GCHQ stepped up spying on South African foreign ministry," at: https://www.theguardian.com/world/2013/jun/16/gchq-south-african-foreign-ministry.

25 RDM News Wire (22 Jun 2015). "British Intelligence caught spying on South Africa's leftie lawyers," *TimesLIVE*, at: https://www.timeslive.co.za/news/south-africa/2015-06-22-british-intelligence-caught-spying-on-south-africas-leftie-lawyers [paywall]; Owen Bowcott (22 Jun 2015). "GCHQ's surveillance of two human rights groups ruled illegal by tribunal," *The Guardian*, at: https://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal.

26 For case examples, see *Right2Know* (2015). "Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements," at: http://bigbrother.r2k.org.za/wp-content/uploads/Big-Brother-Exposed-R2K-handbook-on-surveillance-web.pdf.

27 The study of surveillance capitalism extends back over a decade. The term is often misattributed to retired Harvard Business School professor Shoshana Zuboff; it was actually coined by a diverse set of Marxist scholars in a special issue of *Monthly Review* (available at: https://monthlyreview.org/2014/07/01/mr-066-03-2014-07_0). For the origins of the term "surveillance capitalism", see *Monthly Review* (1 May 2016). "Notes from the editors," at: https://monthlyreview.org/2016/05/01/mr-068-01-2016-05_0. For an insightful review which deems Zuboff's analysis "a step backward in our understanding" of surveillance capitalism, see Evgeny Morozov (4 Feb 2019). "Capitalism's New Clothes," *The Baffler*, at: https://thebaffler.com/latest/capitalisms-new-clothes-morozov. See also, Michael Kwet (forthcoming). "Property Is Not Neutral: Why Shoshana Zuboff and "Critical Data Studies" Are Wrong About Surveillance Capitalism."

28 See Anderson Cooper (9 Apr 2017). "What is "Brain Hacking"? Tech Insiders on Why You Should Care," *60 Minutes*, at: https://www.cbsnews.com/news/brain-hacking-tech-insiders-60-minutes.

29 See Samuel Greengard (2015). *The Internet of Things*. Cambridge, MA: The MIT Press; Laura DeNardis (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*, New Haven, CT: Yale University Press; Michael Kwet and Paul Prinsloo (2020). The 'smart' classroom: a new frontier in the age of the smart university, *Teaching in Higher Education*, 25 (4), pp. 510-526, at: https://www.tandfonline.com/doi/full/10.1080/13562517.2020.1734922.

30 For a framework outlining digital colonialism, see Michael Kwet (16 Jan 2019). "Digital colonialism: US empire and the new imperialism in the Global South," *Race & Class*, 60 (4), at: https://journals.sagepub.com/doi/abs/10.1177/0306396818823172 (free draft at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232297); Michael Kwet (2019). "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley" [note 1]; Michael Kwet (13 Mar 2019). "Digital colonialism is threatening the Global South," *Al Jazeera*, at: https://www.aljazeera.com/indepth/opinion/digital-colonialism-threatening-global-south-190129140828809.html; Michael Kwet (29 Jun 2018). "Break the hold of digital colonialism," *Mail & Guardian*, at: https://mg.co.za/article/2018-06-29-00-break-the-hold-of-digital-colonialism.

See also, among other works, Alfred McCoy (2009). *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State*. Madison, WI: The University of Wisconsin Press; Andres Guadamuz (30 Dec 2017). "Digital Colonialism and Decentralisation," *TechnoLama*, at: https://www.technollama.co.uk/digital-colonialism-and-decentralisation; publications by Nanjira Sambuli (https://nanjira.com); Renata Avila (2018). "Digital Sovereignty or Digital Colonialism?" *International Journal on Human Rights*, 27, at: https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism; Nanjala Nyabola (2018). *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Kenya*. London, UK: Zed Books Ltd (especially Chapter 8); Mishi Choudhary and Eben Moglen, "Beat digital colonialism – What Digital India should mean: A tech policy for the Indian future," *The Times of India*, at: https://timesofindia.indiatimes.com/blogs/toi-edit-page/beat-digital-colonialism-what-digital-india-should-mean-a-tech-policy-for-the-indian-future; and writings by Parminder Jeet Singh at IT for Change, at: https://itforchange.net/Parminder.

31 See Michael Kwet (4 Dec 2017). "Operation Phakisa Education: Why A Secret? Mass Surveillance, Inequality and Race in South Africa's Emerging National E-Education System," *First Monday*, 12(4), at: http://firstmonday.org/ojs/index.php/fm/article/view/8054; Michael Kwet (8 Dec 2017). "Big Brother set to watch each pupil," *Mail & Guardian*, at: https://mg.co.za/article/2017-12-08-00-big-brother-set-to-watch-each-pupil; Michael Kwet (9 Oct 2015). "The Dangers of Paperless Classrooms," *Mail & Guardian*, at: https://mg.co.za/article/2015-10-07-the-dangers-of-paperless-classrooms.

32 See *Right2Know* (researched by Murray Hunter and Tymon Smith) (Jun 2018). "Spooked: Surveillance of Journalists in SA," at: https://www.r2k.org.za/wp-content/uploads/R2K-Surveillance-of-Journalists-Report-2018-web.pdf.

33 See, for example, Julia Angwin, Ariana Tobin and Madeline Varner (21 Nov 2017). "Facebook (Still) Letting Housing Advertisers Exclude Users by Race," *ProPublica*, at: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin; Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner (23 May 2016). "Machine Bias," *ProPublica*, at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

34 For an overview of studies, see Michael Kwet, "Digital colonialism: South Africa's education transformation in the Shadow of Silicon Valley," [note 1] pp. 102-107.

35 See Sam Sole (20 Apr 2017). "Surveillance: The silent spy on citizens and journalists faces court challenge," *Mail & Guardian*, at: https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1.

36 See *Right2Know*, "Spooked" [note 32]; Jane Duncan (2014). "Communications Surveillance in South Africa: The case of the Sunday Times newspaper," pp. 224-227, in Alan Finlay (ed) (2014). *Global Information Society Watch 2014*, APC and Hivos; Admire Mare (Mar 2016). "A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa," *Media Policy and Democracy Project*, pp. 26-34, at: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/duncan_2_comm_surveillance.pdf.

37 See *Electronic Frontier Foundation* (no date). "Threat Modeling," at: https://www.eff.org/files/2015/11/24/3mod_threat-modeling-ssd_9-3-15.pdf.

38 See Eben Moglen (27 May 2014). "Privacy under attack: the NSA files revealed new threats to democracy," *The Guardian*, at: https://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy. Of course, there is more to say about privacy than is discussed in Moglen's definition, but it provides a sufficient approximation for this guide.

39 See, among others, Jonathon W. Penney (2016). "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal*, 1 (2016), pp. 117-182, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645; Jonathon W. Penney (2017). "Internet surveillance, regulation, and chilling effects online: a comparative case study," *Internet Policy Review*, 6 (2), pp. 1-239, at: https://policyreview.info/node/692/pdf; Alex Marthews and Catherine Tucker (29 Apr 2015). "Government Surveillance and Internet Search Behavior," at: https://www.ftc.gov/system/files/documents/public_comments/2015/10/00023-97629.pdf.

40 Michael Kwet, "Operation Phakisa Education" [note 31]. See also, R. Kelly Garrett and Paul N. Edwards (2007). "Revolutionary secrets: Technology's role in the South African anti-apartheid movement," *Social Science Computer Review*, 25 (1), pp. 13–26.

41 For a detailed analysis of what SAPS can do with your metadata, see Murray Hunter (Mar 2020). "Cops and call records: Perspectives on privacy, policing and metadata in South Africa," *Media and Democracy Project*, at: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/cops_and_call_records_web_masterset_26_march.pdf.

42 See *GNU.org* (no date). "What is free software?" at: https://www.gnu.org/philosophy/free-sw.en.html.

43 For more about Free Software licenses, see *Wikipedia* (1 May 2020). "Free-software license," at: https://en.wikipedia.org/wiki/Free_software_license.

44 See Bruce Schneier (15 Sep 1999). "Crypto-Gram," at: https://www.schneier.com/crypto-gram/archives/1999/0915.html.

45 See Edward Snowden (19 Mar 2016). "The Last Lighthouse: Free Software in Dark Times," *Let Snowden In*, at: https://media.libreplanet.org/u/libreplanet/m/libreplanet-2016-the-last-lighthouse-3d51.

46 For details on the history of Free Software policy in South Africa, see Michael Kwet, "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley" [note 1], pp. 179-193. For a core policy document, see Department of Public Service and Administration (DPSA) (1997). "POLICY ON FREE and OPEN SOURCE SOFTWARE USE for SOUTH AFRICAN GOVERNMENT. Appendix A: Policy Implementation Strategy. Department of Public Service and Administration," *DPSA*, at: https://www.gov.za/sites/default/files/gcis_document/201409/fosspolicy0.pdf.

47 See *Right2Know*, 2015, "Big Brother Exposed" [note 26]; Admire Mare, "A qualitative analysis," pp.38-43 [note 36]; *Right2Know*, "Spooked" [note 32].

48 See Murray Hunter, "Cops and call records" [note 41]; Murray Hunter (23 Aug 2017). "Cops gaining access to tens of thousands of cellphone records – R2K," *Politicsweb*, at: http://www.politicsweb.co.za/news-and-analysis/cops-gaining-access-to-tens-of-thousands-of-cellph; Heidi Swart (23 Aug 2017). "Cell phone privacy: Law enforcement pulls 70,000 subscribers' call records each year – and that's a minimum estimate," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2017-08-23-cell-phone-privacy-law-enforcement-pulls-70000-subscribers-call-records-each-year-and-thats-a-minimum-estimate.

49 See note 47.

50 Jenna McLauglin (31 Oct 2016). "South African Spy Company Used by Gadaffi Touts its NSA-Like Capabilities," *The Intercept*, at: https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities. See also, *Privacy International, the Association for Progressive Communications & the Right2Know Campaign* (Apr 2015). "The Right to Privacy in South Africa," pp. 6-7, at: https://privacyinternational.org/sites/default/files/2017-12/PI%20submission%20South%20Africa%20FINAL.pdf.

51 See Laura Silver (5 Feb 2019). "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally," *Pew Research*, at: https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally.

52 Smartphone ownership grew from 37% in 2015 to 60% in 2017. See Jacob Poushter, Caldwell Bishop, and Hanyu Chwe (19 Jun 2018). "Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones: Digital divides remain, both within and across countries," *Pew Research*, pp. 14-15, at: http://assets.pewresearch.org/wp-content/uploads/sites/2/2018/06/15135408/Pew-Research-Center_Global-Tech-Social-Media-Use_2018.06.19.pdf; Laura Silver, "Smartphone Ownership Is Growing" [note 51].

53 See *BusinessDay* (17 Oct 2018). "Right2Know rails against high data costs at commission hearing," at: https://www.businesslive.co.za/bd/national/2018-10-17-right2know-rails--against-high-data-costs-at-commission-hearing.

54 See Cyrus Farivar (4 Oct 2016). "FBI demands Signal user data, but there's not much to hand over," *Ars Technica*, at: https://arstechnica.com/tech-policy/2016/10/fbi-demands-signal-user-data-but-theres-not-much-to-hand-over; Micah Lee (22 Jun 2016). "Battle of the Secure Messaging Apps: How Signal Beats WhatsApp," *The Intercept*, at: https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp.

55 See Lorenzo Franceschi-Bicchierai (10 Jul 2020). "Signal's New PIN Feature Worries Cybersecurity Experts," *VICE News (Motherboard)*, at: https://www.vice.com/en_us/article/pkyzek/signal-new-pin-feature-worries-cybersecurity-experts.

56 For those deeper into the subject, Signal prevents server federation across independent servers, to the consternation of some tech activists who are worried about being locked into the decisions of Moxie Marlenspike and Open Whisper Systems (the maintainers of Signal). See Sander Venema (5 Nov 2016). "Why I won't recommend Signal anymore," at: https://web.archive.org/web/20190427000021/https://sandervenema.ch/2016/11/why-i-wont-recommend-signal-anymore; Sean Gallagher (2 May 2018). "Amazon blocks domain fronting, threatens to shut down Signal's account," *Ars Technica*, at: https://arstechnica.com/information-technology/2018/05/amazon-blocks-domain-fronting-threatens-to-shut-down-signals-account.

57 See Lorenzo Franceschi-Bicchierai, "Signal's New PIN" [note 56].

58 See Matt Mitchell (18 Nov 2016). "How to reach Matt Mitchell securely?" *Medium*, at: https://medium.com/@geminiimatt/how-to-reach-me-securely-80d69a5ce38e.

59 See Wire (19 Sep 2017). "Wire server code now 100% open source – the journey continues," *Medium*, at: https://medium.com/@wireapp/wire-server-code-now-100-open-source-the-journey-continues-88e24164309c.

60 See Jessi Hempel (30 Mar 2018). "A Short History of Facebook's Privacy Gaffes," *Wired*, at: https://www.wired.com/story/facebook-a-history-of-mark-zuckerberg-apologizing; David Nield (12 Jan 2019). "All the Ways Facebook Tracks You – and How to Limit It," *Wired*, at: https://www.wired.com/story/ways-facebook-tracks-you-limit-it.

61 See Brian Barrett (25 Aug 2016). "WhatsApp's Privacy Cred Just Took a Big Hit," *Wired*, at: https://www.wired.com/2016/08/whatsapp-privacy-facebook.

62 See Glenn Greenwald and Ewen MacAskill (7 Jun 2013). "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian*, at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Bruce Schneier (25 Mar 2014). "Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership is Still Going Strong," *The Atlantic*, at: https://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612. As far as we know, all NSA public-private partnerships revealed by Edward Snowden exist to this day.

63 See Andy Greenberg (10 Jan 2020). "Facebook Says Encrypting Messenger by Default Will Take Years," *Wired*, at: https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default; Thomas Germain (7 Mar 2019). "Facebook Promises Encrypted Messaging, but You Don't Need to Wait," *Consumer Reports*, at: https://www.consumerreports.org/privacy/facebook-promises-encrypted-messaging-but-you-dont-need-to-wait.

64 See Sam Biddle (28 Sep 2016). "Apple Logs Your iMessage Contacts – and May Share Them With Police," *The Intercept*, at: https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police; *Apple* (27 Dec 2019). "iMessage and FaceTime & Privacy," at: https://support.apple.com/en-us/HT209110.

65 See Aatif Sulleyman (2 November 2017). "Snapchat adds 'creepy' targeting, letting companies track you online," *The Independent*, at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/snapchat-ad-targeting-ads-app-online-snap-pixel-evan-spiegel-a8033136.html; *Snap* (18 Dec 2019). "Privacy Policy," at: https://web.archive.org/web/20200403010020/https://www.snap.com/en-US/privacy/privacy-policy.

66 See William Turton (24 Jun 2016). "Why You Should Stop Using Telegram Right Now," *Gizmodo*, at: https://gizmodo.com/why-you-should-stop-using-telegram-right-now-1782557415.

67 See Greg Sterling (17 Jun 2019). "Almost 70% of digital ad spending going to Google, Facebook, Amazon, says analyst firm," *Marketing Land*, at: https://marketingland.com/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm-262565; Ian Burrell (13 Mar 2019). "Are Google and Facebook killing advertising?" *Raconteur*, at: https://www.raconteur.net/business-innovation/google-facebook-duopoly.

68 See Nathan Geffen (10 Apr 2017). "Why we're dropping Google Ads," *GroundUp*, at: https://www.groundup.org.za/article/why-were-dropping-google-ads.

69 See Julia Angwin et al., "Facebook (Still) Letting" [note 33].

70 See Ian Paul (18 May 2017). "Twitter rolls out new privacy tools as it ditches Do Not Track and expands data sharing," *PCWorld*, at: https://www.pcworld.com/article/3197343/twitter-rolls-out-new-privacy-tools-as-it-ditches-do-not-track-and-expands-data-sharing.html; Andrew Quodling (13 Apr 2018). "Shadow profiles - Facebook knows about you, even if you're not on Facebook," *The Conversation*, at: https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804; David Ingram (15 Apr 2018). "Facebook fuels broad privacy debate by tracking non-users," *Reuters*, at: https://www.reuters.com/article/us-facebook-privacy-tracking/facebook-fuels-broad-privacy-debate-by-tracking-non-users-idUSKBN1HM0DR; Richard Chirgwin (17 Apr 2018). "Facebook admits it does track non-users, for their own good," *The Register*, at: https://www.theregister.co.uk/2018/04/17/facebook_admits_to_tracking_non_users.

71 See, for example, *Electronic Frontier Foundation* (no date). "NSA Spying," at: https://www.eff.org/nsa-spying.

72 See Muhammed Ikram et al. (2016). "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps," *ICM 2016*, at: https://www.icir.org/vern/papers/vpn-apps-imc16.pdf.

73 See Hanno Labuschange (29 Feb 2020). "The dangers of using a free VPN," *MyBroadband*, at: https://mybroadband.co.za/news/internet/338316-the-dangers-of-using-a-free-vpn.html.

74 See, for example, Yael Grauer (31 Jan 2020). "The Best VPN Service," *Wirecutter*, at: https://thewirecutter.com/reviews/best-vpn-service.

75 See Geoffrey Fowler (21 Jun 2019). "Goodbye, Chrome: Google's web browser has become spy software," *The Washington Post*, at: https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch.

76 See Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps" [note 60].

77 See notes 34 and 39.

78 See Safiya Noble (26 March 2018). "Google Has a Striking History of Bias Against Black Girls," *TIME*, at: https://time.com/5209144/google-search-engine-algorithm-bias-racism.

79 See *DuckDuckGo* (no date). "We don't collect or share personal information.," at: https://duckduckgo.com/privacy.

80 See *Qwant* (21 Feb 2020). "Privacy Policy," at: https://about.qwant.com/legal/privacy.

81 See *Google* (no date). "reCAPTCHA v3: The new way to stop bots," at: https://web.archive.org/web/20200408211814/https://www.google.com/recaptcha/intro/v3.html; James O'Malley (12 Jan 2018). "Captcha if you can: how you've been training AI for years without realising it," *TechRadar*, at: https://www.techradar.com/news/captcha-if-you-can-how-youve-been-training-ai-for-years-without-realising-it.

82 See the Gupta-leaks.com website at: http://www.gupta-leaks.com.

83 For a description of settings, see Micah Lee (5 Sep 2019). "Configuring OnionShare," *GitHub*, at: https://github.com/micahflee/onionshare/wiki/Configuring-OnionShare.

84 See *Mozilla* (no date). "File Encryption," GitHub, at: https://github.com/mozilla/send/blob/master/docs/encryption.md.

85 Riseup Share uses Up1 for client-side encryption. See Up1 (no date). "Up1: A Client-side Encrypted Image Host," *GitHub*, at: https://github.com/Upload/Up1.

86 See Ray Walsh (5 Jul 2019). "How secure are Dropbox, OneDrive, Google Drive and iCloud?" *ProPrivacy*, at: https://proprivacy.com/cloud/guides/how-secure-is-cloud-storage; Barton Gellman and Laura Poitras (7 Jun 2013). "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, at: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

87 See Nation Nyoka (24 Oct 2017). "'We have nothing to hide,' Malema after attempted hacking of his email," *News24*, at: https://www.news24.com/news24/southafrica/news/we-have-nothing-to-hide-malema-after-attempted-hacking-of-his-email-20171024.

88 See Glenn Greenwald (31 Jul 2013). "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian*, at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; *NDR* (26 Jan 2014). "Snowden-Interview: Transcript," at: https://web.archive.org/web/20140128224439/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html.

89 See Glenn Greenwald and Spencer Ackerman (27 Jun 2013). "NSA collected US email records in bulk for more than two years under Obama," *The Guardian*, at: https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama; Glenn Greenwald (31 Jul 2013). "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian*, at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Joseph Menn (4 Oct 2016). "Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence – sources," *Reuters*, at: https://www.reuters.com/article/us-yahoo-nsa-exclusive/exclusive-yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

90 For a comparison of ProtonMail and Tutanota, see *NordVPN* (6 Apr 2020). "Tutanota vs Protonmail: Which one is better?" at: https://nordvpn.com/blog/tutanota. For an explanation of ProtonMail's end-to-end encryption, see *ProtonMail* (7 Mar 2018). "What is end-to-end encryption and how does it work?" at: https://protonmail.com/blog/what-is-end-to-end-encryption.

91 See Declan McCullagh (11 Jul 2013). "NSA docs boast: Now we can wiretap Skype video calls," *CNET*, at: https://www.cnet.com/news/nsa-docs-boast-now-we-can-wiretap-skype-video-calls; Ryan Gallagher (12 Jul 2013). "Timeline: How the World Was Misled About Government Skype Eavesdropping," *Slate*, at: http://www.slate.com/blogs/future_tense/2013/07/12/skype_surveillance_a_timeline_of_public_claims_and_private_government_dealings.html.

92 See Spencer Ackerman and James Ball (28 Feb 2014). "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, at: https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

93 See Micah Lee and Yael Grauer (31 Mar 2020). "Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing," *The Intercept*, at: https://theintercept.com/2020/03/31/zoom-meeting-encryption.

94 See Kari Paul (17 Jun 2020). "Zoom will provide end-to-end encryption to all users after privacy backlash," *The Guardian*, at: https://www.theguardian.com/technology/2020/jun/17/zoom-encryption-free-calls.

95 See *Jitsi* (3 Apr 2020). "Jitsi Meet Security & Privacy," at: https://web.archive.org/web/20200404065051/https://jitsi.org/news/security; Emil Ivov (12 Apr 2020). "This is what end-to-end encryption should look like!" *Jitsi*, at: https://jitsi.org/blog/e2ee.

96 For the leaked document about Skype's collaboration with the NSA, see NSA (Aug 2012). "User's Guide For PRISM Skype Collection," *ACLU*, at: https://www.aclu.org/sites/default/files/field_document/Guide%20for%20Analysts%20on%20How%20to%20Use%20the%20PRISM%20Skype%20Collection.pdf. See also, Glenn Greenwald et al. (12 Jul 2013). "Microsoft handed the NSA access to encrypted messages," *The Guardian*, at: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data; Ryan Gallagher (12 Jul 2013). "Timeline: How the World Was Misled" [note 91].

97 See Joseph Cox (27 Mar 2020). "Zoom Removes Code That Sends Data to Facebook," *VICE News (Motherboard)*, at: https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook.

98 See Aaron Krolik and Natasha Singer (2 Apr 2020). "A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles," *The New York Times*, at: https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html.

99 See Brian X. Chen (8 Apr 2020). "The Lesson We Are Learning From Zoom," *The New York Times*, at: https://www.nytimes.com/article/zoom-privacy-lessons.html.

100 See Eric S. Yuan (2 Apr 2020). "Attendee attention tracking," *Zoom*, at: https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking.

101 Martin Shelton (10 Oct 2019). "Newsrooms, let's talk about G Suite," *Medium*, at: https://medium.com/freedom-of-the-press-foundation/newsrooms-lets-talk-about-g-suite-1672a36eb235. See also Maya Salam (31 Oct 2017). "Google Docs Glitch That Locked Out Users Underscores Privacy Concerns," *The New York Times*, at: https://www.nytimes.com/2017/10/31/technology/google-docs-glitch-bug.html.

102 See Martin Shelton (28 Jan 2020). "Newsrooms, let's talk about Office 365," *Medium*, at: https://medium.com/freedom-of-the-press-foundation/newsrooms-lets-talk-about-office-365-ec38d613ec0c.

103 See *CryptPad* (no date). "Frequently Asked Questions," at: https://cryptpad.fr/faq.html.

104 See Sarah Evans (7 Mar 2014). "Marikana service delivery researchers spooked," *Mail & Guardian*, at: https://mg.co.za/article/2014-03-06-marikana-service-delivery-researchers-spooked.

105 See *eNCA* (23 Apr 2017). "Laptops of journalists stolen19 at SABC's offices in Parliament," at: https://www.enca.com/south-africa/laptops-of-journalists-stolen-at-sabcs-offices-in-parliament; Thomas Hartleb (21 Apr 2015). "Laptop with Marikana evidence stolen," *News24*, at: https://www.news24.com/News24/laptop-with-evidence-of-marikana-stolen-20150421; Jeanette Chabalala (10 Jul 2017). "Two laptops stolen from NPA offices," *News24*, at: https://www.news24.com/news24/southafrica/news/two-laptops-stolen-from-npa-offices-20170710; *The Citizen* (18 Mar 2017). "Chief Justice Mogoeng Mogoeng's offices burgled," at: https://citizen.co.za/news/south-africa/1461845/chief-justice-mogoeng-mogoengs-offices-burgled; Angelique Serrao (7 Nov 2012). "Sinister cases of break-ins and document theft," *IOL News / The Star*, at: https://www.iol.co.za/the-star/sinister-cases-of-break-ins-and-document-theft-1418826; Amanda Khoza (20 Mar 2017). "9 mysterious cases of intimidation and stolen information," *News24*, at: https://www.news24.com/news24/southafrica/news/9-mysterious-cases-of-intimidation-and-stolen-information-20170320; Marianne Thamm (20 Mar 2016). "Documents and computers seized in armed, apartheid military-style robbery at Helen Suzman Foundation offices," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2016-03-20-documents-and-computers-seized-in-armed-apartheid-military-style-robbery-at-helen-suzman-foundation-offices.

106 For the initial story, see Tefo Mahapi (18 Oct 2017). "What we know so far about South Africa's largest ever data breach," *iAfrikan*, at: https://www.iafrikan.com/2017/10/18/south-africas-govault-hacked-over-30-million-personal-records-leaked. For an explanation and further details, see Troy Hunt, "Weekly update 57," *YouTube*, at: https://www.youtube.com/watch?time_continue=68&v=GAJKo4bjhIM; Jan Vermeulen (26 Oct 2017). "Massive South African data leak – Now over 75 million records at risk," *MyBroadband*, at: https://mybroadband.co.za/news/security/234790-massive-south-african-data-leak-now-over-75-million-records-at-risk.html.

107 See Roxanne Henderson and Jacqueline Mackenzie (25 Oct 2019). "Johannesburg City Crippled as Hacker Demands Bitcoin Ransom," *Bloomberg*, at: https://www.bloomberg.com/news/articles/2019-10-25/south-africa-s-johannesburg-shuts-billing-over-security-breach; Chanel Retief (25 Oct 2019). "Attempted hack attack triggers system shutdown in the City of Johannesburg," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2019-10-25-attempted-hack-attack-triggers-system-shutdown-in-the-city-of-johannesburg.

108 *IOL* (21 Jun 2018). "South Africans losing R2.2 billion a year to cyber attacks," at: https://www.iol.co.za/capeargus/news/south-africans-losing-r22-billion-a-year-to-cyber-attacks-15601682.

109 See Jessica Hubbard (13 Mar 2019). "SA business underplaying the danger of cybercrime?" *Fin24*, at: https://www.fin24.com/Finweek/Business-and-economy/sa-business-underplaying-the-danger-of-cybercrime-20190313.

110 See Duncan Alfreds (12 Jul 2018). "SA companies lose on average R36 million every time they get hacked," *Business Insider*, at: https://www.businessinsider.co.za/heres-just-how-much-sa-companies-are-losing-the-cyber-war-to-crooks-20180712.

111 See Bill Marczak et al. (18 Sep 2018). "Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab*, at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries.

112 See Hagar Shezaf (20 Oct 2018). "Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays," *Haazertz*, at: https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027.

113 The common person cannot resist the most sophisticated and expensive forms of hacking, what Edward Snowden calls "voodoo hacking." Yet we know that organisations have been able to subvert was able to thwart the world's most powerful spies. For example, Wikileaks was able to help Edward Snowden escape capture by the United States, even though the US was aware of who works for Wikileaks, and surely tried to intercept their communications. For an example of how intense digital self-defense against nation state actors can become, see Barton Gellman (Jun 2020). "Since I Met Edward Snowden, I've Never Stopped Watching My Back," *The Atlantic*, at: https://www.theatlantic.com/magazine/archive/2020/06/edward-snowden-operation-firstfruits/610573.

114 See Ben Gilbert (17 May 2019). "An insider reveals how the nasty spyware used in the WhatsApp breach lets governments secretly access everything in your smartphone, from text messages to the microphone and cameras," *Business Insider*, at: https://www.businessinsider.com/whatsapp-hack-what-is-pegasus-2019-5#what-is-pegasus-2.

115 See Erik Manukyan (7 Nov 2019). "Summary: WhatsApp Suit Against NSO Group," *Lawfare*, at: https://www.lawfareblog.com/summary-whatsapp-suit-against-nso-group.

116 See Danny Bradbury (17 Jul 2019). "Microsoft, Google and Apple clouds banned in Germany's schools," *Naked Security by Sophos*, at: https://nakedsecurity.sophos.com/2019/07/17/germany-bans-schools-from-using-tech-giants-clouds; Tim Sandle (2 Aug 2019). "German schools ban Office 365 over privacy concerns: Interview," *Digital Journal*, at: http://www.digitaljournal.com/tech-and-science/technology/german-schools-ban-microsoft365-over-privacy-concerns-interview/article/555165.

117 See *GNU.org* (10 Jun 2019). "Microsoft's Software is Malware," at: https://www.gnu.org/proprietary/malware-microsoft.en.html; *GNU.org* (16 Jul 2019). "Apple's Operating Systems Are Malware," at: https://www.gnu.org/proprietary/malware-apple.en.html; *GNU.org* (30 Jul 2019). "Google's Software is Malware," at: https://www.gnu.org/proprietary/malware-google.html; Mark Wilson (5 Jun 2019). "Apple created the privacy dystopia it wants to save you from," *Fast Company*, at: https://www.fastcompany.com/90352021/apple-created-the-privacy-dystopia-it-wants-to-save-you-from; Michael Kwet (14 Jun 2019). "In Stores, Secret Surveillance Tracks Your Every Move," *The New York Times*, at: https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

118 See Narseo Vallina-Rodriguez and Srikanth Sundaresan (29 May 2017). "7 in 10 smartphone apps share your data with third-party services," *The Conversation*, at: http://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404; Yael Grauer (24 Nov 2017). "Staggering Variety of Clandestine Trackers Found in Popular Android Apps," *The Intercept*, at: https://theintercept.com/2017/11/24/staggering-variety-of-clandestine-trackers-found-in-popular-android-apps; Sean O'Brien and Michael Kwet (24 Jan 2018). "Love, sex and trackers – Tinder and other dating apps are spies in your bedroom," *BoingBoing*, at: https://boingboing.net/2018/01/24/love-sex-and-trackers-tind.html; Michael Kwet and Sean O'Brien (14 Dec 2017). "The Targets of Mobile Apps: Your Health, Your Ancestors, and Your Baby," *VICE News (Motherboard)*, at: https://motherboard.vice.com/en_us/article/3kpagb/the-targets-of-mobile-apps-your-health-your-ancestors-and-your-baby; Michael Kwet, "In Stores, Secret Surveillance" [note 117].

119 See Michael Kwet (5 Sep 2018). "Google and Apple's Systems to Track you in Person: What the Media Isn't Telling You," *Counterpunch*, at: https://www.counterpunch.org/2018/09/06/google-and-apples-systems-to-track-you-in-person-what-the-media-isnt-telling-you; Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller and Aaron Krolik (10 Dec 2018). "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times*, at: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html; Michael Kwet, "In Stores, Secret Surveillance" [note 117]; Jennifer Valentino-DeVries (13 Apr 2019). "Tracking Phones, Google is a Dragnet for the Police," *The New York Times*, at: https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

120 See Sean O'Brien and Michael Kwet (21 Jan 2018). "Android Users: To Avoid Malware, Try the F-Droid App Store," *Wired*, at: https://www.wired.com/story/android-users-to-avoid-malware-ditch-googles-app-store; Hans-Christoph Steiner (16 Jan 2020). "Tracking the Trackers: using machine learning to aid ethical decisions," *F-Droid*, at: https://f-droid.org/en/2020/01/16/tracking-the-trackers.html.

121 See, among other examples, Michael Kwet (14 Jun 2019). "In Stores, Secret Surveillance"[note 117] (on how Apple and Google created technology for Bluetooth-based location surveillance); Zack Whittaker (24 May 2018). "I asked Apple for all my data. Here's what was sent back," *ZDNet*, at: https://www.zdnet.com/article/apple-data-collection-stored-request; Glenn Greenwald et al. (12 Jul 2013). "Microsoft handed the NSA access to encrypted messages," *The Guardian*, https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

122 See Michael Kwet, "Apartheid in the Shadows" [note 7].

123 See Michael Kwet, "Apartheid in the Shadows" [note 7].

124 Michael Kwet, "The Microsoft Police State" [note 12].

125 See Michael Kwet (22 Nov 2019). "Smart CCTV Networks Are Driving an AI-Powered Apartheid" [note 7].

126 See Kelly Gillespie (3 Mar 2017). "Favour rigorous debate, not security," *Mail & Guardian*, at: https://mg.co.za/article/2017-03-03-00-favour-rigorous-debate-not-security; Sizwe Mabizela (18 Nov 2016). "Safety and security on campus," *Rhodes University*, at: https://web.archive.org/web/20161119021018/http://www.ru.ac.za/latestnews/safetyandsecurityoncampus.html; *SERI* (2017). "A Double Harm: Police Misuse of Force and Barriers to Necessary Health Care Services," at: https://seri-sa.org/images/A_Double_Harm_Wits_Report_FINAL.pdf.

127 See Michael Kwet, "The Rise of Smart Camera Networks" [note 6].

128 See Michael Kwet, "The Rise of Smart Camera Networks" [note 6].

129 See Heidi Swart (13 Jun 2019). "Visual surveillance and weak cyber security, Part One: When cameras get dangerous," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous; Heidi Swart (26 Jun 2019). "Video Surveillance and Cybersecurity (Part Two): Chinese cyber espionage is a real threat," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2019-06-26-video-surveillance-and-cybersecurity-part-two-chinese-cyber-espionage-is-a-real-threat.

130 See Michael Kwet, "Cmore" [note 14].

131 See Mike Cummings (27 Oct 2017). "Do body cameras affect police officers' behavior? Not so much," *Yale News*, at: https://news.yale.edu/2017/10/27/do-body-cameras-affect-police-officers-behavior-not-so-much.

132 See Michael Kwet, "The Microsoft Police State" [note 12]; Simnikiwe Mzekandaba (30 Oct 2019). "Microsoft tech to combat crime in Durban's inner city," *ITWeb*, at: https://www.itweb.co.za/content/kYbe9MXxPNyMAWpG.

133 See Shaun Swingler, "Meet the Grabber" [note 3].

134 See Michael Kwet, "Cmore" [note 14]; Michael Kwet, "Apartheid in the Shadows" [note 7]; Michael Kwet, "Smart CCTV Networks Are Driving an AI-Powered Apartheid" [note 7]. For South African outlets, see; Jane Duncan, "How CCTV poses a threat" [note 7]; Jane Duncan, "Op-Ed: What Ramaphosa needs to do" [note 7]; Heidi Swart, "Controlling Cape Town" [note 7]; Heidi Swart (21 Jul 2019). "How China's persecuted people are paying the price for Joburg's sense of security," *Daily Maverick*, at: https://www.dailymaverick.co.za/article/2019-07-21-how-chinas-persecuted-people-are-paying-the-price-for-joburgs-sense-of-security; Simon Allison (15 Nov 2019). "Our cameras will make you safe," *Mail & Guardian*, at: https://mg.co.za/article/2019-11-15-00-our-cameras-will-make-you-safe.

135 See Michael Kwet, "Smart CCTV Networks Are Driving an AI-Powered Apartheid" [note 7].

136 See Ari Levy (16 Jan 2020). "Big Tech is worth over $5 trillion now that Alphabet has joined the four comma club," *CNBC*, at: https://www.cnbc.com/2020/01/16/big-tech-worth-over-5-trillion-with-alphabet-joining-four-comma-club.html.

137 For an explanation and framework, see especially Michael Kwet, "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley" [note 1]; Michael Kwet, "Digital colonialism: US empire and the new imperialism in the Global South" [note 29].

138 See Michael Kwet (19 May 2020). "To fix social media, we need to introduce digital socialism," *Al Jazeera*, at: https://www.aljazeera.com/indepth/opinion/fix-social-media-introduce-digital-socialism-200512163043881.html.

139 See Michael Kwet (20 Dec 2019). "Can Twitter Ever Be Decentralized?" *Slate*, at: https://slate.com/technology/2019/12/jack-dorsey-open-decentralized-twitter.html.

140 See Paturi Rajasekhar (7 Feb 2019). "Freedom Box: 'Every old computer is a potential server that can bring Internet connectivity to an entire village'," *Entertainment Times*, at: https://timesofindia.indiatimes.com/entertainment/events/hyderabad/every-old-computer-is-a-potential-server-that-can-bring-internet-connectivity-to-an-entire-village/articleshow/67833580.cms.

141 See Steve Stecklow (28 Oct 2008). "Microsoft Battles Low-Cost Rival for Africa," *The Wall Street Journal*, at: https://www.wsj.com/articles/SB122332198757908625.

142 See David Kirkpatrick (17 Jul 2007). "How Microsoft Conquered China," *CNN Money*, at: https://money.cnn.com/magazines/fortune/fortune_archive/2007/07/23/100134488.

143 See Michael Kwet, "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley" [note 1], Chapter 6.

144 See Michael Kwet, "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley" [note 1]. I first published about problems with the programme at the *Mail & Guardian* in 2015; see Michael Kwet, "The Dangers of Paperless Classrooms" [note 31].

145 See Minister Angie Motshekga (3 Jan 2019). "Basic Education Minister to release Matric 2018 pass rate," *YouTube*, at: https://www.youtube.com/watch?v=ASIh4LRXhS4&feature=youtu.be&t=296; President Cyril Ramaphosa (7 Feb 2019). President Cyril Ramaphosa: 2019 State of the Nation Address," *South African Government*, at: https://www.gov.za/speeches/president-cyril-ramaphosa-2019-state-nation-address-7-feb-2019-0000.

146 See Michael Kwet, "Operation Phakisa Education" [note 31]; Michael Kwet, "Big Brother set to watch each pupil" [note 31]; Michael Kwet, "The dangers of paperless classrooms" [note 31].

147 See *Kerala Infrastructure and Technology for Education (KITE)* (no date). "Free and Open Source Software," at: https://kite.kerala.gov.in/KITE/index.php/welcome/wedo/1; *The Hindu* (17 Apr 2020). "KITE's customised videoconference system," at: https://www.thehindu.com/news/national/kerala/kites-customised-videoconference-system/article31370388.ece.

148 See Kate Wilkinson (15 February 2018). "FACTSHEET: South Africa's official poverty numbers," *Africa Check*, at: https://africacheck.org/factsheets/factsheet-south-africas-official-poverty-numbers.

149 Audrey Lorde (1984). "The Master's Tools Will Never Dismantle the Master's House," at: https://collectiveliberation.org/wp-content/uploads/2013/01/Lorde_The_Masters_Tools.pdf.

150 Archbishop Desmond Tutu (20 May 2007). "Archbishop Desmond Tutu opens Digital Freedom Exposition," *YouTube*, at: https://www.youtube.com/watch?v=RdydCoiru4o.

151 See Michael Kwet, "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley" [note 1], pp. 20-28, 107-109 (on the subject of "tech hegemony" and the techlash framework).

152 *South African Department of Justice* (2013). "Protection of Personal Information Act," at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf, pp. 20, 22, 46.

153 See Aleecia M. McDonald and Lorrei Faith Cranor (2008). "The Cost of Reading Privacy Policies," *I/S Journal of Law and Policy for the Information Society*, at: https://kb.osu.edu/dspace/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf. This also assumes users have the requisite knowledge to understand the Terms and Conditions, which are often couched in vaguely worded in legalese.

154 See Michael Kwet (2021). "Surveillance in South Africa: From Skin Branding to Digital Colonialism," forthcoming in Jeffrey Vagle and Michael Kwet (eds.). *The Cambridge Handbook of Race and Surveillance*, Cambridge University Press. Draft available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3677168.

155 See Michael Kwet (2020). "A Digital Tech New Deal: Digital Socialism, Declonization, and Reparations for a Global Green Economy", forthcoming, *GIS Watch*. Draft available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670986.

156 Zwelakhe Sisulu (1986). "People's Education for People's Power," *Transformation*, 1, pp. 96-117, at: http://transformationjournal.org.za/wp-content/uploads/2017/02/388-341-1-PB.pdf.

157 See, for example, Deric Shannon, Anthony J. Nocella II, and John Asimakopolous (2012). *The Accumulation of Freedom: Writings on Anarchist Economics*. Oakland, CA: AK Press, at: https://libcom.org/files/The%20Accumulation%20of%20Freedom,%20Writings%20on%20Anarchist%20Economics%20-%20%20Deric%20Shannon%20et%20al.pdf; Michael Kwet, "Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley," [note 1], Chapter 3.