RACE & CLASS
SAGE
Los Angeles,
London,
New Delhi,
Singapore,
Washington DC,
Melbourne

Digital colonialism: US empire and the new imperialism in the Global South

MICHAEL KWET

Abstract: This article proposes a conceptual framework of how the United States is reinventing colonialism in the Global South through the domination of digital technology. Using South Africa as a case study, it argues that US multinationals exercise imperial control at the architecture level of the digital ecosystem: software, hardware and network connectivity, which then gives rise to related forms of domination. The monopoly power of multinational corporations is used for resource extraction through rent and surveillance – *economic domination*. By controlling the digital ecosystem, Big Tech corporations control computer-mediated experiences, giving them direct power over political, economic and cultural domains of life – *imperial control*. The centrepiece of surveillance capitalism, Big Data, violates the sanctity of privacy and concentrates economic power in the hands of US corporations – a system of *global surveillance capitalism*. As a feature of surveillance capitalism, Global North intelligence agencies partner with their own corporations to conduct mass and targeted surveillance in the Global South – which intensifies *imperial state surveillance*. US elites have persuaded people that society must proceed according to its ruling class conceptions of the digital world, setting the foundation for *tech hegemony*. The author argues for a different ecosystem that decentralises technology by placing control directly into the hands of the people to counter the rapidly advancing frontier of digital empire.

Michael Kwet is Visiting Fellow at the Information Society Project, Yale Law School and a PhD Candidate in Sociology at Rhodes University, South Africa.

Race & Class
 Vol. 60(4) 3–26
10.1177/0306396818823172 journals.sagepub.com/home/rac

Keywords: Big Data, Big Tech, digital colonialism, digital ecosystem, global surveillance capitalism, South Africa, tech hegemony, US multinationals

Introduction

In March 2015, South Africa's former President Jacob Zuma announced Operation Phakisa in Education (OPE), a model for fast-tracking digital technology to all 26,000 public schools. The plan was fleshed out during a two-week scoping lab organised by the World Bank, followed by a four-week lab facilitated by Deloitte with 120 participants from government, corporations, unions, schools and NGOs. Lab participants were gagged by non-disclosure agreements, and very few details have been disclosed. Two years later, the African National Congress (ANC) released a report declaring that OPE will move forward and 'paperless classrooms' will go national.[1]

If successful, the poor black majority will gain access to laptops, desktops or tablets for the first time, bringing them beyond the world of cheap mobile phones. On the surface, the project appears a step forward towards equity in a changing world. Who wouldn't want computers for poor black students? Yet the project is slated to plant US tech products inside the classroom, and it intends to incorporate Big Data surveillance across the entire education system.[2] No public debate has transpired.

The secretive initiative marks a critical moment in history: many countries in the Global South are on the verge of extending computer devices and Internet connectivity to the poor majority. How will the Global South be impacted by the spread of digital technology? More importantly, should the Global South adopt the products and models of US tech giants, or should they think differently and pursue other options? Can the countries of the Global South shape their own digital destiny?

An insidious new phenomenon, digital colonialism, casts a shadow on the Global South.[3] This structural form of domination is exercised through the centralised ownership and control of the three core pillars of the digital ecosystem: software, hardware, and network connectivity, which vests the United States with immense political, economic, and social power. As such, GAFAM (Google/Alphabet, Amazon, Facebook, Apple, and Microsoft) and other corporate giants, as well as state intelligence agencies like the National Security Agency (NSA), are the *new imperialists* in the international community. Assimilation into the tech products, models, and ideologies of foreign powers – led by the United States – constitutes a twenty-first century form of colonisation.

But there are alternative technologies, models and ideologies for constructing a digital society aligned with human rights, democracy and socioeconomic justice, for which decentralised ownership and control of software, hardware, and the Internet are prerequisites.

***

More than two decades into formal democracy, South Africa is struggling to overcome its apartheid past. Economic inequality has increased, and the country ranks among the most unequal in the world. Racial disparities are high with respect to income, wealth, employment, and education, while residential segregation has persisted. The ANC has delivered some modest services to the poor – including millions of cheap RDP (Reconstruction and Development Programme) houses, access to electricity, and small social welfare grants – yet poverty remains rampant. About 55 per cent of the population falls under the upper limit poverty line of less than $3 per day.[4] Sixty-three per cent of Africans/blacks fall below the poverty line, compared to just under 1 per cent of whites.[5] Given the outcomes of the neoliberal development path favoured by the ANC and the leading opposition party, the Democratic Alliance, some scholars are beginning to label South Africa a 'neo-apartheid' rather than a 'post-apartheid' society.

With technological integration in sight, many countries of the Global South are rushing to construct policies for twenty-first-century life. South Africa is no exception: in anticipation of its own digital transformation, the ANC recently proposed a new framework for the digital era.[6]

Despite recent attention to new technologies, members of government, NGOs, business classes and intellectuals have provided little critique of what paths are available at the architectural level. Instead, they have been aiming to 'catch up' with the North by seeking to place mainstream digital tech into every corner of society, while training South Africans in digital literacy for assimilation into US products. The published record on digital tech in South Africa fails to critique Big Tech multinationals (e.g. GAFAM, Uber and Netflix) and their models for the digital society: Big Data, artificial intelligence, and machine learning; centralised cloud services; the gig economy; the spread of CCTV surveillance; as well as industry-specific trends, such as predictive analytics in private security, policing, education, finance, and employment.

This article attempts to answer the questions entirely absent from public discourse; such as, 'are cloud centres built by Amazon, Microsoft, and Google good for the country?' or 'which technologies best promote privacy rights, transparency, collaboration, and local development?'.

Economic domination – corporate colonisation and monopoly power

Under colonialism, Europeans dispossessed the natives of their land, settled their territories, put them to work as slaves and servants, instituted horrific acts of violence, and perpetuated dependency and plunder through strategic underdevelopment. Corporations played a pivotal role through the 'pathological pursuit of profit and power'.[7] In 1602, the Dutch East India Company became the first modern global corporation. Fifty years later, it initiated European conquest in Southern Africa with the establishment of the Cape Colony.

Over the next two centuries, whites seized large swathes of land as colonists expanded into the interior. After the discovery of diamonds and gold, the British and the Afrikaners consolidated the remaining majority of land and further subjugated the African population under racist regimes of labour exploitation. In no time flat, a handful of corporations came to dominate large parts of the economy.[8]

Today, a new form of corporate colonisation is taking place. Instead of the conquest of land, Big Tech corporations are colonising digital technology. The following functions are all dominated by a handful of US multinationals: search engines (Google); web browsers (Google Chrome); smartphone and tablet operating systems (Google Android, Apple iOS); desktop and laptop operating systems (Microsoft Windows); 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 others. GAFAM now comprise the five wealthiest corporations in the world, with a combined market cap exceeding $3 trillion.[9] If South Africans integrate Big Tech products into their society, the United States will obtain enormous power over their economy and create technological dependencies that will lead to perpetual resource extraction.

Early research and case examples suggest the economic impact of Big Tech intermediaries is detrimental to local African industries. Murphy, Carmody and Surborg, who studied the role of ICTs among small, medium, and micro-sized enterprises (SMMEs) in South Africa's and Tanzania's wood and tourism industries, found that ICTs introduced the dominance of information intermediaries. Increased use of ICTs also led to greater worker surveillance in some instances. They concluded that ICT integration is, on balance, benefiting foreign-owned businesses and corporations.[10]

Similar conclusions can be derived from press accounts of the transportation industry. Since Uber began operating in Johannesburg in 2013, there have been labour strikes and violent clashes in the 'South African taxi wars'. Several e-hailing taxi murders have been carried out by metered taxi drivers, who have warned that Uber will 'burn' if it remains in South Africa. At the same time, many Uber drivers endure onerous working conditions for low pay.[11]

Uber has had devastating effects in Africa and beyond.[12] The company takes around 25 per cent commission for each trip, in addition to hidden costs,[13] leading to an outflow of revenue from the local economy to foreign coffers. Moreover, it is able to undercut local markets by offering artificially low prices: Uber can operate at a loss – to the tune of billions – thanks to funding from Wall Street and other wealthy investors.[14] With the backing of corporate finance, it leverages predatory subsidies, network effects, Big Data analytics, and the deregulatory effects of its position as an 'intermediary' to stamp out competition and colonise

the market. Within just two years, Uber sported a net worth of R1.65 billion ($125 million) inside South Africa.[15]

Similar problems have emerged in the media. In April 2017, the online news outlet *GroundUp* dropped Google Ads from its website. *GroundUp*'s Nathan Geffen explains the Google advertising model is 'broken' for publishers who 'have to put up with poor quality, misleading adverts in exchange for small change'. 'The problem', Geffen says, 'is that nearly all the power in the online advertising relationship lies with Google.' The ad giant also serves up censorship threats: in one example, Google issued a warning to *GroundUp* for publishing a picture containing a painted bare breast as part of a protest action.[16]

In November 2017, *Financial Mail*'s Anton Harber wrote a feature story deeming Google and Facebook 'the biggest threat to South African news media'.[17] Google takes 70 per cent of local online advertising, while social media – led by Facebook – takes another 12 per cent. The major South African media groups are left with just 8 per cent of the pie. The Google and Facebook 'nemesis' is an expanding duopoly: the two take 77 per cent of online advertising spend in the US and captured virtually all the ad growth in 2016.[18] If this continues, Harber exclaims, 'the big two could have a devastating effect on the media's role in defining democracy'.[19]

These early examples provide clear instances of digital colonialism whereby foreign corporations undermine local development, dominate the market, and extract revenue from the Global South, with power obtained primarily through the *structural* domination of digital architecture, which leads to more general forms of *imperial control*.

Imperial control through architectural design

Colonial conquest typically entails dispossession of valuable resources from the native peoples and ownership and control of infrastructure by colonial powers. In many parts of the Global South, critical infrastructure such as railways was designed by foreign imperialists not to benefit the indigenous population, but to service the mother country. In the arrangement that emerged through European colonialism, raw materials were extracted by exploited local labour and shipped back to the empire. In some cases, colonial forces would import the cheap, machine-made industrial products to the villages, undermining local artisans and the capacity to build competitor industries. In Africa and elsewhere, railroads were built from the country interior straight to the ports and military stations, with little 'spread effect' to connect up the indigenous people. The architectural design of the production system was not engineered to benefit the local inhabitants, but to 'serve immediate European needs'.[20]

Under digital colonialism, foreign powers, led by the US, are planting infrastructure in the Global South engineered for their own needs, enabling economic and cultural domination while imposing privatised forms of governance. To

accomplish this task, major corporations design digital technology to ensure their own dominance over critical functions in the tech ecosystem. This allows them to accumulate profits from revenues derived from rent (in the form of intellectual property or access to infrastructure) and surveillance (in the form of Big Data). It also empowers them to exercise control over the flow of information (such as the distribution of news and streaming services), social activities (like social networking and cultural exchange), and a plethora of other political, social, economic and military functions mediated by their technologies.

The control of code is foundational to digital domination. In *Code: and Other Laws of Cyberspace*, Lawrence Lessig famously argued that computer code shapes the rules, norms and behaviours of computer-mediated experiences in ways similar to architecture in physical space (e.g. imperial railways designed for colonisation).[21] 'Code is law' in the sense that it has the power to usurp legal, institutional and social norms impacting the political, economic and cultural domains of society. This critical insight has been applied in fields like copyright, free speech regulation, Internet governance, blockchain, privacy, and even torts. What has been missed, however, is how US dominance of code – and other forms of digital architecture – usurps other countries' sovereignty.

Digital forms of power are linked through the three core pillars of the digital ecosystem: software, hardware and network connectivity.[22] (Software is the set of instructions that define and determine what your computer can do. Hardware is the physical equipment used for computer experiences. The network is the set of protocols and standards computers use to talk to each other, and the connections they make.)

Software functions as the coded logic that constrains and enables particular user experiences. For example, software determines rules and policies such as whether or not users can post a message anonymously at a website, or whether or not users can make a copy of a copyright-restricted file like an e-book. The rules that a programmer codes into the software largely determine technological freedoms and shape users' experiences using their devices. Thus, software exerts a powerful influence on the behaviour, policies and freedoms of people using digital technology.

Control over software is a source of digital domination primarily exercised through software licences and hardware ownership. Free Software licences allow people to use, study, modify and share software as they see fit.[23] By contrast, non-free software licences grant a software designer control over users by precluding the ability to exercise those freedoms. With proprietary software, the human-readable source code is closed off to the public, and owners usually restrict the ability to use the software without paying. In the case of Microsoft Windows, for example, the public must pay for the programme in order to use it, they cannot read the source code to understand how it works, they cannot change its behaviour by changing the code, and they cannot share a copy with others. Thus with proprietary licensing, Microsoft maintains absolute control over how the

software works. The same goes for other proprietary apps, like Google Play or Adobe Photoshop.[24] By design, non-free software provides the owner power over the user experience. It is authoritarian software.

Control over hardware is a second source of digital domination. This can take at least three forms: software run on third-party servers, centralised ownership of hardware, or hardware designed to prevent users from changing the software.

In the first scenario, software is executed on someone else's computer. As a result, users are dispossessed of their ability to control it. This is typically accomplished through Software as a Service (SaaS) in the cloud. For example, when you visit the Facebook website, the interface you are provided executes on third-party hardware (i.e. on Facebook's cloud servers). Because users cannot change the code running on Facebook's servers, they cannot get rid of the 'like' button or change the Facebook experience. 'There is no cloud', the saying goes, 'just someone else's computer'. Corporations and other third parties design cloud services for remote control over the user experience. This gives them immense power over individuals, groups and society.[25]

In the second scenario, people become dispossessed of hardware ownership itself. With the rise of cloud computing, it is possible that hardware manufacturers will soon only offer low-powered, low-memory devices (similar to the terminals of the 1960s and 1970s) and computer processing and data storage will be primarily conducted in centralised clouds. With end-users dispossessed of processing power and storage, software and data would be under the absolute control of the owners and operators of clouds.[26]

In the third scenario, hardware is manufactured with locks that prevent users from changing the software on the devices. By locking down devices to a predetermined set of software choices, the hardware manufacturer determines which software is allowed to run when you turn on your device.[27] Thus, hardware restrictions can prevent the public from controlling their devices, granting device manufacturers power over users.

Control over network connectivity is a third source of digital domination. Net neutrality regulation proposes that Internet traffic should be 'neutral' so that Internet Service Providers (ISPs) treat content flowing through their cables, cellular towers and satellites equally. According to this philosophy, those who own the pipes are 'common carriers' and should almost never be allowed to manipulate the data that flows through them.[28] This constrains the ability of wealthy media providers to pay for faster content delivery speeds than less wealthy providers (such as grassroots organisations, small businesses, and common people). More importantly, by treating traffic equally, net neutrality prevents network discrimination against various forms of traffic critical to civil rights and liberties. For example, the Tor browser facilitates anonymous Internet communications, but the use of the Tor network can be detected by ISPs and throttled (i.e. slowed to a crawl).[29] Net neutrality prevents this form of discrimination and protects the end user's freedom to utilise the Internet as they wish, without third-party

favouritism, blocking, or throttling. Let us consider some concrete examples as to how software, hardware, and networks constitute sources of power and control related to social justice in the Global South.

Intellectual property and empire

The copyright industry is threatened by the mass sharing of paywalled publications over the Internet (what they label 'piracy'). Given that hard drive capacity and Internet speeds will rapidly increase over time, the capacity to share vast libraries of music, movies, books, and other media is steadily increasing. What will be done when each person has a 40 terabyte hard drive and can trade the entire collection of popular music from the last century within an hour? Advances in technology deepen the need for architectural control to police the copyright system.

One way to stop file sharing is to control software. The industry built Digital Rights Management (DRM) software, for example, to prevent copyright-restricted publications from playing on a user's computer unless the user pays to access it first. This works well with proprietary software because users cannot remove the DRM. (However, if the DRM software is Free Software – which allows people the freedom to use, study, modify and share the software – people can remove the DRM code that locks the content.) Thus, industry is bolstered by proprietary software as a means to enforce copyright.

A second way to prevent sharing is to take control of the hardware. If, for example, people stop running software on their own devices, and instead run their computer experiences through centralised cloud servers, then cloud providers can determine their 'access' to copyrighted data. In this scenario, users cannot copy and trade media over the Internet because the data 'streams' to their device from a content owner's platform (e.g. Netflix or Spotify) which provides media content through its servers. Thus, the widespread distribution of storage capacity and broadband Internet threatens the copyright monopoly.[30]

A third way to prevent sharing media is to control the network. People may own and control their software and hardware, but if they can be spied on by an ISP or government, then they can be fined or arrested for copyright infringement, or have their Internet connection throttled or terminated. People might use privacy protection technologies to conceal their content sharing – such as the Tor network or Virtual Private Networks (VPNs) – but this can be thwarted by ISPs throttling Tor or VPNs. In this scenario, control of the network (ISP discrimination) is used to make anonymous content sharing impractical. Thus, public control of the network threatens copyright enforcement.

To bring this back to colonialism, US multinationals have designed digital architecture which, in one way or another, allows them to accumulate vast fortunes based on rent or data extraction. In the case of copyright, control over software, hardware, or the Internet is used to protect the copyright monopoly in the name of intellectual property rights. Given that the marginal cost of producing

digital works is near-zero, prominent intellectuals and activists have challenged copyright paywalls in the interest of socioeconomic justice and out of concern that draconian technologies are needed to enforce digital forms of copyright.[31] Free access to digital publications for all people on planet earth, irrespective of their wealth, could improve education, culture, equality, democracy, and innovation. Western technology has been engineered to block free sharing, which impoverishes poor people's ability to obtain knowledge and culture, and reduces communication between rich and poor.

Intellectual property rights date back centuries, but they became a fixation of the West in the late twentieth century as western corporations came to dominate intellectual property. Despite strong IP protections, much of the development in the domain of technological innovation has been driven by the public sector. The Internet, GPS, multi-touch screens, HTML, the Siri virtual personal assistant, LCD displays, microprocessors, RAM memory, hard disk drives, Google's search algorithm, and lithium-ion batteries were all developed by public institutions or with a heavy dose of public funding.[32] Additionally, 80 per cent of basic scientific research and development in the US is funded by government and non-profit sectors.[33] Thus the foundational knowledge and technologies of the digital world have been largely driven by state-led research and development.

The expansion of copyright protections is also a recent phenomenon. The United States did not observe foreign copyrights until the end of the nineteenth century. For about a century prior, it printed copyrighted works produced by Europeans without paying licensing fees. As its own domestic industry developed, the US changed its tune in order to protect its local content industry. Initially, copyrights lasted just fourteen years, with a right of renewal for another fourteen years. By the end of the twentieth century, the US muscled the international community into accepting lengthy copyright terms (life of the author plus several decades). While the US (and other countries) built up its knowledge economies without respecting foreign copyrights, today it seeks to 'kick away the ladder' and impose extensive copyright restrictions on the rest of the world.

Countries in the Global South have accepted these terms in large part because of the pressures exerted through international trade agreements and organisations. In particular, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by the World Trade Organization (WTO), requires member countries to provide a number of intellectual property protections, including copyright and patents. Developing countries have ratified TRIPS because it is a necessary prerequisite to membership in the WTO.[34] In 2004, developing countries, including South Africa, proposed a development agenda at the World Intellectual Property Organization (WIPO) that would bridge the 'knowledge gap' and 'digital divide' through 'public interest flexibilities' with respect to intellectual property.[35] While recommendations made in 2007 included special considerations for developing countries (e.g. technology transfer and increased research sharing), they are far from demanding the drastic weakening of

intellectual property rights.[36] If copyrights and patents are to be reduced or phased out, developing countries and developed world allies will have to push for a shift to government procurement of knowledge production.[37]

Big Tech Internet service provision

Facebook's Free Basics service offers another case of how Big Tech corporations expand empire in the Global South. Free Basics offers a stripped-down version of free Internet services to people with little or no disposable income. Facebook decides which content and websites the poor can access – while conveniently providing Facebook itself within the app. Free Basics is zero-rated by ISPs, meaning that data transfers inside the app are paid for by ISPs instead of their customers. The ISPs hope that the limited Internet experience will lead to paying customers who, having tasted a free sample, will purchase data for the full experience. Free Basics not only has Facebook playing Internet gatekeeper of the poor, it also violates net neutrality laws: zero-rated offerings place content providers on an unequal footing. Several countries have terminated Free Basics, in part due to popular backlash.[38] However, Internet.org has put over 100 million users from over sixty countries, including South Africa, into the Facebook platform, which channels them towards the Facebook ecosystem.

Integrating platforms like Facebook outside the US does more than drain local advertising revenue: it undermines various forms of local governance. Seventy-five per cent of web publisher's traffic now comes from Google (46 per cent) and Facebook (29 per cent).[39] Centralisation of services into their hands provides them with centralised control over communications – by way of code. These two firms filter search results and news feeds with proprietary black box algorithms, granting them enormous power to shape who sees what news. Leftist outlets have published data suggesting that Google censors socialist views, while Facebook has been found to favour mainstream liberal media.[40]

Platforms also regulate freedom of speech and association.[41] If an online social network detects certain keywords and forms of speech, it can censor it, or ban the user. Moreover, it can prohibit the right to associate with others in the pursuit of social, political, economic, cultural and religious ends. This has been carried out against Palestinians (e.g. with the removal of the page for the political party, Fatah), as well as the far Right.[42] As private overlords of critical information infrastructure, US multinationals have the power to regulate the press, speech and association in foreign territories, as they see fit. And corporations increasingly profit from Big Data surveillance, an exploitative human rights transgression against the Global South.

Global surveillance capitalism

From a historical perspective, surveillance capitalism is nothing new. During the era of slavery, racial phenotypes were used by Europeans to identify fugitive

slaves, while various surveillance tactics were used to police black bodies. In South Africa, colonists instituted pass laws and branded the skins of blacks and livestock to segregate the people and control black labour.

In the digital era, surveillance capitalism has been variously interpreted. In the mid-2000s, criticisms of Internet surveillance began to mount and, in 2014, the term 'surveillance capitalism' was coined by several prominent scholars in a special summer issue of *Monthly Review*, in which the authors focused on state-corporate surveillance, commercial exploitation, and Internet governance. Other scholars have devoted attention to issues like data monetisation and algorithmic discrimination.

Big Data is the central component of surveillance capitalism. Corporations and states are collecting, storing and processing enormous centralised databases of information about the world's netizens. This enables them to infer traits about people (such as their sexuality, religion, political affiliations and behavioural tendencies) that individuals do not disclose themselves. The data is then used to manipulate individuals, groups and organisations for the interests of corporate profits and state power.

The Big Data society is a project for total surveillance of the human species. Harnessing advanced statistics and artificial intelligence to make sense of enormous troves of data, corporations and governments seek God-like omniscience to manage the population. Much of the data collection is made possible by centralisation in the cloud. The presence of Big Tech multinationals in the Global South extends the reach of surveillance capitalism to its inhabitants – with the US empire at the centre.

By its very design, Big Data violates privacy. To make sense of the gargantuan data sets collected, data miners make heavy use of artificial intelligence. AI typically 'learns' by analysing enormous datasets for the purpose of predicting outcomes. When applied to people, it collects personal and historical information to predict the future. Because machines do not 'think', Big Data must derive its predictive accuracy from the richness of data that can be collected about individuals and groups. Given that massive amounts of data are needed, it generally requires mass surveillance.

Additionally, those who have access to the most valuable *types* of data, coupled with vast *quantities* of it, have a supreme advantage over competitors. Facebook, for example, has access to over two billion people's sensitive information – what they 'like', who they are friends with, who they talk to, where they travel physically, and so on. Google dominates search engines, as well as data from its ad services and smartphone activity (via Google Android). Amazon has unique and valuable commercial data, including the habits of their customers while they are shopping at Amazon.com (the market funnel), their entire purchase histories, plus whatever other data they capture or acquire. Few companies can amass these *kinds* of data sets.

It is nearly impossible for Global South firms to compete with these established giants, for a number of reasons. First, network effects create considerable barriers

to entry for competition. With network effects, the more users in a network, the more valuable that network becomes. Online platforms tend to concentrate user bases because the more users they have, the better the network is. Just as people do not want to have fifty different telephones on fifty separate networks, they do not want to have fifty social media accounts. They also do not want to have many separate e-hailing services, search engines, e-commerce platforms, and so on.

Second, economies of scale pose serious barriers to entry. It is very expensive to run centralised social networks because cloud infrastructure is costly, quality products require teams of skilled programmers, data must be curated effectively, and the service must be monetised to cover those costs. Moreover, competitors include multi-billion dollar corporations, which already dominate the market, enjoy the benefit of network effects, have accumulated brand equity and trade secrets, and have the power to acquire smaller companies.

This leads to a dynamic where the largest sets of valuable data – such as social data (Facebook, Twitter), e-commerce (Amazon), and search (Google) – are dominated by a handful of 'winners' (multinationals). Even corporations and countries within the Global North are beginning to express concerns about the data monopolisation tied to Big Data and AI.[43] However, simple reforms will not fix the problem, because the structural design of the ecosystem favours concentration. There is little reason to believe the Global South will produce viable competitors.

With surveillance the new revenue model for tech, the world's people are subjects of the state-corporate ruling class in the US.[44] Under this arrangement, the overly capacious term 'Big Data' has been used to gloss over surveillance activity and power dynamics. Applied to humans, Big Data is little more than a euphemism for surveillance. Extraction and monetisation of sensitive human information yields substantially different economic and ethical outcomes than, say, oil extraction by machines. Producing 'ethical Big Data' for people, as some scholars advocate, is akin to 'clean coal' for the environment.

Surveillance capitalism thus presents society with an unethical privacy downgrade that leaves the Global South disadvantaged. Like the railroads of empire, surveillance capitalists extract data out of the Global South, process it in the metropolitan centre, and spit back information services to colonial subjects, who cannot compete. To make matters worse, with such large, pristine databases in the hands of the private sector, intelligence agencies, led by the United States, piggyback off US corporations for their own mass surveillance programmes. As whistleblowers have revealed, most (if not all) of the large US tech giants are partnered to the National Security Agency.[45] Global North domination of technical architecture thus enables another element of digital colonialism – state surveillance – rendering it even more problematic.

Imperial state surveillance

Alfred McCoy details the genesis of the global surveillance state in his seminal work, *Policing America's Empire*. During the late nineteenth century, McCoy

writes, the technological capacity for mass surveillance was created through 'America's first information revolution' whereby the quadruplex telegraph, commercial typewriter, Dewey decimal system, biometrics, photographic files, and the Hollerith punched card machine combined to enable 'the management of textual, statistical, and analytical data'.[46] Using the latest technologies, the US military identified, recorded and analysed networks of Filipino/a leaders, as well as their finances, property, political loyalties and kinship networks. The surveillance information was used to pacify resistance to American conquest.

In South Africa, the US has long participated in surveillance activities. At the turn of the nineteenth century, US mining officials working in South Africa pushed for the surveillance of black miners. In 1897, a leading American engineer, Sydney Jennings, praised the 'most excellent' pass laws, testifying that 'if properly carried out, and efficiently administered, [they] will enable us to get complete control over our kaffiri labourers'.[47]

At mid-century, the United States upped its participation, this time in support of apartheid. IBM supplied the punched card system used to denationalise Africans and register the population under the four-category race system (African, Coloured, Indian and White). By the end of the 1970s, it won the contract for the Book of Life reference register system designed to expand panoptic surveillance to the entire population.[48] Other US corporations profited from business in the region by providing white supremacists the arms, vehicles, energy resources, financial support and computers used to systematically oppress blacks.[49] American intelligence also targeted anti-apartheid activists. During the post-second world war period, the CIA supported white liberal anti-communist student programmes in the South African university system, and they likely helped arrest Nelson Mandela in 1962.[50] In July 2018, thousands of declassified documents revealed FBI surveillance of Nelson Mandela and extensive investigations into the anti-apartheid movement.

US contributions to surveillance inside South Africa receded with the transition from apartheid to democracy. With the spread of digital technology, however, its role has re-emerged. During the 2000s, a handful of whistleblowers revealed the existence of global mass and targeted surveillance programmes carried out by the US intelligence community. A cache of National Security Agency documents leaked by Edward Snowden details many of these. The NSA utilises two primary methods for data collection: partnerships with corporations (via the PRISM programme) and the tapping of the Internet backbone (via the UPSTREAM programme). The extent of the NSA's data collection can be estimated by the size of its storage facilities, such as its $2 billion, 25,000 square-foot facility in Bluffdale, Utah. According to NSA whistleblower William Binney, the facilities collect trillions of phone calls and emails, in addition to sources like banking and social networking.[51]

Western intelligence agencies have used surveillance to target economic and human rights organisations. For example, Britain's Government Communications

Headquarters (GCHQ) attempted to retrieve the briefings of the South African delegates to G20 and G8 summit meetings. It also breached the European Convention on Human Rights for spying on the South African-based Legal Resources Centre (LRC), a public interest clinic dedicated to defending human rights.[52]

The deployment of Big Tech products in the Global South extends the eyes and ears of foreign intelligence. The US stranglehold over tech infrastructure, combined with a vast pool of resources, provides it with leverage over other countries. When countries like South Africa want information about a person of interest, they must apply through the Mutual Legal Assistance Treaty to access private information from social networking platforms like Twitter or Facebook. US spy agencies, by contrast, can demand access in the name of national security. Power asymmetries thus give the Global North the upper hand in data-sharing agreements. The US also possesses superior resources to exploit Big Data: it houses the most advanced equipment in the world, and has an army of advanced mathematicians and computer scientists to make sense of data repositories. Countries in the Global South, by comparison, have a small budget, a paltry repository of data, and less capacity to analyse large data sets. In the domain of state-corporate surveillance, the Global North holds the power. It is therefore in its interest to maintain structural control of the tech ecosystem.

Tech hegemony – ideological domination

Colonialism was not just a physical act of aggression, it was an ideology formed to justify conquest and pacify resistance. In South Africa, Afrikaners appealed to select passages in the Bible to cast themselves as God's chosen people for settling occupied land. During the nineteenth century, Europeans formulated the theory of biological race in service of capitalist exploitation. Britain's Francis Galton played a key role: his theories of race were developed over a two-year trip to Southern Africa (extending from the Cape up to present-day Namibia), where he developed extreme disdain for Africans. Soon thereafter, Galton coined the term 'eugenics' and improved the fingerprinting techniques introduced to South African police forces in 1900 by Sir Edward Henry. Galton went on to revolutionise the field of statistics, inventing the concepts of statistical correlation and regression to the mean, which were marshalled in service of social Darwinist ideologies of racial intelligence enthusiastically accepted by the British intellectual classes.[53]

Indeed, doctrines of domination – be it through religious missions, racial ordering, appeals to nationalism or 'civilising' duties – pervaded colonial society. Under apartheid, Africans received dumbed down 'Bantu education' designed to instil deference to Europeans in preparation for a life of menial labour and servitude. As Walter Rodney put it, 'Colonial schooling was education for subordination, exploitation, the creation of mental confusion and the development of underdevelopment.'[54]

In the twenty-first century, Big Tech corporations have fashioned a new 'Manifest Destiny' for the digital age. Western doctrines glorify Big Data, centralised clouds, proprietary systems, smart cities littered with surveillance, automation, predictive analytics, and similar inventions. Commentators may acknowledge potential deficiencies – the loss of privacy, job losses to machines, or algorithmic discrimination – but consider the core technologies an inevitable part of technological 'progress'. In South Africa, this narrative is delivered via World Economic Forum founder Klaus Schwab's theory of the so-called[55] 'Fourth Industrial Revolution' (4IR), which privileges the private sector and promotes the trending instruments of domination characterising digital capitalism. South African politicians, journalists and intellectuals (featured in the media) have internalised his doctrine. Scarcely an article or radio show discussing technology fails to mention the 4IR.

Meanwhile, South African elites are attempting to fast-track Big Tech products into the classroom behind closed doors through Operation Phakisa Education. Poor students and families are dependent upon the state to provide a more equal digital experience by subsidising access to productivity devices (such as laptops, desktops or tablets) and high-speed broadband. The importance of technology choices for schools cannot be overstated: the specific technologies deployed will forge path dependencies by shaping the habits, preferences and knowledge base of the first tech generation from childhood. Education offers the ultimate breeding ground for Big Tech imperialism; product placement in schools can be used to capture emerging markets and tighten the stranglehold of Big Tech products, brands, models and ideology in the Global South. The youth will be more likely to consume the products they receive in school as adults, while the future generation of tech developers will likely become developers of products for the ecosystems they grow up using: Microsoft, Google, Apple – or Free Software like GNU/Linux.

Despite the ramifications of going digital, published voices are calling for assimilation, with no substantive debate. As University of Witwatersrand Vice Chancellor Adam Habib put it, 'Considerations of [technological innovations] have not even entered the public discourse and we are at a collective risk of once again merely being victims of economic forces and processes beyond our control.' Like so many others in South Africa, however, Habib has so far bought into the 4IR narrative.

The Free Software Movement

Big Tech colonisation in South Africa can be countered with publicly owned and controlled technology built for freedom *by design* at the architectural level. The Free Software Movement (FSM) has been at the forefront of this political struggle. The FSM developed within the centre of empire in response to enclosure of the software commons, first through proprietary software and now through Internet

centralisation. It has concentrated on developing forms of technology that grant control to individuals and communities for the purpose of individual and collective freedom. During the 2000s, Free Software (also called Free and Open Source Software (FOSS)) was endorsed for public sector implementation across the Global South, including in South Africa. The development and dispersion of the Free Software philosophy across the world resembles the development of socialism within Europe as a reaction to land enclosure and industrial exploitation, and its subsequent spread across liberation movements throughout the world.

Software is a central component of freedom in the twenty-first century. Because software largely determines what your computer can do, it shapes your level of digital freedom. This insight led MIT computer programmer Richard Stallman to found the Free Software Movement in 1983. He recognised that if you would like to change how a feature on your computer works, fix a bug with a patch, or remove an undesirable feature imposed on you by the software developer, then you must be able to access and modify the programme's source code. Certain freedoms are thus necessary for users to be able to control how their devices work, so that they may control their experience when using them.

Four essential freedoms define Free Software: the freedom to run the programme as you wish; the freedom to study how the programme works, and change it; the freedom to redistribute verbatim copies; and the freedom to distribute copies of your modified versions to others. Access to the source code is a precondition of the first and third freedoms above.[56] Taken together, these four freedoms enable the individual and collective control essential to freedom. From a communal perspective, they make it possible for a group of users to work together and change the programme to do what they together want it to do. Any software that grants the four essential freedoms is called 'Free Software'.[57]

Impressed by the anti-possessive design of Free Software, Archbishop Desmond Tutu has endorsed the FSM. Introducing Stallman at the University of Western Cape in 2007, he stated:

> 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 … 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.[58]

Free Software alone, however, cannot provide the freedom to control technology. In *Die Gedanken Sind Frie*, Columbia law professor Eben Moglen developed a framework that provides a more complete account of the digital ecosystem. According to Moglen, the three core pillars of the digital ecosystem must be arranged to prevent authoritarian forms of digital technology. Software must be Free Software so that the public has the capacity to control its devices; hardware

must be Free Hardware without digital locks and widely distributed in the hands of the people;[59] and the Internet must be neutral and provide bandwidth for all people on equal terms.

Moglen adds that the trio of Free Software, Free Hardware and Free Spectrum (network connectivity) form the foundation for Free Culture, whereby anyone with a device and the Internet can freely access, produce and share published works.[60] Taken together, the core pillars of the digital ecosystem are essential components which, by their very freedom and openness, empower the public – rather than states, corporations, or any other third parties – to exercise direct and collective control over the devices and ecosystem shaping their lives. In 2016, Edward Snowden echoed this sentiment, stating, 'we're very rapidly approaching a point in human history where we will need to seize the means of our communication'.[61] Digital rights advocates argue that new technology is needed to decentralise the Internet, secure privacy, and subvert centralisation in the cloud.

Internet decentralisation

The present client-server network model has billions of users as clients at the edge requesting information from a small number of (predominantly corporate) servers in the centre who process, store and deliver information back to the clients. This architecture is problematic as it confers enormous power on corporations and states, which own and operate the clouds. In a global context, this model facilitates colonial dispossession.

As an antidote to this dilemma, the Free Software Movement is building decentralised networking alternatives. In February 2010, Eben Moglen and his colleagues launched the FreedomBox project in reaction to cloud centralisation. The project is designed to run a secure, personal server that protects privacy and provides infrastructure for communities to network their online activities without the need for centralised intermediaries. On this model, users run the FreedomBox (Free and Open Source) software on a device in their home. They may install it on a small, inexpensive device plugged into the wall which operates as a personal cloud. It offers a wireless access point and a hard drive that stores users' personal data, so they can access their information from any device over the Internet. It operates as a personal privacy protector: with the click of a button, users can enable Tor, and it will route their traffic through the Tor network to provide them with anonymity. It offers other services, such as private email and ad blocking. Crucially, FreedomBox allows the decentralised hosting of alternative platforms built for privacy, such as the GNU Social and Mastodon social networks, through either peer-to-peer or highly decentralised networks with servers based in local communities. On the FreedomBox model, each unit functions as a client *and* a server. The technology is explicitly designed to retrofit decentralisation into the Internet.[62]

To be sure, there are problems that new technologies do not (or cannot) address. For example, cellular data communications are not sufficiently covered by FreedomBox and require new technologies and legal solutions to curtail mobile surveillance.[63] Online purchases for home delivery and the expansion of 'smart' CCTV surveillance offer privacy challenges that cannot be fixed with alternative technologies. Activism and regulations such as Jack Balkin and Jonathan Zittrain's information fiduciaries proposal will play a critical role in emerging technological struggles, in addition to broader struggles over socioeconomic justice. With information fiduciaries, companies must exercise duties of loyalty, care and trust in how they handle your data.[64] Nevertheless, these kinds of regulations have limitations, as they do not prevent the mass collection of personal data. By contrast, a free and open Internet based on Free Software, Free Hardware, and decentralised (neutral) networking would drastically reduce digital domination by curtailing network effects; undercutting monopolies; resisting censorship; blocking critical forms of Big Data and state surveillance; eliminating authoritarian software controls; building in transparency; making technology and knowledge more affordable and accessible to the poor; and facilitating customisation, diversity and local control.[65]

New decentralisation technologies have to be user-friendly with simple interfaces accessible to the masses; millions and then billions of people need to use them instead of surveillance services; devices must be affordable to the poor; ISPs must be prohibited from throttling technologies such as Bit Torrent and Tor; and sufficient funding is needed for development. Because these kinds of changes strike at the heart of the world's empire, they require a strong movement driven from below. Popular participation, education, activism and legal innovation are critical to countering tech hegemony.[66]

Resisting ideological domination

There are real alternatives. Activists, parents, students, teachers and policy-makers can put People's Tech for People's Power into the hands of teachers, learners and their families. Schools can become places to equip the Global South with technologies that facilitate education, sharing, individual and collective control and ownership, direct democracy, local sovereignty, real privacy, and the capacity for local business and innovation in an attempt to drive foreign imperialists out of their countries and forge a new digital society.

Yet these issues are missing from public debate. In the North, critics focus on the problems of algorithmic discrimination, fake news and the need for regulation to temper the power of Big Tech. However, loose privacy and anti-trust regulations that keep technical architecture intact will not rein in Big Tech, nor will they sufficiently constrain its global reach.

New technologies are often viewed as something that 'comes out' on the market rather than products designed with particular values and power relations

embedded in them. From an engineering perspective, it does not have to be this way: digital technology can be owned and controlled by the popular classes. Discussions around tech should be holistic and address structural inequality, identity, culture, and politics.[67] It is not enough to focus on US and European experiences when thinking about the digital world, as most discussions do in the North. Many countries in the Global South are digitising their societies, and the ecosystem must be viewed from a global perspective. A paradigm shift is needed to change the focus from outcomes on the surface for Westerners (in domains like privacy and discrimination) to structural power at the technical architectural level within a global context.[68]

South Africa has the capacity to address this task and develop a grassroots movement against digital colonisation. During the 1970s and 1980s, anti-apartheid activists protested against IBM and other corporations supplying computers for apartheid. In the 1980s, they launched the People's Education for People's Power movement in support of direct democracy in education. During the 2000s, they fought and won a battle to access generic HIV/AIDS medication. Led by the Treatment Action Campaign, activists waged a successful war against the intellectual property rights of Big Pharma. Today, South Africans and others in the Global South are preparing to push back against imperial technology. It remains to be seen what specific objections will be made and what alternatives will be proposed. Without structural changes, the march of technological 'progress' will resemble the colonial past. A movement from below could ignite a global movement against digital colonialism and for technology built for freedom.

References

1 *African National Congress*, '54th National Conference: report and resolutions', December 2017, p. 26, http://www.anc.org.za/sites/default/files/54th_National_Conference_Report.pdf.

2 Michael Kwet, 'Operation Phakisa Education: why a secret? Mass surveillance, inequality, and race in South Africa's emerging national e-education system', *First Monday* 22, no. 12 (2017), https://firstmonday.org/ojs/index.php/fm/article/view/8054/6585; Michael Kwet, 'Big Brother set to watch each pupil',' *Mail & Guardian*, 8 December 2017, https://mg.co.za/article/2017-12-08-00-big-brother-set-to-watch-each-pupil.

3 Michael Kwet, 'Break the hold of digital colonialism', *Mail & Guardian*, 29 June 2018, https://mg.co.za/article/2018-06-29-00-break-the-hold-of-digital-colonialism.

4 Kate Wilkinson, 'Factsheet: South Africa's official poverty numbers', *Africa Check*, 15 February 2018, https://africacheck.org/factsheets/factsheet-south-africas-official-poverty-numbers.

5 Kate Wilkinson, 'Mail Online's claim of 400,000+ poor whites in South Africa incorrect', *Africa Check*, 19 April 2016, https://africacheck.org/reports/mail-onlines-claim-of-400000-poor-whites-in-south-africa-incorrect.

6 *African National Congress*, 'Communications and the Battle of Ideas: discussion document', 2017, http://www.anc.org.za/sites/default/files/National%20Policy%20Conference%202017%20Communications_1.pdf.

7 Joel Bakan, *The Corporation: the pathological pursuit of profit and power* (New York: Free Press, 2005); Dominique Lapierre, *A Rainbow in the Night: the tumultuous birth of South Africa* (Cambridge, MA: Da Capo Press, 2009).

8 Martin Legassick, 'South Africa: capital accumulation and violence,' *Economy and Society* 3, no. 3 (1974), pp. 259–64.
9 *The Daily Records*, 'Top 10 largest companies in the world by market cap', 26 March 2018, http://www.thedailyrecords.com/2018-2019-2020-2021/world-famous-top-10-list/highest-selling-brands-products-companies-reviews/largest-companies-world-by-market-cap-most-valuable/12829.
10 James T. Murphy, Pádraig Carmody and Björn Surborg, 'Industrial transformation or business as usual? Information and communication technologies and Africa's place in the global information economy', *Review of African Political Economy* 41, no. 140 (2014).
11 Rumana Akoob, 'Uber will "burn" if it continues to run, say metered taxi drivers,' *Mail & Guardian*, 10 March 2017, https://mg.co.za/article/2017-03-10-uber-will-burn-if-it-continues-to-run-say-metered-axi-drivers; Gadeeja Abbas, 'Attack on Uber "a warning"', *Cape Argus*, 11 July 2016, https://www.iol.co.za/news/attack-on-uber-driver-a-warning-2044206; Kimon de Greef, 'Uber and out: drivers in Cape Town are working 24-hour shifts for low pay', *GroundUp*, 26 May 2016, https://www.groundup.org.za/article/uber-and-out-drivers-cape-town-are-working-24-hour-shifts-low-pay.
12 Camilla Houeland, 'What is Uber up to in Africa?', *Africa is a Country*, 9 March 2018, https://africasacountry.com/2018/04/what-is-uber-up-to-in-africa; Amanda Erickson, 'India's Uber drivers went on strike because they're making $3 a day', *Washington Post*, 19 March 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/03/19/indias-uber-drivers-went-on-strike-today-because-theyre-making-almost-nothing.
13 Ridester Staff, 'Uber fees: how much does Uber pay, actually? (With case studies)', *Ridester*, 16 July 2018, https://www.ridester.com/uber-fees.
14 Hubert Horan, 'Will the growth of Uber increase economic welfare?', *Transportation Law Journal* 44, no. 33 (2017), pp. 38–44.
15 Rumana Akoob, 'Here's why metered taxis are so pissed off with Uber in South Africa', *The Daily Vox*, 22 September 2017, https://www.thedailyvox.co.za/heres-why-metered-taxis-are-so-p-d-off-with-uber-in-south-africa-rumana-akoob.
16 Nathan Geffen, 'Why we're dropping Google ads', *GroundUp*, 10 April 2017, https://www.groundup.org.za/article/why-were-dropping-google-ads.
17 Anton Harber, 'How Google and Facebook are the biggest threat to South African news media', *Financial Mail*, 16 November 2017, https://www.businesslive.co.za/fm/features/cover-story/2017-11-16-how-google-and-facebook-are-the-biggest-threat-to-south-african-news-media.
18 Matthew Ingram, 'Google and Facebook account for nearly all growth in digital ads', *Fortune*, 26 April 2017, http://fortune.com/2017/04/26/google-facebook-digital-ads.
19 Harber, 'How Google and Facebook are the biggest threat to South African news media'.
20 Mario Azevedo, 'The human price of development: the Brazzaville railroad and the Sara of Chad', *African Studies Review* 24, no. 1 (1981), p. 3. See also, L. S. Stavrianos, *Global Rift: the Third World comes of age* (William Morrow & Co, 1981), pp. 176–91; G. H. Pirie, 'The decivilizing rails: railways and underdevelopment in Southern Africa', *Journal of Economic and Social Geography* 73, no. 4 (1982); Rémi Jedwab, Edward Kerby and Alexander Moradi, 'How colonial railroads defined Africa's economic geography', *VoxEU*, 2 March 2017, https://voxeu.org/article/how-colonial-railroads-defined-africa-s-economic-geography.
21 See also, Joel Reidenberg, 'Lex Informatica: the formation of information policy rules through technology', *Texas Law Review* 76, no. 3 (1998).
22 Eben Moglen, '"Die gedanken sind frei": free software and the struggle for free thought', Wizards of OS 3, opening keynote, 10 June 2004, http://moglen.law.columbia.edu/publications/berlin-keynote.html. The digital ecosystem is complex and there many elements not covered in this article, such as protocols, standards, and organisational bodies. To keep the discussion manageable, this article keeps to more basic considerations about software, hard-

ware and network connectivity. For literature on these topics, see, *inter alia*, Laura DeNardis, *The Global War for Internet Governance* (New Haven, CT: Yale University Press, 2014); Yochai Benkler, 'Degrees of freedom, dimensions of power', *Dædalus* 145, no. 1 (2016).

23 Gnu.org, 'What is free software?', *Gnu.org*, 12 June 2018, https://www.gnu.org/philosophy/free-sw.en.html. See Section II for a discussion of free software.

24 Some non-free software is proprietary, but users are allowed to use it and share it for free (e.g. Skype). However, because it is non-free (the code remains closed off to the public), Skype retains exclusive control over the way it works.

25 Richard Stallman, 'Who does that server really serve?', *Gnu.org*, 5 June 2018, https://www.gnu.org/philosophy/who-does-that-server-really-serve.en.html.

26 The semiconductor and telecommunications giant, Qualcomm, believes this scenario will arise due to the eventual ubiquity of affordable high-speed Internet and corporate server farms providing cloud-based experiences. As David Pierce put it, 'Someday soon, your phone could just be a screen, a battery, and a processor for the simple things – and the things you'd rather not send over the internet, like your fingerprint or passcode … When those screens need to do complicated things, whether it's gaming-level graphics or helpful voice assistants, you can call on the cloud.' David Pierce, 'Want to see the future? Look at the chips', *Wired*, 8 January 2018, https://www.wired.com/story/qualcomm-moves-beyond-mobile.

27 Apple uses this mechanism to force users to pass a 'signature check' when they turn on their iPhone. See John Sullivan, 'Why free software and Apple's iPhone don't mix', *Free Software Foundation*, 30 July 2008, https://www.fsf.org/blogs/community/why-free-software-and-apples-iphone-dont-mix; Molly de Blanc, 'Apple App Store anniversary marks ten years of proprietary appsploitation', *Free Software Foundation*, 31 July 2018, https://www.fsf.org/blogs/community/apple-app-store-anniversary-marks-ten-years-of-proprietary-appsploitation.

28 Tim Wu, 'Network neutrality, broadband discrimination', *Journal of Telecommunications and High Technology Law* 2, no. 1 (2003).

29 Simurgh Aryan, Homa Aryan and J. Alex Halderman, 'Internet censorship in Iran: a first look', *USENIX*, 13 August 2013, https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf.

30 DRM is needed to prevent people from recording live streams. (This was a source of controversy when the World Wide Web Consortium decided to endorse Encrypted Media Extensions in HTML5.)

31 See, *inter alia*, Eben Moglen, 'The dotCommunist Manifesto', January 2003, http://moglen.law.columbia.edu/publications/dcm.html; Alan Story, Colin Darch and Debora Halbert, 'The copy/South dossier: issues in the economics, politics, and ideology of copyright in the global South' (2006), https://www.gutenberg.org/files/22746/22746-p/22746-p.pdf; Dean Baker, 'Working paper: is intellectual property the root of all evil? Patents, copyrights, and inequality', October 2018, http://cepr.net/images/stories/reports/ip-2018-10.pdf.

32 See Mariana Mazzucato, *The Entrepreneurial State: debunking public vs. private sector myths* (New York: Public Affairs, 2015), pp. 93–116.

33 Amy Kapczynski, 'The cost of price: why and how to get beyond intellectual property internalism', *UCLA Law Review* 59 (2012), p. 972, https://pdfs.semanticscholar.org/2c88/2a926eac4885ac217126dab48b99899efcc6.pdf.

34 Without membership in the WTO, developing countries would not have a voice in the running of world trade, and would be subjected to bilateral pressures for liberalisation from developed countries. See Ha-Joon Chang, 'Only protection can build developing economies', *Le Monde diplomatique*, August 2003, https://www.globalpolicy.org/component/content/article/162/27898.html.

35 World Intellectual Property Organization (WIPO), 'Doc. WO/GA/31/11', (2004), http://www Proposal by Argentina and Brazil for the Establish a Development Agenda for WIPO.wipo.int/edocs/mdocs/govbody/en/wo_ga_31/wo_ga_31_11.pdf.

36 World Intellectual Property Organization (WIPO), 'The 45 Adopted Recommendations under the WIPO Development Agenda,' (2007), http://www.wipo.int/ip-development/en/agenda/recommendations.html.
37 World Intellectual Property Organization, 'Doc. WO/GA/31/11'.
38 Taylor Hatmaker, 'Facebook's Free Basics program ended quietly in Myanmar last year', *TechCrunch*, 1 May 2018, https://techcrunch.com/2018/05/01/facebook-free-basics-ending-myanmar-internet-org.
39 The numbers account for 1 million articles across thousands of websites. Twitter only adds 2.2 per cent. *Parse.ly*, 'The authority report', (2018), https://learn.parsely.com/rs/314-EBB-255/images/authority-report-15.pdf.
40 Daisuke Wakabayashi, 'As Google fights fake news, voices on the margins raise alarm', *The New York Times*, 26 September 2017, https://www.nytimes.com/2017/09/26/technology/google-search-bias-claims.html; Michael Nunez, 'Former Facebook workers: we routinely suppressed conservative news', *Gizmodo*, 9 April 2016, https://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006.
41 Jack Balkin, 'Free speech in the algorithmic society: big data, private governance, and new school speech regulation', *UC Davis Law Review* 51, no. 3 (2018), https://lawreview.law.ucdavis.edu/issues/51/3/Essays/51-3_Balkin.pdf; Peter Swire, 'Social networks, privacy, and freedom of association: data protection vs. data empowerment', *North Carolina Law Review* 90, no. 5 (2012).
42 Glenn Greenwald, 'Facebook says it is deleting accounts at the direction of the U.S. and Israeli governments', *The Intercept*, 30 December 2017, https://theintercept.com/2017/12/30/facebook-says-it-is-deleting-accounts-at-the-direction-of-the-u-s-and-israeli-governments. Thanks to my colleague Kamel Ajji for comments on freedom of association.
43 House of Lords Select Committee on Artificial Intelligence, 'AI in the UK: ready, willing and able?', 16 April 2018, https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.
44 Chinese tech corporations are so far primarily directed at their internal market. This is likely to change as companies like Tencent expand cloud and AI services beyond the domestic market, and it is worth monitoring the expansion of Chinese tech closely.
45 *National Security Agency*, 'NSA strategic partnerships: alliances with over 80 major global corporations supporting both missions', n.d., https://www.aclu.org/files/natsec/nsa/20140722/NSA%20Strategic%20Partnerships.pdf.
46 Alfred McCoy, *Policing America's Empire: the United States, the Philippines, and the rise of the surveillance state* (Madison, WI: The University of Wisconsin Press, 2009), p. 21.
47 The Witwatersrand Chamber of Mines, Johannesburg, S.A.R., 'Evidence and report of the Industrial Commission of Enquiry' (1897), p. 44; see also, Keith Breckenridge, *Biometric State: the global politics of identification and surveillance in South Africa, 1850 to the present* (New York: Cambridge University Press, 2014), pp. 67–68.
48 Michael Kwet, 'Apartheid in the shadows', *Counterpunch*, 3 May 2017, https://www.counterpunch.org/2017/05/03/apartheid-in-the-shadows-the-usa-ibm-and-south-africas-digital-police-state.
49 Henry F. Jackson, *From the Congo to Soweto: U.S. foreign policy toward Africa since 1960* (New York: William Morrow and Company, Inc., 1982), pp. 244–82.
50 Malcolm Ray, *Free Fall: why South African universities are in a race against time* (Johannesburg: Bookstorm [Pty] Ltd, 2016), pp. 129–76; Feliks Garcia, 'Former CIA agent admits involvement in Nelson Mandela's arrest', *The Independent*, 15 May 2016, https://www.independent.co.uk/news/world/africa/nelson-mandela-cia-arrest-south-africa-a7030751.html.
51 William Binney, 'The government is profiling you (the NSA is spying on you)', *YouTube*, 7 June 2013, https://www.youtube.com/watch?v=qB3KR8fWNh0.

52 'How GCHQ stepped up spying on South African foreign ministry', *The Guardian*, 16 June 2013, https://www.theguardian.com/world/2013/jun/16/gchq-south-african-foreign-ministry; RDM Newswire, 'British intelligence caught spying on South Africa's leftie lawyers', *TimesLIVE*, 22 June 2015, http://www.timeslive.co.za/local/2015/06/22/British-Intelligence-caught-spying-on-South-Africa's-leftie-lawyers.
53 Breckenridge, *Biometric State*.
54 Walter Rodney, *How Europe Underdeveloped Africa* (Washington, DC: Howard University Press, 1972/1981), p. 241.
55 For a criticism of the term's legitimacy, see Jeremy Rifkin, 'The 2016 World Economic Forum misfires with its fourth industrial revolution theme', *The Huffington Post*, 14 January 2016, https://www.huffingtonpost.com/jeremy-rifkin/the-2016-world-economic-f_b_8975326.html.
56 See Gnu.org, 'What is free software?'.
57 The term 'Free' in 'Free Software' denotes 'freedom', not price. The terminology can be confusing given that Free Software is often exchanged for free (meaning, you don't have to pay for it) given that everyone is free to send a copy to each other without charging money for it. Nonetheless, the term 'Free' in Free Software connotes 'Freedom', and what matters is not whether a user paid for the software, but what kind of freedom the software gives them once they have it. According to Stallman, the term 'Freedom Software' has been trademarked, so the FSM uses 'Free Software' instead.
58 Archbishop Desmond Tutu, 'Archbishop Desmond Tutu opens Digital Freedom Exposition', *YouTube*, 20 May 2007, https://www.youtube.com/watch?v=RdydCoiru4o.
59 We should also include free hardware design as part of Free Hardware. See Richard Stallman, 'Hardware designs should be free. Here's how to do it', *Wired*, 18 March 2015, https://www.wired.com/2015/03/richard-stallman-how-to-make-hardware-designs-free.
60 Moglen, '"Die gedanken sind frei"'. This assumes people have the resources to make use of the information. Language barriers, education, and other factors can present a barrier to accessibility, even if the information becomes freely available to communities. See Knowledge Commons Brasil, 'Digital colonialism & the internet as a tool of cultural hegemony', http://www.knowledgecommons.in/brasil/en/whats-wrong-with-current-internet-governance/digital-colonialism-the-internet-as-a-tool-of-cultural-hegemony.
61 Edward Snowden, 'The last lighthouse: free software in dark times', *IO/Terror*, 19 March 2016, http://ioterror.com/items/show/34.
62 Eben Moglen, 'Better than rage against the machine: saving privacy in one hell of a dangerous world', *I/O Terror*, 25 September 2017, http://ioterror.com/items/show/43.
63 For a study on the architectural problems of cell phone surveillance, see Stephen B. Wicker, *Cellular Convergence and the Death of Privacy* (New York: Oxford University Press, 2013).
64 Jack M. Balkin, 'Information fiduciaries and the First Amendment', *UC Davis Law Review* 49, no. 4 (2016), https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf; Jack M. Balkin and Jonathan Zittrain, 'A grand bargain to make tech companies trustworthy', *The Atlantic*, 3 October 2016, https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346.
65 Examples of People's Technologies include Debian GNU/Linux (a Free Software operating system), LibreOffice (an alternative to Microsoft Office), Gimp (an alternative to Adobe Photoshop), F-Droid (an Android app repository that offers Free Software apps audited to remove third-party advertising trackers), Tor (for Internet anonymity), Jitsi (an alternative to Skype), and chat apps like Signal and Wire.
66 Of course, new technologies cannot fix deep-seated issues such as climate change, poverty, segregation, militarism, capitalism, state power and various forms of domination (e.g. race, class and gender). The struggle to control technology takes place *alongside* these other issues, which often intersect in various ways.

67 Seda Gürses, Arun Kundnani and Joris Van Hoboken, 'Crypto and empire: the contradictions of counter-surveillance advocacy', *Media, Culture & Society* 38, no. 4 (2016).

68 'Critical algorithmic scholars' have formulated a partial but limited structural assessment of algorithmic discrimination, in that they link discrimination to the way algorithmic systems work. However, they do not dig deeper and address the core pillars of the tech ecosystem, which are then left to corporations to design for their own interests. It should be noted that this paper does not cover all aspects of digital colonialism. There are components and complexities that could not be covered in such a small space (e.g. open standards, blockchain, Internet governance, and labour exploitation producing hardware). Other issues should be explored, including South-South imperialism, especially in light of tech giants in China (e.g. Baidu, Alibaba, and Tencent). Environmental sustainability is another consideration for further inquiry. Circumstances will vary by place and time, and it will take many minds to grapple with this complex and understudied subject.