

South Africa | Freedom House

Overview

Internet freedom declined in South Africa during the coverage period, in part due to election-related factors. Self-censorship, online harassment, and online manipulation all increased in the run-up to the general elections in May 2019. Though concerns persist about South Africa's surveillance capabilities, there were no reported instances of blocking or filtering, nor restrictions on the use of social media for online mobilization.

Although South Africa has cultivated a reputation as a proponent of human rights and a leader on the African continent, in recent years, the ruling African National Congress (ANC) has been accused of undermining state institutions in order to protect corrupt officials and preserve its power as its support base began to wane.

Key Developments

June 1, 2018 – May 31, 2019

- In November 2018, the national telecommunications regulatory body, the Independent Communications Authority of South Africa (ICASA), launched an inquiry into the cost of data; there is hope that this process will contribute to a reduction in data costs ([see A2](#)).
- The Electronic Communications Amendment (ECA) Bill, which had been criticized for granting extensive regulatory powers to the Department of Telecommunications and Postal Services (DTPS) at the expense of ICASA's independence, was withdrawn in February 2019 ([see A5](#)).
- In March 2019, Parliament passed the Film and Publications Bill, which would empower the Film and Publications Board (FPB) to issue takedown orders for a wide range of content. The bill is meant to protect children from adult content and to prevent hate speech, but analysts have expressed concern that the vague wording of the legislation will make online content vulnerable to censorship. At the end of the reporting period, the bill awaited the president's signature ([see B3](#)).
- In November 2018, the National Assembly passed a substantially revised third version of the controversial Cybercrimes Bill (formerly known as the Cybercrimes and Cybersecurity Bill). The version of the bill that passed no longer contained provisions on cybersecurity, and dispensed with other provisions that had concerned rights activists ([see C2](#)).
- Encroachments on privacy rights remained a major concern during the coverage period, especially in regard to inadequacies in the legal framework surrounding surveillance and the interception of communications, lack of regulation of foreign signal interception, and the continued delay in making the Information Regulator fully operational. Additionally, a 2018 report by Citizen

Lab identified South Africa as one of 45 countries worldwide using Pegasus, a targeted spyware software developed by the Israeli technology firm NSO ([see C5](#)).

- Online attacks against journalists intensified during the run-up to the May 2019 general elections, which analysts believe contributed to increased self-censorship by the media ([see C7](#)).

A Obstacles to Access

Access to the internet continued to expand across the country and the government has taken some steps to address high costs, which remain a barrier to access. The ECA Bill, which has been criticized for granting extensive powers to the DTSP at the expense of the regulatory body's independence, was withdrawn in 2019.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	46
--	----

Internet penetration has expanded rapidly in South Africa. According to the latest data from the International Telecommunication Union (ITU), the internet penetration rate reached 56 percent in 2017. According to the 2018 General Household Survey conducted by Statistics South Africa, the national statistics agency, nearly 65 percent of South African households have at least one member who can access the internet at home, work, school, or internet cafés,¹ up from 53 percent in 2015.² The majority of internet users (60 percent) access the internet through their mobile devices.³

The government has prioritized access to free public Wi-Fi with the adoption of its broadband policy, the SA Connect program, in 2013.⁴ SA Connect aims to provide affordable, high-quality and high-speed broadband access to schools, clinics, police stations, and other government facilities, particularly in underserved communities. A 98.7 percent cut in the budget of the DTSP greatly limited the efficiency of the program in the 2018–2019 financial year.⁵ Mobile operators are obligated to contribute to SA Connect implementation as part of their license conditions. According to the May 2018 SA Connect progress report, mobile operators had connected 4,366 schools out of the 5,250 that were targeted for connectivity in a five-year period.⁶

Several other initiatives in metropolitan areas have enjoyed modest success in rolling out public Wi-Fi, including Cape Town, Durban, Johannesburg, Tswane,⁷ and the Ekurhuleni municipality.⁸ Similar projects are also being rolled out in other provinces and towns across the country.⁹

The fiber market in South Africa has grown at an exponential rate. Most suburban areas of the major urban centers (including Pretoria, Cape Town, Johannesburg, Durban, and Port Elizabeth) are already covered with fiber-optic cables, and new “last mile” providers of fiber have begun to wire homes by connecting to competitive internet backbones run by larger operators. At least 12 companies provide fiber network infrastructure,¹⁰ with partially state-owned Telkom providing 157,400 kilometers of fiber, the largest share as of 2018, which connects over 2.5 million

premises; other companies provide a considerably smaller share of fiber.[11](#)

The average mobile internet connection speed is 25.47 Mbps, while the average speed for a fixed line connection is 18.31 Mbps. [12](#) South Africa has an average download speed of 6.38 Mbps, which is 76th out of 200 countries assessed by Cable, a UK-based telecommunications company.[13](#)

The availability of the internet has been significantly limited by power cuts introduced by the national power company, Eskom, in 2019, to stave off years of mismanagement. For five consecutive days in February 2019,[14](#) and another 10 days in March 2019,[15](#) Eskom conducted load-shedding due to reduced power-generating capacity resulting from technical faults caused by lack of maintenance at power stations, as well as operational, structural, and financial problems.[16](#) Infrastructure damage that occurred during Cyclone Idai in 2019 was also a contributing factor. [17](#)

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	13
---	----

High costs remain a primary obstacle to access. Recent market trends show that users are spending a greater proportion of income, at the individual and household level, on data, and less on voice or SMS services.[18](#)

Prepaid mobile data remains unaffordable for most,[19](#) at a cost of 2.5 percent of the average monthly income in South Africa.[20](#) The high cost contributes to the relatively low rates of internet use.[21](#) In 2017, South Africa ranked 35th out of 49 African countries in affordability for prepaid mobile data bundles, with an average cost of \$8.28. Though mobile operators are gradually providing more low-cost data packages to lower-income customers,[22](#) the vast majority of South Africans without internet access are those earning less than 7,200 South African rands (\$500) per month (representing 42 percent of the population). Those without internet access have pinpointed the high costs as the main reason for their lack of connectivity.[23](#)

The information and communications technology (ICT) regulatory body, ICASA, has taken steps to address the high cost of data in two ways. First, the introduction of the End-User and Subscriber Service Charter Regulation Amendment of 2018, which came into force in February 2019, requires service providers to give users the option to roll over their data bundles from month to month for a maximum period of three years; to transfer their data to another user within the same network; and to provide opt-in and opt-out choices for out-of-bundle data charges, which are considerably more expensive, upon exhaustion of their data.[24](#)

In November 2018, ICASA also commenced a market inquiry into mobile broadband services, as part of an initiative to reduce the cost of communication by promoting competition in the ICT sector through possible regulation of the mobile broadband market.[25](#) The inquiry is expected to be completed by early 2020 and could potentially lead to a reduction in data costs.[26](#)

Zero-rated offerings by mobile operators essentially offer free internet access to a few OTT services such as free basics on Facebook, Twitter, and educational services including D6 Communicator for schools and Vodacom e-school learning apps.[27](#) A few other services are partially zero-rated in that users receive them as part of a paid

package. However, zero-rated services are often used by South Africans who are already connected to reduce their costs of access, and not necessarily their exclusive means of accessing the internet.²⁸

Though the country has achieved nearly 100 percent 3G network coverage, there are disparities in internet access between urban and rural dwellers.²⁹ Internet penetration is significantly higher in urban areas. According to data published by Research ICT Africa in July 2018, a majority of urban dwellers (61 percent) have access to the internet, compared to a minority of rural dwellers (40 percent).³⁰ In terms of the gender gap, Research ICT Africa reported that 12 percent more men have access to the internet than women.³¹ Access to the internet among youths is relatively high, at 70 percent, compared to the 53 percent of the entire population.³² The higher rates of youth connectivity is no doubt influenced by the high level of access to smartphones by young people; 71 percent of youths have smartphones, compared to 55 percent of the general population.

Importantly, SIM card registration requirements (see C4), which include proof of residence, present an obstacle to mobile phone usage for many South Africans who live in informal settlements.

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	66
--	----

There is no evidence that the government exercises control over internet infrastructure for censorship or to restrict connectivity.

The government does not have direct control over the country's internet backbone or its connection to the international internet, and there have been no intentional disruptions to connectivity. International internet connectivity is facilitated via five undersea cables—SAT-3, SAFE, WACS, EASSy, and SEACOM—all of which are owned and operated by a consortium of private companies.³³ Several operators oversee South Africa's national fiber networks, including partly state-owned Telkom and privately owned MTN, Vodacom, Cell-C, Neotel-Liquid, and Broadband Infraco, among others. Internet traffic between different networks is exchanged at internet exchange points (IXPs) located in Johannesburg, Cape Town, and Durban, which are operated by South Africa's nonprofit Internet Service Providers' Association (ISPA) and NapAfrica.³⁴ The three internet exchange points are hosted in vendor-neutral data centers owned by the South African firm Teraco.³⁵

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	46
--	----

South Africa has a competitive ISP market. The ISPA currently has 186 members in South Africa, which are mostly private enterprises.³⁶ However, the fixed-line connectivity market is dominated by Telkom, of which the government has a 40 percent share, as well as an additional 12 percent share through the state-owned Public Investment Corporation.³⁷ Telkom effectively possesses a monopoly, despite the introduction of a second national operator, Neotel, in 2006.³⁸ There are four

major mobile carriers—Vodacom, MTN, Cell-C, and Telkom Mobile—all of which are privately owned, with the exception of Telkom Mobile.

The licensing processes for fixed and mobile phones, as well as internet services, are overseen by ICASA, and are clear and easily accessible on ICASA's website.³⁹ The licensing fees imposed by ICASA are reasonable and do not impose an undue barrier to the diversity of service providers.

While no informal connections between licensees or prospective licensees and government officials is required for service providers, ICASA is seen by some as a “fractured and weak” institution, which affects its capacity to execute its mandate, including licensing.⁴⁰

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	24
--	----

The autonomy of the regulatory body, ICASA, is protected by the constitution. A transparent and participatory appointment process involving parliamentary oversight is guaranteed by the law that established ICASA.⁴¹ There is, however, a perception that in practice, political interference is a problem in the agency, and that membership of the ICASA board is open only to supporters of the ruling party.⁴²

ICASA's independence has also been compromised due to encroachments on its mandate by a number of government entities. In addition to ICASA, the DTPS, the .za Domain Name Authority (.ZADNA), and the Universal Service and Access Agency of South Africa (USAASA) have regulatory power over ICTs. The proliferation of regulatory bodies has led to redundancy and poor coordination, and contributes to the perception that the country lacks a comprehensive approach to the regulation of ICTs.

In 2016, the cabinet approved the National Integrated ICT Policy White Paper,⁴³ which outlines the overarching policy framework aimed at transforming South Africa into an inclusive and innovative digital and knowledge society.⁴⁴ One of the bills proposed in the white paper is the ICT Sector Commission and Tribunal Bill. The bill would consolidate regulation of the ICT sector through the introduction of an ICT sector commission and tribunal, but the legislation has not yet been passed.⁴⁵ Another key bill emanating from the white paper that would have significantly impacted supply-side aspects of the ICT sector is the ECA Bill, which was published in 2017 for public comment. The bill was withdrawn by the minister of telecommunications and postal services in February 2019, citing the need for “further consultations.”⁴⁶ The bill had been widely criticized for granting extensive powers to the DTPS, by giving it a greater role in oversight of the sector, raising concerns that this would erode the independence of ICASA.⁴⁷ The ECA Bill was also intended to facilitate the implementation of a wholesale open access network (WOAN) as a model for spectrum allocation.⁴⁸ This aspect of the legislation also drew further criticism for undermining the role of ICASA in the allocation and management of spectrum.⁴⁹

Another key actor in the regulation of ICTs is the FPB, which traditionally regulates the distribution of films, games, and other publications. However, recent amendments to the Film and Publications Act, 1996, which were passed by Parliament in February 2019 and awaited the president's signature at the end of the

reporting period, would extend the authority of the FPB to regulate such content on the internet ([see B3](#)).⁵⁰ In 2016, the FPB signed a memorandum of understanding with ICASA to address regulatory overlaps created by the proposed amendments, which will effectively create cojurisdiction over online content.⁵¹ These proposals further complicate the regulation of online content. However, it remains unclear how the two bodies will implement the agreement.

Access providers and other internet-related groups are active in lobbying for a better legislative and policy environment for the sector. In 2009, the ISPA was recognized as a self-regulatory body by the Department of Communications, and exercises authority over its members through transparent processes ([see B3](#)).⁵²

B Limits on Content

The recently enacted Films and Publications Amendment Act, which aims to protect children from racist, harmful, and violent content online, will give the FBP sweeping powers to censor internet content, if signed into law by the President. This is despite some positive changes made to the Bill by Parliament before its adoption in March 2019. Online self-censorship was more prevalent and online manipulation through social media disinformation campaigns was documented ahead of the May 2019 elections.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	66
---	----

Neither the state nor other actors block or filter internet and other ICT content, and there is no evidence of blocking or content filtering on mobile phones.

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	34
--	----

State and nonstate actors do not frequently force publishers, content hosts, or digital platforms to delete legitimate content. Decisions on takedowns for online content are made not by the state but by the self-regulatory body, the ISPA.⁵³ In 2017, a controversial case of content removal made headlines when the news website Black Opinion was taken down by its web host after the ISPA received a complaint that the site was inciting racial hatred.⁵⁴ Linked to a land-rights lobby group called Black First Land First, the news site had published articles criticizing “white monopoly capital.”⁵⁵ The website was restored two weeks after it was taken down.⁵⁶

ECTA requires ISPs to respond to takedown notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the ISPA—the industry’s representative body—are not held liable for third-party content that they do not create or select, though they can lose their protection from liability if they do not respond to takedown requests.⁵⁷

According to Google, between January and June 2018, a single request was received from the South African government, backed by a court order, for the removal of

content on Google+, which was reportedly related to online harassment.[58](#) Google agreed to remove the content.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	34
---	----

Restrictions on the internet are generally transparent and proportional, with a few exceptions. The ISPA takes a self-regulatory approach to restricting access to unlawful internet and digital content hosted by its members. This process is in accordance with the takedown procedures provided in the Electronic Communications and Transaction Act (ECTA) of 2002,[59](#) and is guided by the ISPA's complaints procedures.[60](#) ISPs often err on the side of caution by taking down content upon receipt of a notice to avoid litigation (see [B2](#)), and there is no incentive for providers to defend the rights of the original content creator if they believe the takedown notice was requested in bad faith.

Though no specific reference is made to a proportionality test as a consideration in restricting access, the ISPA code of conduct requires members to respect freedoms of speech and expression as guaranteed by the constitution, and to act lawfully and cooperate with law enforcement agencies.[61](#) There is an internal appeals process available to those who may be aggrieved by the ISPA's actions, as well as an avenue for appeal in the courts.[62](#)

The ISPA reports annually on activities related to restrictions on content. Takedown notifications (TDNs) lodged with the ISPA increased from 464 in 2017 to 608 in 2018; of those, 233 were accepted (up from 210 in 2017), 366 rejected, and 9 withdrawn. Of the notices accepted, 216 requests resulted in content being removed. The main reasons for removals included copyright or trademark infringements, fraud, malware or phishing, defamation, hate speech, harassment, and invasion of privacy.[63](#)

If signed into law, the Films and Publications Amendment Act will empower the FPB to issue take down orders for content adjudged to be prohibited. The amendment has been criticized by ISPA for amongst other things, exceeding the mandate of the FPB as well as opening online content to State censorship given the quasi-government nature of the FPB and its limited capacity compared to courts in adjudicating justifiable limitations to freedom of expression.[64](#) As of the end of the coverage period, the amendment had been passed by the legislature and was waiting for signature by the president.[65](#)

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	34
---	----

Although the government does not limit or manipulate online discussions, online self-censorship is a growing concern in South Africa. During the reporting period, particularly in the run-up to the 2019 national and provincial elections, the severity of online attacks against journalists increased sharply, leading to greater self-censorship online (see [C7](#)). In particular, the leader of the Economic Freedom Fighters (EFF)

political party, Julius Malema, has on several occasions attacked and encouraged attacks against journalists online.

Analysts contend that these attacks form part of a well-orchestrated cyberbullying strategy to deter other journalists and commentators from reports or utterances critical of the EFF. [66](#)

Despite the perception that online self-censorship by journalists has increased, ordinary citizens and journalists, including those who have been subjected to online abuse, continue to report on politically sensitive issues. [67](#)

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	24
--	----

Manipulation of the online space by political actors through bogus social media profiles, targeted commenting on social media posts, and bots, is a growing problem in South Africa. [68](#) A study conducted on political disinformation on Twitter in South Africa between 2014 and 2018 revealed that main political and interest groups, including ANC- and EFF-related accounts, were most active in manipulating the platform, likely using bots and trolls. [69](#) In the run-up to the 2019 elections, the online space was weaponized not only by the EFF, but also by other major political parties and their supporters to discredit critics and spread disinformation. [70](#)

News reports in 2017 revealed the execution of a coordinated online campaign by supporters of the powerful Gupta family to influence and confuse public opinion through the proliferation of disinformation. Hundreds of automated bots on Twitter harassed journalists who reported critically about the Gupta family and their ties to former president Zuma. [71](#) The campaign, which produced 220,000 tweets and hundreds of Facebook posts, also targeted political figures including then-finance minister Pravin Gordhan and then-deputy president Cyril Ramaphosa, with the purpose of discrediting them. [72](#)

The government and the ruling ANC has not attempted to overtly influence the editorial lines of media outlets. However, in March 2019, the ANC's head of elections, Fikile Mbalula, reportedly attempted to coerce the South African Broadcasting Corporation (SABC), the public broadcaster, to increase its coverage of the ANC's election campaigns; Mbalula accused the SABC of a "clampdown" and "blackout" of the party's campaign activities. [73](#)

The government has at times attempted to control media content, particularly on the former Gupta-owned 24-hour news channel ANN7 and the New Age newspaper, [74](#) both of which served as the mouthpiece of the ANC government. [75](#) The 2013 purchase of the Independent Group, a large media conglomerate, by ANC ally Iqbal Survé, and persistent interference with the SABC, have taken a toll on fair and balanced media content in South Africa. [76](#)

The ongoing state capture inquiry, which examines the influence of the Gupta family and other powerful interests on the government, revealed in January 2019 that several journalists received monthly bribes from the contracting firm Bosasa (now known as African Global Operations) to inform the company of potential negative

stories about it, as well as to write articles that presented Bosasa in a flattering light.⁷⁷

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	23
---	----

For the most part, there are not economic and regulatory constraints that significantly affect users' ability to publish content online. The online environment in South Africa is net neutral, although net neutrality has not been expressly provided for in law or policy.⁷⁸ The ISPA is at the forefront in promoting net neutrality, and believes that it is essential for the transparent management of networks and preventing anticompetitive behavior.⁷⁹ The government has indicated that it intends to include net neutrality in an expected amendment to the ECTA.⁸⁰

The role of politicized advertising may affect economic viability. In the past, Gupta-owned pro-government ANN7 new channel and the New Age newspaper (see B5) routinely received a massive share of government advertising, reaching in the hundreds of millions of rands.⁸¹

In 2017, the FPB proposed revisions to the tariff structure that would require online streaming services to pay a licensing fee per film and per series season that they offer, as opposed to the current structure, which involves payment of a flat fee.⁸² The size of the fee was criticized by industry stakeholders as unjustifiable (in relation to the actual cost of classification) and prohibitive for smaller competitors providing content streaming services.⁸³ If adopted, these revisions would benefit content distributors with fewer titles, while those with more content would pay significantly more than the current license fee of 795,000 South African rands (\$55,000), which was imposed in 2016.⁸⁴ Although some major content distributors such as Google, Apple, and MultiChoice had paid the license fees by the end of 2017, other major players such as Netflix and Microsoft refused to pay. Netflix continues to lobby the FPB for continued self-regulation of content on their platforms.⁸⁵ The revisions to the structure had not yet passed by the end of the reporting period.

B7 0-4 pts

Does the online information landscape lack diversity?	34
---	----

Online media in South Africa is vibrant, representing a wide range of international and national viewpoints and perspectives.

Web-only news platforms, such as the Daily Maverick and News24, have become particularly popular in recent years, with key news stories often broken online before print or broadcast outlets, illustrating how online media is growing as a primary news source.

While content in both English and Afrikaans is well-represented online, 9 of South Africa's 11 official languages are underrepresented on the internet, including on government websites. Additionally, the perspectives of women, rural dwellers, persons with disabilities, sexual minorities, and ethnic and religious minorities are underrepresented and marginalized in the media, including online media.⁸⁶

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	66
---	----

Neither the government nor nonstate actors restrict the use of digital tools for mobilization and campaigning. South Africa has a robust online community that addresses contemporary social, economic, and political issues. In 2018, successful social media campaigns addressed issues such as the blood donation drive by the South African National Blood Services (SANBS), the changing nature of traditional family structures, and gender stereotyping.⁸⁷

Local sources report that pressure by online advocacy groups has had an impact on ICASA, which introduced the End-User and Subscriber Service Charter Regulation Amendment in 28 February 2019, and also commenced a market inquiry into mobile broadband services that could result in lower data costs (see A2).

In 2016, civil society groups advocated to bring down the high cost of digital communications, using the hashtag #DataMustFall.⁸⁸ The government responded positively to the campaign, and in 2017, a competition commission launched an inquiry with the aim of understanding critical elements within the market and value chain that lead to high prices for data services, and ultimately to make recommendations that could lower the cost of data.⁸⁹ The commission is expected to conclude its inquiry by the end of 2019.⁹⁰

C Violations of User Rights

Facing resistance from rights activists, the controversial draft Cybercrimes and Cybersecurity Bill was altered and became the Cybercrimes Bill, which now conforms to international human rights standards. Persistent concerns remain about the extent of the government's surveillance capabilities. Online harassment increased in the run-up to the 2019 elections.

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	56
--	----

The constitution provides for freedom of the press and freedom of expression, among other guarantees. It also includes constraints on “propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm.”⁹¹ The right of access to information held by the state, and in limited circumstances by private bodies, is also guaranteed by the constitution.⁹² These rights apply to all journalists equally, whether operating online or offline. However, observers have expressed concern that, if signed into law, the Films and Publications Amendment Act, will make online content vulnerable to censorship (see B3).

In a positive development for internet freedom, in July 2018 South Africa voted in favor of the UN Human Rights Council (UNHRC) resolution on “the promotion, protection, and enjoyment of human rights on the internet.”⁹³ South Africa had

previously voted against a 2016 version of the resolution, siding with repressive countries such as China, Russia, and Saudi Arabia.[94](#)

The judiciary is generally regarded as independent and in recent years has been seen as the branch of government that has been most dedicated to upholding the rule of law by constraining the executive and legislative branches from arbitrary actions.[95](#)

However, the police and other law enforcement agencies have been criticized for failing to adequately investigate and prosecute EFF supporters who have threatened and attacked journalists, contributing to an environment of impunity and threatening the rights guaranteed in the constitution. Notably, Floyd Shivambu, deputy president of the EFF, was filmed assaulting a photojournalist in March 2018, and has not faced criminal charges.[96](#)

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	24
---	----

A number of laws are vulnerable to being misused to prosecute online journalists and activists. Libel is not a criminal offense, though civil laws can be applied to online content. The offense of *crimen injuria*, or insulting the dignity of a person, has been invoked to prosecute online harassment.[97](#)

Defamation is a criminal offense, though prosecutions are rare and until recently, defamation charges were not brought against people for online activity.

A draft Cybercrimes and Cybersecurity Bill, first introduced in 2015, was criticized by civil society activists for its ambiguous language, which they claim has the potential to infringe on freedom of expression.[98](#) In the second version of the bill introduced in 2017, a chapter on “malicious communications” would penalize the dissemination of a “data message which is harmful,” the definition of which includes content that is “inherently false,” without further specifications.[99](#) The bill also contained a number of provisions that were vaguely worded, leading to concerns that it could be used to censor political speech online,[100](#) while other aspects of the bill would enhance the state’s surveillance powers (see C5).

In October 2018, a substantially revised third version of the bill was presented by the Department of Justice and Constitutional Development. The legislation, renamed the Cybercrimes Bill, no longer contained language on cybersecurity.[101](#) The amendment also addressed the ambiguous definition of “unlawful,” bringing it in line with the Protection of Personal Information Act (POPIA) of 2013, and dispensed with crimes related to “critical infrastructure.”[102](#) This version was passed by the National Assembly in November 2018, and awaited passage by the National Council of Provinces at the end of the coverage period.[103](#)

C3 0-6 pts

Are individuals penalized for online activities?	66
--	----

No individual was prosecuted, detained, or sanctioned by the state for protected political, social, or religious speech online during the coverage period. In May 2019, the High Court in Gauteng found the EFF guilty of defamation in relation for a

statement it circulated on Twitter accusing former finance minister Trevor Manuel of nepotism and corruption.[104](#) The court ordered the EFF to issue an apology and remove the offending statement within 24 hours, pay approximately \$35,000 in damages, and to refrain from making similar statements in the future.

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	34
--	----

South Africa has few restrictions on anonymous communication or encryption. There are no laws requiring internet users, website owners, or bloggers in South Africa to register with the government or any of its agencies to operate. Users are also not required to use their real names when posting comments on the internet, including on social media platforms.

The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) of 2002, however, compromises users' rights to anonymous communication by requiring mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of physical address to service providers.[105](#) An identification number is legally required for any SIM card purchase, and registration requires proof of residence and an identity document.[106](#) Beyond privacy concerns, the RICA requirements can be an obstacle to mobile phone usage for the many South Africans who live in informal settlements with no recognized address.

Users are not explicitly prohibited from using encryption to safeguard their communications. However, RICA empowers a judge to force the disclosure of decryption keys or to require assistance in decryption in specified circumstances, upon approval of a request made by the police, military, intelligence, or other law enforcement agencies.[107](#)

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	26
---	----

Strong concerns about potentially unchecked government surveillance powers over online activity remain, but some legal safeguards related to surveillance do exist. RICA does not permit the blanket collection of metadata (communications-related information), but provides for a stringent process for the targeted collection of metadata, the interception of communications, and the decryption of private communications, all of which require a court order.[108](#)

However, the threshold for granting a court order is low, oversight is insufficient, and users do not have to be informed that their communications have been intercepted.[109](#) A loophole in RICA allows communications to be intercepted under the Criminal Procedure Act, which lacks RICA's safeguards and has been abused by law enforcement agencies.[110](#) Up to 95 percent of court orders involving the interception of communications are not approved by a RICA judge; most of the court orders outside of RICA are for metadata. The metadata of between 70,000 and 195,000 mobile users is collected every year.[111](#) Telecommunications service

providers are also required to store the metadata of all customers for three to five years, a provision that concerns privacy advocates.[112](#)

In a 2018 report by Citizen Lab, a Canadian internet watchdog, South Africa is listed as one of 45 countries worldwide using Pegasus, a targeted spyware software developed by the Israeli technology firm NSO. Pegasus is known to be used by governments to spy on journalists, human rights defenders, and the opposition.[113](#)

South Africa has the technical capacity to undertake bulk and targeted surveillance and research has acknowledged that bulk surveillance is being undertaken by various government agencies.[114](#) This is particularly concerning because RICA's oversight applies only to domestic signal interception and not to the interception of foreign signals, which include communications such as emails. Foreign signals are communications that originate from outside of South Africa but pass through or terminate in the country.[115](#) The National Communication Centre (NCC) is responsible for intercepting foreign signals and does so without oversight.

The South African police possess the international mobile subscriber identity (IMSI) technology, also known as "stingray," for bulk interception, although the extent of its use is uncertain.[116](#) The Ministry of State Security does not believe that the IMSI is governed by RICA, and its use is therefore unregulated.[117](#) The government has claimed that the technology is only used for national security matters.[118](#) Nonetheless, consistent weaknesses in oversight mechanisms within the state security departments leave surveillance open to abuse. The interception of communications that originate outside of South Africa are also essentially unregulated.[119](#) According to additional reporting from Privacy International, published in August 2019, South African security agencies claim that while bulk surveillance is meant to focus on foreign communications, their surveillance system is unable to discern between international and domestic communications and therefore collects both.[120](#) South Africa's intelligence services are also reported to be using a social media analytics and monitoring tool called Media Sonar, which allows for the searching and analyzing of social media content of users within a defined geolocation and using keyword searches.[121](#)

Concerns over the potentially unchecked government surveillance powers over online activity remain, but were somewhat addressed when Dr. Setlhomamaru Isaac Dintwe was appointed as the new inspector general of intelligence (IGI) in 2017. The position had previously been vacant for an extended period due to challenges in the recruitment process.[122](#) As an independent actor accountable to Parliament through the Joint Standing Committee on Intelligence,[123](#) the IGI was expected to strengthen oversight mechanisms for intelligence agencies and determine their compliance with the legislative framework and constitution.[124](#) However, upon assuming office, Dintwe had difficulty fulfilling his mandate due to interference by leadership in the intelligence community. In April 2018, Dintwe filed an urgent court application to prohibit Arthur Fraser, the director general of the State Security Agency (SSA), from intervening in the execution of his mandate.[125](#) Fraser was subsequently transferred out of the SSA, alleviating the crisis.[126](#)

Beyond RICA, South Africa has a legal framework protecting the constitutional right to privacy, which has not yet become fully operational. POPIA includes provisions to protect users' online security, privacy, and data, and allows an individual to bring civil claims against those who contravene the law.[127](#) Penalties for contravening the law are stiff, including prison terms and fines of up to 10 million South African rands (\$650,000).

While a few elements of POPIA came into force by presidential proclamation in 2014, the Information Regulator remains unable to enforce its provisions and settle complaints, because much of the law will only become operational after a necessary staff complement is in place and a proclamation of POPIA's coming into force is made by the president.¹²⁸ Once the proclamation is made, it will take at least another 12 months for the law to be fully implemented. In December 2018, the Information Regulator issued its final regulations, which provide for the processes to be adhered to in the processing of personal information in accordance with POPIA.¹²⁹

Journalists have been frequently targeted for surveillance by the state, usually as a means of identifying confidential sources.¹³⁰ For example, in May 2018, it emerged that the telephone conversations of investigative journalist Jacques Pauw had been intercepted while he was reporting on state capture during the Zuma administration.¹³¹ Nonstate actors have also targeted journalists for surveillance purposes. In March 2018, the Mail & Guardian disclosed that journalist Athandiwe Saba's telephone records were obtained by a private investigator hired by the Railway Safety Regulator, likely with the assistance of the police or National Prosecuting Authority. Saba had reported critically on the regulator.¹³²

In light of the concerns about RICA's implementation and the overall system of surveillance of private communications in South Africa, a case was filed by the Amabhungane Centre for Investigative Journalism in April 2017, challenging the constitutionality of RICA. In September 2019, after the report coverage period ended, the court ruled against the constitutionality of some provisions of RICA.¹³³

In February 2019, a private company, Vumacam, commenced the installation of 15,000 CCTV cameras in a number of Johannesburg suburbs.¹³⁴ The installation of the cameras followed an agreement between Vumacam and the city of Johannesburg, which was part of an effort to address rising crime. Vumacam monetizes its network of CCTV cameras through the purchase of its footage by security companies operating in neighborhoods within its coverage area. Analysts have expressed concern that Vumacam's CCTV network is potentially a tool for unchecked mass surveillance.¹³⁵ Additionally, there is no evidence that a privacy impact assessment was conducted by the city of Johannesburg or Vumacam.¹³⁶ Concerns have also been raised that Vumacam is not registered with the Private Security Industry Regulatory Authority.¹³⁷

Provisions in the Cybercrimes and Cyber Security Bill that could have enhanced the state's interception powers were removed in October 2018 (see C2).

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	36
--	----

RICA provides for a legal process for the interception of communications, and service providers are, under certain circumstances, required to aid the government in surveillance.

According to RICA, service providers, including ISPs, are required to use systems with the technical capacity for communications to be intercepted, and are also required to retain customer metadata for three to five years.¹³⁸ RICA specifically requires service providers to intercept and provide the communications of their

customers upon a directive by a judge.¹³⁹ In practice, however, the bulk of requests for information are not made through RICA, and are thus not transparent or subject to appeal (see C5). However, neither RICA nor POPIA impose data localization requirements.

While the ECTA does not require ISPs to actively monitor content or to seek information on unlawful activity, the minister of communications may, under certain circumstances, require ISPs to provide information on illegal activities of their users or information that facilitates the identification of users.¹⁴⁰

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	45
---	----

There were some cases of extralegal intimidation or violence reported against bloggers, journalists, and online users during the coverage period.

Members of the EFF, including leader Julius Malema, have attacked and encouraged attacks against journalists online on several occasions. In March 2019, for example, veteran journalist Karima Brown mistakenly posted a message directed to her staff on a WhatsApp Group that included EFF members. In response, Malema posted a screenshot of the message, which contained her mobile number, on Twitter. Brown then received a barrage of abusive and threatening messages from EFF supporters.¹⁴¹ Several other journalists, including Adriaan Basson of News24¹⁴² and Pauli van Wyk of the Daily Maverick, have also faced online attacks by Malema.

Although the EFF has threatened online journalists more prominently and with apparently more frequency than other political actors, supporters of the ANC have also been known to threaten and harass online critics. In September 2018, a prominent ANC member allegedly sent *Sunday Times* journalist Qaanitah Hunter an image of a gun in a text message, in response to an article she wrote about former president Zuma.¹⁴³

The South African National Editors' Forum has taken the EFF to court over allegedly enabling the intimidation and harassment of journalists. The case began in court after the coverage period ended, in August 2019.¹⁴⁴

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	23
---	----

South Africa is highly vulnerable to cybersecurity threats on many fronts, though independent news outlets and opposition voices were not subject to targeted technical attacks during the coverage period.

In the largest financial sector data breach in South African history, Liberty announced that its website had been hacked in June 2018, exposing the email addresses of its customers. The hacker had demanded a ransom, which Liberty decided not to pay.¹⁴⁵ In May 2018, the website ViewFines, which provides information on traffic fines, was hacked, exposing the personal information of almost

a million users, such as their identification numbers, mobile phone numbers, and full names.¹⁴⁶

Government websites are often hacked. Most of the hacks are perpetrated by amateur hackers with no apparent political motivations other than to advertise their skills. The government website of the National Cybersecurity Hub, whose objective is to protect South African citizens and businesses online, was hacked in August 2018.¹⁴⁷ These attacks are usually short-lived, with the websites restored within a few days.¹⁴⁸

The ECTA contains provisions that protect against cyberattack by criminalizing: access or interception of an individual's data without permission; interference with an individual's data without permission; unlawful production, sale, procurement, design, distribution, or possession of a device used to overcome security measures or the protection of data; the use of such a device to unlawfully overcome security measures for the protection of data; and interference with an information system that protects data.¹⁴⁹