

South Africa

	2016	2017		
Internet Freedom Status	Free	Free	Population:	55.9 million
Obstacles to Access (0-25)	8	8	Internet Penetration 2016 (ITU):	54 percent
Limits on Content (0-35)	6	6	Social Media/ICT Apps Blocked:	No
Violations of User Rights (0-40)	11	11	Political/Social Content Blocked:	No
TOTAL* (0-100)	25	25	Bloggers/ICT Users Arrested:	No
			Press Freedom 2017 Status:	Partly Free

* 0=most free, 100=least free

Key Developments: June 2016 – May 2017

- The telecommunications ministry interdicted the auction of spectrum to expand telecommunications networks, instead putting forward a publicly-owned model of spectrum allocation in a move that was widely criticized as an impediment to competition and investment (see **Regulatory Bodies**).
- South Africa voted against the UN Resolution for “the Promotion, Protection and Enjoyment of Human Rights on the Internet” in July 2016, joining China, Russia, and Saudi Arabia as dissenters (see **Introduction** and **Legal Environment**).
- The Film and Publications Amendment Bill introduced in 2015 may impose intermediary liability and a censorship regime on South Africa’s online content but was stalled in deliberation due to potential overlap with a new Cybercrimes and Cybersecurity Bill (see **Content Removal** and **Legal Environment**).
- The appointment of an Inspector-General of Intelligence in March 2017 is expected to strengthen oversight mechanisms for state intelligence and surveillance activities (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom in South Africa remains free and open, with access to the internet available to over half the country's population. Increased access is a core concern for government, civil society, and the private sector, which has led to collaborative efforts between public and private players to expand the information and communication technology (ICT) sector.

While the South African government has not proactively restricted access to ICTs or online content, officials have increasingly expressed apprehension over potential threats posed by ICT advancement, which was reflected in the country's July 2016 vote against the UN Resolution aimed at "the Promotion, Protection and Enjoyment of Human Rights on the Internet." The vote led civil society to worry that South Africa may seek to follow the example of internet governance set by other countries that voted against the resolution, including China, Russia, and Saudi Arabia, all of which have a record of repression against internet rights.

Two legislative proposals have the potential to restrain South Africa's internet freedom. The Film and Publications Amendment Bill—drafted for the purpose of protecting children from racist, harmful, and violent content online—has been widely criticized for giving the government sweeping powers to censor content through an onerous classification system. The Cybercrimes and Cyber Security Bill has been criticized for its ambiguous language that threatens to infringe on freedom of expression and privacy rights. Both bills were still under review as of October 2017.

In a positive step, an Inspector-General of Intelligence appointed in March 2017 is expected to strengthen oversight mechanisms for state intelligence and surveillance activities. A new Information Regulator was also appointed in October 2016 and is expected to give effect to the constitutional right to privacy by introducing measures that ensure personal information is processed legally by responsible parties.

Obstacles to Access

Access to quality and relatively affordable internet in South Africa is growing, primarily among low income communities through government subsidized Wi-Fi projects across the country. The telecommunications ministry interdicted the auction of spectrum to expand telecommunications networks, instead putting forward a publicly-owned model of spectrum allocation in a move that was widely criticized as an impediment to competition and investment.

Availability and Ease of Access

Internet penetration has expanded rapidly in South Africa, though many believe that the expansion has not kept up with the country's socioeconomic development. According to the latest data from the International Telecommunication Union (ITU), internet penetration reached 54 percent of the South African population in 2016, up from 52 percent in 2015. Similar access rates have been reported by the state's statistics agency in the 2015 General Household Survey, which noted that over 53 percent of South African households have at least one member who can access the internet

at home, work, school, or internet cafes.¹ However, this figure is significantly biased towards urban areas with more than half of households in metropolitans such as Gauteng (66 percent) and Western Cape (63 percent) having access to the internet.² In contrast, only 39 percent of households in Limpopo, a predominantly rural province, have access to the internet.³

Key Access Indicators		
Internet penetration (ITU) ^a	2016	54.0%
	2015	51.9%
	2011	34.0%
Mobile penetration (ITU) ^b	2016	142%
	2015	159%
	2011	123%
Average connection speeds (Akamai) ^c	2017(Q1)	6.7 Mbps
	2016(Q1)	6.5 Mbps

^a International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2016," <http://bit.ly/1cblxxY>.

^b International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2016," <http://bit.ly/1cblxxY>.

^c Akamai, "State of the Internet - Connectivity Report, Q1 2017," <https://goo.gl/TQH7L7>.

Another survey found that internet users were disproportionately white (50 percent), and speak either English (65.5 percent) or Afrikaans (39 percent).⁴

Mobile phone penetration is much more extensive, reaching 142 percent in 2016,⁵ with over 57 percent of internet users accessing the internet on their mobile devices.⁶ Meanwhile, the country's average internet connection speed has improved from 6.5 Mbps in 2016 to 6.7 Mbps in 2017, just below the global average of 7.0 Mbps, according to Akamai's first quarter "State of the Internet" report for 2017.⁷

High costs to access remain a primary obstacle to access for South Africans. According to the 2017 Affordability Drivers Index (ADI) rankings, South Africa is ranked 22nd of 53 countries,⁸ and is noted for having some of the highest costs of mobile communication in Africa. Recent market trends show that users are spending a greater proportion of income, at the individual and household level, on data and less towards voice or SMS services.⁹

A monopoly in the fixed-line broadband market makes it a challenge to reduce overall broadband costs, and there is a general perception that mobile operators overcharge to maximize profits. However, in the past few years several metropolitan areas including the cities of Tshwane, Johannesburg, and Cape Town, as well as the Ekurhuleni municipality¹⁰ are expanding access to

1 Statistics South Africa, "General Household Survey, 2015," June 2016, <http://www.statssa.gov.za/publications/P0318/P03182015.pdf>

2 Statistics South Africa, "General Household Survey, 2015," June 2016.

3 Statistics South Africa, "General Household Survey, 2015," June 2016.

4 "South African Internet users: age, gender, and race," *MyBroadband*, September 19, 2014, <http://bit.ly/XQtK5x>

5 As a result of separate subscriptions for voice and data services and the use multiple SIM cards in order to make use of multiple product offerings, common among prepaid users.

6 'South Africa's big smartphone Internet uptake', *MyBroadband*, accessed 29 March, 2016, <http://bit.ly/1Sj3fKQ>

7 Akamai, "State of the Internet, Q1 2017 Report," <https://goo.gl/TQH7L7>

8 "2017 Affordability Report," Alliance for Affordable Internet. Accessed 04 June 2017, <http://bit.ly/2lv3q0m>

9 ResearchICT Africa, UPDATE: State of prepaid market in South Africa: Submission to the Parliament of South Africa on "The Cost to Communicate in South Africa", <http://bit.ly/2o0fpnF>

10 "Free WiFi for Ekurhuleni," *ITWeb*, 10 November, 2016, accessed 29 March, 2016, <http://bit.ly/1XZT5mH>

free public Wi-Fi infrastructure, providing users with access up to 500MB of free data per day.¹¹ In October 2015, the city of Tshwane's Project Isizwe recorded 1 million unique users, a figure that is particularly significant given that the project services primarily low income areas within the city.¹²

Restrictions on Connectivity

The South African government does not have direct control over the country's internet backbone or its connection to the international internet. International internet connectivity is facilitated via fibre undersea cables—SAT-3, SAFE, WACS, EASSy, and SEACOM—all of which are owned and operated by a consortium of private companies.¹³ Several operators oversee South Africa's national fiber networks, including partly state-owned Telkom and privately owned MTN, Vodacom, Neotel, and FibreCo, 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 ISP Association (ISPA) and NapAfrica.¹⁴

ICT Market

The Internet Service Providers Association (ISPA) currently has 184 members in South Africa and has never experienced a period of negative growth over the past 21 years.¹⁵ However, the fixed-line connectivity market is dominated by Telkom,¹⁶ a partly state-owned company of which the government has a 40 percent share and an additional 12 percent share through the state-owned Public Investment Corporation.¹⁷ Telkom effectively possesses a monopoly, despite the introduction of a second national operator, Neotel, in 2006.¹⁸ In the mobile market, there are five mobile phone companies—Vodacom, MTN, Cell-C, Virgin Mobile, and Telkom Mobile—all of which are privately owned except for Telkom Mobile, which falls under the partly state-owned Telkom.

The fiber market in South Africa has been growing at an exponential rate. Most suburban areas in the main South African cities (including Pretoria, Cape Town and Johannesburg, Durban, and Port Elisabeth) are already covered with fibre-optic cables, and new "last mile" providers of fiber have begun to wire homes by connecting to competitive internet backbones operated by bigger operators. The model that most of these providers have adopted is open access: they provide FTTH (fiber to the home) or FTTB (fiber to the building), and the customer can select an ISP from a large number of competitive options.

Access providers and other internet-related groups are active in lobbying for better legislation and regulations. The ISPA was recognized as a self-regulatory body by the Department of Communications in 2009.¹⁹

11 "City of Tshwane doubles daily free WiFi data limit for residents," *HTXT.Africa*, 10 November, 2015, accessed 29 March, 2016, <http://bit.ly/1ZI4eK8>

12 "Tshwane free Wi-Fi hits one million device milestone," *TimesLIVE*, accessed 29 March, 2016, <http://bit.ly/1XZT5mH>

13 "This is what South Africa's Internet actually looks like," *MyBroadband*, March 9, 2014, <http://bit.ly/1r5maRn>

14 Jan Vermeulen, "Here is who controls the Internet in South Africa," *MyBroadband*, July 17, 2014, <http://bit.ly/1oQTm8p>

15 ISPA membership shows solid growth. *MyBroadband*, 26 January 2017, <http://bit.ly/2n27mHS>

16 Quinton Bronkhorst, "SA's biggest ICT challenges," *BusinessTech*, December 26, 2013, <http://bit.ly/1W2ySdR>

17 "Here is Government's shareholding in South African telecoms companies," *MyBroadband*, June 23, 2015, <http://bit.ly/1MS4Vgf>

18 As reported in Freedom House 2013, Neotel has chosen to focus on providing wireless internet and telecom services, which has had minimal impact on last mile connectivity and the associated price of broadband.

19 Internet Service Providers Association, <http://ispa.org.za/about-ispa/>

Regulatory Bodies

The autonomy of the regulatory body, the Independent Communications Authority of South Africa (ICASA), is protected by the South African constitution, although telecom observers contend that ICASA's independence has weakened as a result of various incidents over the past few years.

In September 2016, ICASA initiated the process to auction spectrum in the 700MHz, 800MHz, and 2,600MHz bands that is critical to the expansion of telecommunications networks.²⁰ However, the Minister of Telecommunications and Postal Services, Siyabonga Cwele, interdicted ICASA from proceeding with the auction,²¹ instead putting forward an alternative model of spectrum allocation in the form of a publicly-owned wholesale open access network,²² a move that was widely criticized as an impediment to competition and investment.²³ According to the ministry, auctioning spectrum to private companies would result in the duplication of infrastructure; shared infrastructure would ultimately drive down the cost of communication through competition among services.²⁴ The ministry's proposal for a wholesale open access network was approved by the cabinet as part of the National Integrated ICT Policy,²⁵ a white paper that provides direction for the development of electronic communications in South Africa, including the alignment of existing legislation and has implications on the regulation of the sector.

The Film and Publications Board (FPB) traditionally regulates the distribution of films, games, and other publications in South Africa but may soon regulate internet content under proposed amendments to the Film and Publications Act, 1996 (see "Content Removal"). In March 2016, the FPB signed a memorandum of understanding with ICASA to address regulatory overlaps created by the proposed amendments, which will effectively create co-jurisdiction over online content.²⁶ However, as of March 2017, it remains unclear how the two bodies will implement the agreement.

Limits on Content

The Film and Publications Amendment Bill introduced in 2015 may impose intermediary liability and a censorship regime on South Africa's online content but was stalled in deliberation due to potential overlap with a new Cybercrimes and Cybersecurity Bill. Digital activism around the high cost of data elicited positive parliamentary action but with no concrete improvements due to bureaucratic inertia.

Blocking and Filtering

Under the current legal and regulatory framework, neither the state nor other actors block or filter internet and other ICT content, and there is no blocking or content filtering on mobile phones. However, government officials have increasingly pronounced the need for social media regulation,

20 "Spectrum auction postponed, BEE requirements relaxed," *MyBroadband*, 25 September 2016, <http://bit.ly/2n1gRXJ>

21 "Cwele gets interdict against Icasa: 4G spectrum licensing must stop," *MyBroadband*: 30 September 2016, <http://bit.ly/2nwryR>

22 "Government unrelenting about wholesale open access network," EE Publishers, 23 February 2017, <http://bit.ly/2ov9rMg>

23 "Open Access wireless networks threaten competition and investment," Research ICT Africa, Policy Brief No. 5 2016 <http://bit.ly/2nCqXKN>

24 "Let's not build another monopoly," Tech Central, 20 February, 2017. <http://bit.ly/2r2WVpl>

25 "Cabinet finally approves SA ICT policy," Fin24 tech, 29 September 2016, <http://bit.ly/2nOgLL5>

26 'ICASA signs a Memorandum Of Understanding with the Film and Publication Board', Independent Communications Authority of South Africa, accessed 11 March 2016, <http://bit.ly/1ZAg9tz>

leading to concerns of online censorship. In March 2017, Minister of State Security David Mahlobo reiterated calls to regulate social media, stating that it was being abused to, among other things, peddle false information.²⁷ Media freedom advocacy groups sounded alarms over the potential political agenda behind the government's repeated fear-mongering tactics around fake news.²⁸

Content Removal

During this report's coverage period, there were no reported incidences of legal, administrative, or other means used to force the deletion of content from the internet in a way that contravenes international norms for free speech or access to information.

Section 77 of the Electronic Communications Act of 2002 (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 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.²⁹ As a result, ISPs often err on the side of caution by taking down content upon receipt of a notice to avoid litigation, 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. Meanwhile, any member of the public can submit a takedown notice, and there are no existing or proposed appeal mechanisms for content creators or providers.

In 2016, a total of 355 takedown notices were lodged with ISPA; of those, 220 were accepted, 127 rejected, and 8 were either withdrawn or duplicate requests. Of the 220 notices accepted, 211 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.³⁰

In July 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.³¹ Linked to a lands rights lobby group called Black First Land First, the news site had published articles criticizing "white monopoly" over capital.³² The website was restored two weeks later.³³

The Film and Publications Amendment Bill introduced in 2015 may impose intermediary liability and a censorship regime on South Africa's online content. Drafted for the purpose of protecting children from racist, harmful, and violent content online, initial amendments proposed in May 2016 aimed to allow the FPB to pre-censor online content or take down existing content—including user-generated

27 "Social media in SA could be regulated," Mail and Guardian, 05 Mar 2017, <http://bit.ly/2nz3zh8>

28 "Panel slams Mahlobo's call for social media regulation," The Citizen, 3 March 2017, <http://bit.ly/2nNtcvS>

29 Section 73 of the Electronic Communications and Transactions Act of 2002 (ECTA) reaffirms the limitation of service provider liability for information that is transmitted, stored or routed via a system under its control. *Electronic Communications and Transactions Act of 2002*, Government Gazette, Republic of South Africa, <http://bit.ly/1pWWWGF>.

30 Take-down Statistics. ISPA, 2016, <http://bit.ly/2n3Kc3R>

31 "Drive to shut down websites with links to BLF," Times Live, July 17, 2017, <https://www.timeslive.co.za/politics/2017-07-17-website-with-links-to-guptas-shut-down/>

32 "Why Hetzner shut down Gupta-linked website," My Broadband, July 17, 2017, <https://mybroadband.co.za/news/internet/220116-why-hetzner-shut-down-gupta-linked-website.html>

33 "Black Opinion is back online!," Black Opinion, July 24, 2017, <https://blackopinion.co.za/2017/07/24/black-opinion-back-online/>

content—that failed to meet certain classification requirements.³⁴ The proposed policy was widely criticized for giving the government “wide-sweeping powers to censor content on the internet.”³⁵ Based on critical stakeholder feedback, the FPB released a revised bill in October 2016, which is still up for discussion as of October 2017.³⁶ However, with the introduction of the Cybercrimes and Cybersecurity Bill to Parliament in February 2017 (see Legal Environment), progress on the Film and Publications Amendment Bill have been stalled due to concerns of possible overlap between the two bills.³⁷

Media, Diversity, and Content Manipulation

Online media in South Africa is vibrant, representing a wide range of viewpoints and perspectives. Web-only news platforms, such as the *Daily Maverick*, have become particularly popular in recent years, with key news stories often broken online before print or broadcast, illustrating how online media is growing as a primary source of news in the country. In line with this development, recent anecdotal evidence suggests that South African youth are increasingly reliant on the internet and radio for information and are less dependent on television and print news for current affairs.³⁸ Similarly, there are indications that in rural areas with internet access, the online versions of community newspapers are being accessed ahead of their print versions.³⁹ Nevertheless, while both English- and Afrikaans-language content is well represented online, 9 of South Africa’s 11 official languages are underrepresented, including on government websites.

New registration fees on video streaming services threaten to impede local content creation. In March 2016, the Film and Publications Board directed video streaming services, including Netflix, to pay a ZAR 795,000 (approximately US\$50,000) registration fee to distribute content under the self-classification criterion imposed on online distributors by the FPB.⁴⁰ The size of the fee has been criticized by industry stakeholders as unjustifiable (in relation to the actual cost of classification) and prohibitive for smaller competitors providing content streaming services.⁴¹ As of mid-2017, Netflix along with other online content distributors had not paid the prescribed fee.⁴²

Online self-censorship is low in South Africa, and the government does not limit or manipulate online discussions. Nevertheless, ANC-aligned businessmen have made significant inroads into the media landscape by acquiring or launching new media products over the past few years, leading to concerns over increasing pro-government bias among prominent media outlets.

34 Rebecca Kahn, “Scary new Internet censorship law for South Africa,” *Huffington Post*, August 9, 2015, www.huffingonpost.com/rebecca-kahn/south-africa-might-get-the-b-8102720.html; “Scary new Internet censorship law for South Africa,” *MyBroadband*, October 20, 2015, <http://mybroadband.co.za/news/internet/142980-scary-new-internet-censorship-law-for-south-africa.html>.

35 Paula Gilbert, “Internet ‘censorship’ Bill may see changes,” *ITWeb*, October 18, 2016, http://www.itweb.co.za/index.php?option=com_content&view=article&id=156791.

36 The Film & Publications Board and online content regulation, *Ellipsis Regulatory Solutions*, <http://www.ellipsis.co.za/the-film-publications-board-and-online-content-regulation/>; Paula Gilbert, “Internet ‘censorship’ Bill may see changes,” *ITWeb*, October 18, 2016, http://www.itweb.co.za/index.php?option=com_content&view=article&id=156791.

37 The Film & Publications Board and online content regulation, *Ellipsis Regulatory Solutions*, 26 January 2017, <http://bit.ly/1PDMrMA>.

38 Suggested by Anton Harber, Professor of Journalism and Media Studies at the University of Witwatersrand.

39 Suggested in an access workshop held in East London in November 2013, run by Afesis-Corplan.

40 Gareth van Zyl, “EXCLUSIVE: FPB asks Netflix to pay R795k licensing fee,” *FinTech24*, April 2016, <http://bit.ly/1YUL2bz>.

41 Jan Vermeulen, “Netflix – don’t pay R795,000 to the FPB,” *MyBroadband*, March 23, 2016, <http://bit.ly/1XQcUPA>.

42 “Honeymoon will soon be over for Netflix in South Africa” *MyBroadband*, 13 March 2017, <http://bit.ly/2nvwUDW>.

In line with the growing trend of online manipulation disrupting democratic processes in countries around the world, news reports in July 2017 revealed the existence of hundreds of automated bots on Twitter that work to harass journalists who report critically about the wealthy Gupta family and their influential ties to President Zuma.⁴³ The harassment may have the effect of increasing self-censorship among critical reporters and distorting the online information landscape with misleading narratives and false information.

Digital Activism

The internet has become a successful tool for online mobilization and democratic debate in South Africa, and the use of the internet and other ICTs for social mobilization has been mostly uninhibited by government restrictions.

In September 2016, civil society took on the call to bring down the high cost of digital communications using the hashtag DataMustFall.⁴⁴ Eliciting a positive response, parliament's portfolio committee on telecommunications and postal services convened a hearing with submissions presented by the communications department, the regulator (ICASA), civil society organisations, telecoms operators and the public on the cost to communicate and on mobile data in particular.⁴⁵ However, despite the minister of telecommunications issuing ICASA with a directive to hold an inquiry which would finalise regulations to ensure effective competition, bureaucratic inertia within ICASA has resulted in little progress towards bringing down the cost of data.⁴⁶

Violations of User Rights

South Africa voted against the UN Resolution for "the Promotion, Protection and Enjoyment of Human Rights on the Internet" in July 2016 and continued to deliberate on the draft Cybercrimes and Cyber Security Bill, which has provisions that may threaten freedom of expression and privacy rights. The appointment of an Inspector-General of Intelligence in March 2017 is expected to strengthen oversight mechanisms for state intelligence and surveillance activities.

Legal Environment

The South African constitution provides for freedom of the press and other media, freedom of information, 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."⁴⁷ Libel is not a criminal offense, though civil laws can be applied to online content, and criminal law has been invoked on at

43 Katherine Child, "Pro-Gupta bots unmasked," Times Live, July 10, 2017, <https://www.timeslive.co.za/politics/2017-07-10-pro-gupta-bots-unmasked/>; Andrew Fraser, "TechCentral: We go inside the Guptabot fake news network," Daily Maverick, September 5, 2017, <https://www.dailymaverick.co.za/article/2017-09-05-techcentral-we-go-inside-the-guptabot-fake-news-network>

44 "#DataMustFall: SA Twitter gives networks ultimatum to lower prices," *hxtx.africa*, 15 September 2016, <http://bit.ly/2oqrrb5>

45 RSA Parliament, Portfolio Committee On Telecommunications And Postal Services. Public Hearing on Cost to Communicate: public hearings: Day 1 <http://bit.ly/2rCp4SQ> and Day 2 <http://bit.ly/2qXllpG>

46 Competition Commission probe on high cost of data on the cards. TimesLive, 24 May 2017, <http://bit.ly/2s4UnHa>

47 Constitution of the Republic of South Africa, Bill of Rights, Chapter 2, Section 16, May 8, 1996, <http://bit.ly/1RUcGly>

least one occasion to prosecute against injurious material.⁴⁸ The judiciary in South Africa is generally regarded as independent.

In a worrisome development for internet freedom, South Africa voted against the UN Resolution for “the Promotion, Protection and Enjoyment of Human Rights on the Internet” in July 2016, siding with repressive countries such as China, Russia, and Saudi Arabia among the few objectors. In its opposition, South Africa’s deputy permanent representative to the UN noted concerns that the resolution failed to take into account hate speech and incitement, which pose unique challenges to freedom of expression in South Africa’s post-apartheid society.⁴⁹

Meanwhile, the draft Cybercrimes and Cyber Security Bill—first published in August 2015 for public comment—has been criticized by civil society for its ambiguous language that has the potential to infringe on freedom of expression.⁵⁰ In the 2017 version of the bill introduced in February, a chapter on “Malicious Communications” penalizes the dissemination of a “data message which is harmful,” the definition of which includes content that is “inherently false” without further specifications.⁵¹ Human rights advocates worry that the vague provision could be interpreted to censor political speech.⁵² The bill also includes problematic provisions that may enhance the state’s surveillance powers (see Surveillance, Privacy, and Anonymity). As of September 2017, formal proceedings towards the review of the bill by the portfolio committee were ongoing with public hearings scheduled for discussion.⁵³

Prosecutions and Detentions for Online Activities

Individuals were not prosecuted, detained, or sanctioned by law enforcement agencies for political, social, or religious speech online during the coverage period.

Surveillance, Privacy, and Anonymity

Concerns over the potentially unchecked powers of government surveillance of online activities remains high in South Africa but were addressed when Dr. Setlhomamaru Isaac Dintwe was appointed as the new Inspector-General of Intelligence in March 2017. The position had previously been vacant for an extended period due to challenges in the recruitment process.⁵⁴ As an independent actor accountable to parliament through the Joint Standing Committee on Intelligence,⁵⁵ the Inspector-General of Intelligence is expected to strengthen oversight mechanisms

48 See: Freedom House, “South Africa,” *Freedom of the Net 2011*, <http://bit.ly/1PEi9Oa>

49 Gareth van Zyl, “Why SA voted against internet freedoms at the UN,” *fin24* *ech*, July 5, 2016, <http://www.fin24.com/ech/News/why-sa-voted-against-internet-freedoms-at-the-un-20160705>

50 CYBERCRIMES AND CYBERSECURITY BILL, 2015: <http://www.justice.gov.za/legislation/invitations/cybercrimesbill2015.pdf>

51 Cybercrimes and Cybersecurity Bill 2017, Chapter 3, Section 17: <https://www.ellipsis.co.za/wp-content/uploads/2017/02/b-6-2017-cybercrimes.pdf>

52 South African Human Rights Commission Submission on the Cybercrimes and Cybersecurity Bill [B6-2017], https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_SAHRC.pdf; https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_CFCR.pdf

53 The Cybercrimes and Cybersecurity Bill, updates by Ellipsis, accessed September 11, 2017, <https://www.ellipsis.co.za/cybercrimes-and-cybersecurity-bill/>

54 Setlhomamaru Dintwe appointed as SA’s top spook. ILO, 13 March 2017, <http://bit.ly/2n4DTNa>

55 Mandate: Office of the Inspector-General of Intelligence, Accessed 30 March 2017, <http://bit.ly/2o39EFF>

over the activities of the South African Intelligence Services and determine their compliance with the legislative framework and Constitution.⁵⁶

The Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA) regulates the surveillance of domestic communications. Among its provisions, RICA requires ISPs to retain customer data for an undetermined period of time and bans any communications system that cannot be monitored, placing the onus and financial responsibility on service providers to ensure their systems have the capacity and technical requirements for interception.⁵⁷ While RICA requires a court order for the interception of domestic communications, the General Intelligence Laws Amendment Act (known locally as the “Spy Bill”) passed in July 2013 enables security agencies to monitor and intercept foreign signals (electronic communications stemming from abroad) without any judicial oversight.⁵⁸

RICA also compromises users’ right to anonymous communication by requiring mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of a physical address to service providers.⁵⁹ An identification number is legally required for any SIM card purchase, and registration requires proof of residence and an identity document.⁶⁰ For the many South Africans who live in informal settlements, this can be an obstacle to mobile phone usage. Meanwhile, users are not explicitly prohibited from using encryption, and internet cafes are not required to register users or monitor customer communications.

Despite the legal framework for the interception of communications established under RICA, there have been worrying reports that the National Communications Centre (NCC)—the government body tasked with collecting intercepted signals—conducts surveillance without regard to RICA, thus extralegally. In a June 2013 investigative report, the *Mail & Guardian* reported that the NCC monitors mobile phone conversations, SMS, and emails, “largely unregulated and free of oversight.”⁶¹ According to the report, the NCC also has the technical capacity and staffing to monitor both SMS and voice traffic originating from outside South Africa. Calls from foreign countries to recipients in South Africa can ostensibly be monitored for certain keywords; the NCC then intercepts and records flagged conversations. While some interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system also allows the NCC to record South African citizens’ conversations without a warrant and is subject to abuse without sufficient oversight mechanisms.⁶²

Persistent concerns over government surveillance grew further after reports in 2015 found that state security organizations possess stingray (or “grabber”) technology that can mimic cell phone towers and capture cell phone metadata within a certain vicinity. In September 2015, Hlanwgani Mulaudzi, a spokesperson for the government investigation bureau known as the Hawks,⁶³ confirmed that South African security officials have access to grabber technology but noted that the technology was used

56 Mandate: Office of the Inspector-General of Intelligence, Accessed 30 March 2017, <http://bit.ly/2o39EFF>

57 Section 30, Act No. 70, 2002, Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002, Government Gazette, 22 January 2003, <http://bit.ly/1M5uQSD>

58 “Zuma passes ‘spy bill,’” *News24*, July 25, 2013, <http://bit.ly/1hOxVlf>

59 Chapter 7, “Duties of Telecommunication Service Provider and Customer,” RICA, <http://bit.ly/1W2EbKc>

60 Nicola Mawson, “‘Major’ RICA Threat Identified” *ITWeb*, May 27, 2010, <http://bit.ly/16aWGqe>

61 Phillip de Wet, “Spy wars: South Africa is not innocent,” *Mail & Guardian*, June 21, 2013, <http://bit.ly/1jRPVD9>

62 Moshoeshe Monare, “Every Call You Take, They’ll Be Watching You,” *Independent*, August 24, 2008, <http://bit.ly/1RmaimM>

63 The Hawks are South Africa’s Directorate for Priority Crime Investigation (DPCI) which targets organized crime, economic crime, corruption, and other serious crime referred to it by the President or the South African Police Service.

specifically for national security matters only.⁶⁴ Nonetheless, consistent weaknesses in oversight mechanisms within the state security departments leave surveillance open to abuse.

The proposed Cybercrimes and Cyber Security Bill revised in February 2017 includes a provision that may enhance the state's interception powers. According to the Centre for Constitutional Rights, section 38 of the bill, which provides for the interception of "indirect communication, obtaining of real-time communication-related information and archived related information," both conflicts with and echoes the problematic aspects of RICA, potentially infringing on privacy rights.⁶⁵ As of September 2017, formal proceedings towards the review of the bill by the portfolio committee were ongoing with public hearings scheduled for discussion.⁶⁶

As a positive measure, the Protection of Personal Information (POPI) Act, signed into law in November 2013, provides measures to protect users' online security, privacy, and data. No law ensuring the constitutional right to privacy existed previous to POPI, which allows an individual to bring civil claims against those who contravene the act.⁶⁷ Penalties for contravening the law are stiff, including prison terms and fines of up to ZAR 10 million (approximately US\$650,000).

To further strengthen the right to privacy enshrined in POPI, President Jacob Zuma appointed Pansy Tlakula as Information Regulator in October 2016.⁶⁸ Known for her independence, Tlakula had previously served as the Chairperson of the Independent Electoral Commission Advocate and as the Special Rapporteur on Freedom of Expression and Access to Information at the African Commission on Human and Peoples' Rights. Primarily tasked with monitoring, enforcing compliance, and handling complaints related to POPI,⁶⁹ the Office of the Information Regulator is expected to give effect to the constitutional right to privacy by introducing measures that ensure personal information is processed legally by responsible parties.⁷⁰

Intimidation and Violence

There were no cases of extralegal intimidation or violence reported against bloggers, journalists, or online users during the coverage period.

Technical Attacks

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. 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.

64 "Grabber used for 'national security,'" ITWeb, 8 September, 2015, <http://bit.ly/1RDPadu>

65 Centre for Constitutional Rights, submission on the Cybercrimes Bill, August 10, 2017, https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_CFCR.pdf

66 The Cybercrimes and Cybersecurity Bill, updates by Ellipsis, accessed September 11, 2017, <https://www.ellipsis.co.za/cybercrimes-and-cybersecurity-bill/>

67 Lucien Pierce, "Protection of Personal Information Act: Are you compliant?" *Mail & Guardian*, December 2, 2013, <http://bit.ly/1ZUn16t>

68 "Pansy Tlakula appointed as new information regulator.," News24, 26 October 2016, <http://bit.ly/2e35kRC>

69 Protection of Personal Information Act (2013). Department of Justice, <http://bit.ly/2ourhPs>

70 "Minister Michael Masutha meets with Information Regulator," South African Government press release, 11 Jan 2017, <http://bit.ly/2ouwhE7>