FREEDOM
ON THE NET
2014

Freedom House

South Africa

	2013	2014
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	7	7
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	11	11
TOTAL* (0-100)	**26**	**26**

* 0=most free, 100=least free

Population:	53 million
Internet Penetration 2013:	49 percent
Social Media/ICT Apps Blocked:	No
Political/Social Content Blocked:	No
Bloggers/ICT Users Arrested:	No
Press Freedom 2014 Status:	Partly Free

Key Developments: May 2013 – May 2014

- A new broadband policy called South Africa Connect was initiated in December 2013, with aims to provide every citizen access to a broadband connection at a cost of 2.5 percent or less of the average monthly income by 2020. This policy was complemented by the rollout of broadband plans in provinces like Gauteng, which aim to provide free internet access to the poor (see **Obstacles to Access**).

- There were no incidents of online censorship in South Africa during the coverage period, though video clips from a new satellite news channel posted on YouTube were taken down for alleged copyright violations in August 2013; some speculated political motivation behind the requests (see **Limits on Content**).

- While the online sphere is becoming a dominant source of news and information for South Africans, acquisitions by politically-aligned companies of major news outlets and the launch of new media products by pro-ANC businesses indicated the government's growing influence in the media (see **Limits on Content**).

- The General Intelligence Laws Amendment Bill, enacted in July 2013, provides state security agencies with an ambiguous authority to intercept "foreign signals intelligence" without judicial oversight (see **Violations of User Rights**).

Introduction

The digital media environment in South Africa can be described as generally free and open. A culture of free expression exists online, with diverse content available. Moreover, potentially significant moves by the government, such as the passage of a new broadband policy and funding of at least one major public access broadband initiative, suggests a positive trend toward access to the internet generally, especially for the poor. Access is a core concern for both civil society and the private sector, and in this regard, there has been an effective collaboration of interests between public and private players. While the Telkom monopoly remains a challenge in reducing overall landline costs, and there remains a general perception that mobile operators overcharge to maximize profits, public calls for a strengthening of the communications regulator to pay attention to these challenges are positive signs.

The online sphere remains diverse and active in South Africa, and marginalized communities are projected to benefit from new access initiatives over time. However, there is little evidence that the industry as a whole—including service providers, internet intermediaries, and media houses—is building a media environment based on principles of human rights and constitutional rights. The cost of access remains high, largely from profiteering and monopolistic practices, and intermediaries err on the side of caution when it comes to takedowns requests of illegal content. In August 2013, several video clips of on-air blunders from the newly launched African satellite news channel, Africa News Network 7 (ANN7), were taken down from YouTube for alleged copyright violations, though some speculated political motivation behind the requests. Meanwhile, acquisitions by companies of major news outlets aligned with the ruling African National Congress (ANC) ruling party and the launch of new media products by pro-ANC businesses during the coverage period indicated the government's growing influence in the media.

The Protection of State Information Bill (POSIB), or so-called "Secrecy Bill," made movements toward becoming law in 2014, threatening to criminalize the possession and distribution of state information, including online. Government surveillance powers increased with the passage of the General Intelligence Laws Amendment Act (or "Spy Bill") in July 2013, which ambiguously provides security agencies authority over communications from foreign servers without judicial oversight. Meanwhile, government requests for user data from Google and Facebook increased over the past year.

Obstacles to Access

Although internet penetration has expanded rapidly in South Africa, in part due to the EASSY and SEACOM fiber-optic cables, many believe that this expansion has not been fast enough for the socioeconomic development needs of the country. Nonetheless, the internet is steadily spreading across the country, with 49 percent of the South African population having access by the end of 2013, up from 41 percent in 2012, according to the International Telecommunication Union (ITU).[1] A recent household survey released in August 2013 by Statistics South Africa, the official statistics body in the country, stated that 41 percent of households have at least one member of

[1] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2013," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

the household who has access to the internet, whether at home, work, or at other locations such as internet cafes. However, access tends to fall along socioeconomic lines, with less than 10 percent of South African households enjoying the internet at home.[2]

Most internet users access the internet from their mobile phones,[3] as fixed-line broadband reached only 3 percent of the population in 2013.[4] By contrast, mobile phone penetration is 148 percent[5] as a result of separate subscriptions for voice and data services.[6] According to ITU estimates, over 25 percent of South Africans have access to mobile broadband.[7] Meanwhile, the average internet connection speed in the country is 2.6 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai's "State of the Internet" report.[8] In addition, South Africa's broadband adoption (characterized by connection speeds greater than 4 Mbps) is about 8 percent of the internet population, while the country's narrowband adoption (connection speeds below 256 kbps) is 2 percent.[9]

In an attempt to reach its universal service targets, the government, via the Universal Service and Access Agency of South Africa (USSASA), has launched various access initiatives since 1994 such as telecenters and multi-purpose community centers (now called Thusong centers). In December 2013, the Department of Communications implemented a new broadband policy called South Africa Connect, which aims to provide every citizen with access to a broadband connection at a cost of 2.5 percent or less of the average monthly income by 2020.[10] The policy also aims to give 90 percent of South Africans access to a minimum speed of 5 Mbps.

In February 2014, the Gauteng provincial government awarded a ZAR 1.5 billion (US$135 million) tender to develop the Gauteng Broadband Network to service 316 government owned buildings, 45 Thusong centers, 9 economic development zones, and 20 townships in the province. Access to the internet at these points is expected to be free, with 95 percent of the province's population connected to high-speed broadband following the completion of the 1,600 kilometer fiber-optic cable network in 2019.[11]

There are hundreds of ISPs in South Africa, with 170 ISPs belonging to South Africa's ISP Association

[2] "South Africa's Internet access states revealed," *MyBroadband*, August 26, 2013, http://mybroadband.co.za/news/internet/85165-south-africas-internet-access-stats-revealed.html.

[3] As the Statistics South Africa survey also found, nearly 80 percent of households *only* have mobile phones. See: "South Africa's Internet access states revealed," *MyBroadband*, August 26, 2013.

[4] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2013."

[5] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2013."

[6] Peter Lange, "South Africa – Telecoms, Mobile, Broadband and Forecases," BuddeComm, June 18, 2014, http://www.budde.com.au/Research/South-Africa-Telecoms-Mobile-Broadband-and-Forecasts.html.

[7] International Telecommunication Union, "South Africa Profile (latest data available: 2013)," *ICT-Eye*, accessed August 1, 2014, http://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=8.

[8] Akamai, "Average Connection Speed: South Africa," map visualization, *The State of the Internet Q1* (2014), http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

[9] Akamai, "Broadband Adoption (connections to Akamai >4 Mbps): South Africa," map visualization, *The State of the Internet,* Q1 2014; Akamai, "Narrowband Adoption (connections to Akamai <256 kbps): South Africa," map visualization, *The State of the Internet,* Q1 2014, http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

[10] "South Africa Connect: the new broadband policy," *MyBroadband*, December 8, 2013, http://mybroadband.co.za/news/government/93243-south-africa-connect-the-new-broadband-policy.html.

[11] Nontobeko Ndaba, "R1.5bn for cheaper internet access," *IOL Scitech*, February 11, 2014, http://www.iol.co.za/scitech/technology/telecoms/r1-5bn-for-cheaper-internet-access-1.1645111#.UvqA3bRdJzc.

(ISPA),[12] though the fixed-line connectivity market is still dominated by the Telkom monopoly[13]—a partly state-owned company of which the government has a 39 percent share and an additional 10.5 percent share through the state-owned Public Investment Corporation—despite the introduction of a second national operator Neotel.[14] By mid-2013, Neotel was reported to have 3,000 business customers and 152,000 consumer customers, compared to around 4 million customers using Telkom's service.

Meanwhile, there are five mobile phone companies—Vodacom, MTN, Cell-C, Virgin Mobile, and 8ta—all of which are privately owned except for 8ta, which falls under the partly state-owned Telkom. Prices for mobile services are relatively expensive, while the quality of mobile services is reportedly low.[15] As pointed out by the research firm World Wide Worx, data charges as high as ZAR 1-2 (US$0.10-0.20) per megabyte has resulted in South Africa's mobile internet uptake falling behind other African countries, such as Nigeria and Kenya.[16] South Africa's mobile affordability ranked 33rd out of 44 African countries surveyed by Research ICT Africa in 2012 for the cheapest price available from dominant operators.[17]

While the market for telecoms is fairly open, cybercafes face regulatory controls that impact their economic viability. Pursuant to Section 27(A)1 of the Electronic Communications Act, internet service providers (ISPs) and internet cafes are required to register with the Film and Publications Board (FPB), which falls under the Department of Home Affairs and is a relic, albeit a reformed one, of the Apartheid publication censorship regime. The registration requirements are not unreasonably onerous,[18] though failing to register is an offence that may be subject to a fine, six months of prison, or both. Although many internet cafes do register with the board, there is little public evidence of enforcement.

Access providers and other internet-related groups are self-organized and quite active in lobbying the government for better legislation and regulations. The autonomy of the regulatory body, the Independent Communications Authority of South Africa (ICASA), is protected by the South African constitution, although several incidents in 2011 involving ministerial policy directives sent to the regulator have called into question the extent of its independence.[19] In 2013, the Open Society Foundation conducted a review of ICASA, which found that while the institutional structure of the

[12] ISPA, "List of Members," accessed August 15, 2014, http://ispa.org.za/membership/list-of-members/.

[13] Quinton Bronkhorst, "SA's biggest ICT challenges," *BusinessTech*, December 26, 2013, http://businesstech.co.za/news/it-services/51088/sas-biggest-ict-challenges/.

[14] 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.

[15] "Mobile network quality: Vodacom vs MTN vs Cell C," *MyBroadband*, February 6, 2014, http://mybroadband.co.za/news/cellular/96253-mobile-network-quality-vodacom-vs-mtn-vs-cell-c.html.

[16] Sarah Wild, "Bridging the gaping digital divide," *Mail & Guardian*, August 16, 2013, http://mg.co.za/article/2013-08-16-00-bridging-the-gaping-digital-divide.

[17] Research ICT Africa, "South Africa's Mobile Termination Rate Debate: What the Evidence Tells Us," Policy Brief SA 2, November 2012, http://bit.ly/1aFoaE7.

[18] The applicant needs to provide his or her name, business name, national identification number, address and contact details, and nature of his or her business. The cost of registration is ZAR 462 (US$47). See, Internet Service Providers Association, "ISPA ISPs/Internet Cafés Training Course," January 2011, http://bit.ly/1bmQTP5.

[19] See: Freedom House, "South Africa," Freedom on the Net 2012, http://www.freedomhouse.org/report/freedom-net/2012/south-africa; Open Society Initiative for Southern Africa, *South Africa*, Public Broadcasting in Africa Series (Johannesburg: Open Society Initiative for Southern Africa, 2010), http://bit.ly/GzyPq8.

regulator, including in its independence from the state, is strong, the regulator lacks leadership and independence, including financial independence, for it to be fully functional.

Limits on Content

There were no incidents of online censorship in South Africa during the coverage period, though video clips from a new satellite news channel posted on YouTube were taken down for alleged copyright violations in August 2013. ANC-aligned businessmen made significant inroads into the media landscape by acquiring and launching new media products over the past year, indicating the government's growing influence in the media.

Internet content and social media platforms remain mostly free from government censorship and interference in South Africa.[20] YouTube, Facebook, Twitter, and international blog-hosting platforms are freely available.

The Electronic Communications and Transactions Act of 2002 (ECTA) requires ISPs to respond to take-down notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the Internet Service Providers' Association (ISPA)—the industry representative body—are not held liable for third-party content that they do not create or select,[21] though they can lose their protection from liability if they do not respond to takedown requests. 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.[22]

Meanwhile, any member of the public can submit a takedown notice, and there are no existing or proposed appeals mechanisms for content creators or providers. The Department of Communications has suggested improving this with a new ECTA provision that would allow a service provider to respond to the grounds of a complaint before acting upon a notice. The complainant could then reconsider and decide to withdraw the notice or send a final takedown request that would obligate the service provider to act or lose its protection from liability.[23] This proposed mechanism, however, still falls short of an actual appeals process, which remained absent as of mid-2014.

The Film and Publications Board (FPB) also regulates media and internet content in South Africa,

[20] The most recent report of government interference on freedom of expression online occurred in September 2012, when the Constitutional Court upheld a 2011 Gauteng High Court judgment ruling the controversial 2009 amendments to the Films and Publications Act of 1996 unconstitutional, based on the conclusion that the prescreening of publications (including internet content) would affect the value of news and be an unjustifiable limitation on freedom of expression. Before the Constitutional Court ruling, an art gallery successfully appealed the classification of a controversial painting of President Jacob Zuma known as "The Spear," which the ruling party tried to ban from public display and dissemination online. See, "South Africa," *Freedom on the Net 2013*.

[21] The Ministry of Communications has recognized the association as an industry representative body under the act. The association acts as an agent on behalf of its 160 members and provides the ministry with annual information about the total number of take-down notices issued, the actions taken in response, and the final results. Most of the complaints lodged are resolved amicably, with ISPA's clients agreeing to take down the offending content.

[22] Alex Comninos, "Intermediary Liability in South Africa," Intermediary Liability in Africa Research Papers, 4, October 2012, http://www.apc.org/en/pubs/intermediary-liability-south-africa.

[23] Andrew Rens, "Notice and Take Down or Notice and Notice and Take Down?" *ex Africa semper aliquid novi* (blog), November 30, 2012, http://aliquidnovi.org/notice-and-take-down-or-notice-and-notice-and-take-down/.

though it has departed dramatically from its Apartheid-era predecessor's censorship activities. Today, the FPB focuses on content classification only.[24] Critics, however, have pointed to the FPB's broadening powers following several amendments since 1996, when the body was created, which increased the range of material classified by the Film and Publications Act (1996) and "reduced the independence of the Board and the transparency of its appointment process."[25] In addition, ISPs are required to register with the FPB and must reasonably prevent and report the distribution of child pornography through their services. Nonetheless, in its 2013-2018 Strategic Plan published in January 2014, the FPB recognized its "limited capacity and procedures for the regulation of content distributed online and mobile platforms" and accordingly outlined a plan to implement the requisite infrastructure needed to "establish an efficient and effective online and new media content regulatory strategy for the country."[26]

In August 2013, several video clips of on-air blunders from the newly launched African satellite news channel, Africa News Network 7 (ANN7), were taken down from YouTube after they were uploaded by members of the public.[27] Although the takedown requests cited copyright violations, some speculated political motivation behind the requests, given that ANN7 is controlled by the powerful Gupta family from India, whose business dealings in South Africa and proximity to President Jacob Zuma have come under intense public criticism.

While copyright violations comprise the majority of takedown requests, Google's most recent transparency report from the January to June 2013 reporting period noted that the platform had received five court orders to remove eight items from its Blogger and Google+ services for content related to bullying or harassment. Google also reported that it had received one request "from the Counter Intelligence Agency to remove a blog post that allegedly infringed copyright by criticizing a media release that the agency had issued." The platform did not comply with any of the requests from that period.[28]

Online self-censorship is low in South Africa, and the government does not actively try to limit or manipulate online discussions. Nevertheless, the ANC-led government frequently complains about antigovernment media bias, and in response, ANC-aligned businessmen have made significant inroads into the media landscape by acquiring or launching new media products over the past few years. Most recently, the Independent News & Media consortium, which has over 13 mainstream newspapers under its belt, was bought by Sekunjalo Investment Holdings, a company that is said to be highly politically connected. Other shareholders in the acquisition included two Chinese companies, possibly as part of China's supposed "soft power" strategy of influence in Africa.[29]

Citizens are able to access a wide range of viewpoints and perspectives online. Web-only news

[24] The FPB's motto is: "We inform, you choose."

[25] Jane Duncan, "Monitoring and defending freedom of expression on the internet in South Africa," 2011, https://www.apc.org/en/system/files/SouthAfrica_GISW11_UP_web.pdf.

[26] "Film and Publication Board Strategic Plan for the Fiscal Years 2013/14 – 2017/18," Film and Publication Board, January 2014, http://www.fpb.org.za/profile-fpb/governance/strategic-plan.

[27] Rudolph Muller, "ANN7 videos disappearing explained," *MyBroadband,* August 26, 2013, http://mybroadband.co.za/news/broadcasting/85229-ann7-videos-disappearing-explained.html.

[28] Google, "South Africa," Transparency Report, January to June 2013, http://www.google.com/transparencyreport/removals/government/ZA/?metric=items&p=2013-06.

[29] Craig McKune, "Chinese companies scoop shares in Independent News," *Mail & Guardian*, August 15, 2013, http://mg.co.za/article/2013-08-15-chinese-companies-scoop-shares-in-independent-news.

platforms, such as the *Daily Maverick*, have attracted widespread attention in recent years. In some instances, key news stories have been broken online, 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 the South African youth are increasingly relying on the internet and radio for information and are depending less on television and print news for current affairs.[30] Similarly, there are indications that in rural areas with internet access, the online versions of community newspapers, rather than their print versions, are being accessed ahead of the print publication.[31] 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.

There are a number of political and consumer-activist websites, though the internet is not yet a key space or tool for social or political mobilization. Nevertheless, individuals and groups openly express their views via email, instant messaging, chat rooms, and social media, while the South African blogosphere has become highly active in discussing issues such as HIV/AIDS and the environment. The internet and mobile phones are increasingly used for political organization, as seen during the protests and activism against the controversial Protection of State Information Bill (POSIB) in 2012 and 2013, which President Jacob Zuma vetoed based on questions of its constitutionality and sent back to the National Assembly for reconsideration in September 2013.[32] (The bill was subsequently revised and sent back to the president for his signature, which is still outstanding as of mid-2014. See "Violations of User Rights.")

Violations of User Rights

A so-called "Secrecy Bill" made movements toward becoming law in 2014, threatening to criminalize the possession and distribution of state information, including online. Government surveillance powers increased with the passage of the General Intelligence Laws Amendment Act (or "Spy Bill"), which ambiguously grants security agencies authority over communications from foreign servers without judicial oversight. Meanwhile, government requests for user data from Google and Facebook grew.

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."[33] The judiciary in South Africa is independent and has issued a few rulings protecting online freedom of expression in recent years. Libel is not a criminal offense, though civil laws can be applied to online content, and criminal law has been invoked on at least one occasion to prosecute against injurious material.[34]

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

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

[32] "President refuses to sign draconian bill into law," Reporters Without Borders, September 12, 2013, http://en.rsf.org/afrique-du-sud-president-refuses-to-sign-12-09-2013,45168.html.

[33] Constitution of the Republic of South Africa, May 8, 1996, Bill of Rights, Chapter 2, Section 16, http://www.info.gov.za/documents/constitution/.

[34] See: Freedom House, "South Africa," *Freedom of the Net 2011*, http://www.freedomhouse.org/report/freedom-net/2011/south-africa.

In November 2013, the Protection of Personal Information Act was signed into law, enacting 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.[35] Penalties for contravening the law are stiff, including prison terms and fines of up to ZAR 10 million (over US$900,000). However, the president has yet to set a commencement date for the new legislation as of mid-2014.[36]

One piece of legislation debated throughout the coverage period—the Protection of State Information Bill (POSIB), also known as the "Secrecy Bill"—threatens to infringe on freedom of expression, press freedom, and internet freedom, if passed. In general, POSIB aims to implement a system to regulate state information, but instead places harsh restrictions on the possession or distribution of classified state information with penalties of up to 25 years in prison. Individuals who intentionally access leaked information, including internet users, would be held criminally liable and face up to 10 years in prison. Adopted by the National Assembly in November 2013, the bill still awaited President Jacob Zuma's signature as of mid-2014.[37] Opposition parties have called the bill an "assault" on democracy, while numerous civil society groups, including the South African National Editor's Forum (SANEF) and the Right2Know campaign, have actively protested the bill.[38]

The right to anonymous communication is compromised by legislation known as the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), which requires mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of a physical address to service providers.[39] An identification number is legally required for any SIM card purchase, and registration requires proof of residence and an identity document.[40] As many people in South Africa do not live in formal housing, this can be an obstacle to mobile phone usage.

The interception of communications is explicitly prohibited under RICA, unless permission is received from a judge designated to rule on the practice,[41] which includes guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards. RICA also 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.[42] Nonetheless, civil society organizations have called for greater transparency in RICA's

[35] Lucien Pierce, "Protection of Personal Information Act: Are you compliant?" *Mail & Guardian*, December 2, 2013, http://mg.co.za/article/2013-12-02-protection-of-personal-information-act-are-you-compliant/.

[36] "Dangers of data hoarding," Gadget, October 29, 2014, http://www.gadget.co.za/pebble.asp?relid=9091.

[37] "Parliament sends secrecy Bill back to Zuma again," *Mail & Guardian*, November 12, 2013, http://mg.co.za/article/2013-11-12-secrecy-bill-to-be-sent-back-to-zuma-again.

[38] "Secrecy Bill," Right2Know, accessed November 4, 2014, http://www.r2k.org.za/secrecy-bill/.

[39] Chapter 7, "Duties of Telecommunication Service Provider and Customer," RICA, http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.

[40] Nicola Mawson, "'Major' RICA Threat Identified," *ITWeb*, May 27, 2010, http://bit.ly/16aWGqe.

[41] Act No. 70, 2002, Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002, Government Gazette, 22 January 2003.

[42] 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://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/regulation-of-interception-of-communication-and-provision-of-communication-related-information-act-70-of-2002/act/70-of-2002-regulation-of-interception-of-communications-and-act-1-apr-2012-28-jul-2013-pdf/download.

implementation.[43] Meanwhile, internet cafes are not required to register users or monitor customer communications.

Government surveillance has become a growing concern in South Africa, particularly following the passage of the General Intelligence Laws Amendment Act (known locally as the "Spy Bill") in July 2013, which originally intended to formalize the monitoring and interception of foreign signals (electronic communications stemming from abroad) without oversight.[44] Prior to its passage, judicial permission was only required for the surveillance of local communications under RICA, which meant that state security apparatuses could monitor foreign signals (including on servers belonging to Facebook and Google) without any form of oversight. In response to civil society pushback against the "Spy Bill,"[45] the final version signed by the president in July omitted all mention of "foreign signals," creating concern that the exclusion would allow security agencies to continue to intercept foreign communications without any judicial review.[46]

Meanwhile, the National Communications Centre's (NCC) surveillance of mobile phone conversations, SMSs, and emails continues to raise a level of criticism from the media for its lack of transparency. The NCC also has the technical capacity and staffing to monitor both SMS and voice traffic originating 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.[47] In June 2013, critical analysis by the *Mail & Guardian* newspaper stated that the NCC "remains largely unregulated and free of oversight, while Parliament continues to fret about what its legal status should be."[48]

Government requests for user data on international communications platforms have been on the rise in recent years. Between July 2013 and June 2014, a total of nine requests were made by the government for information on nine separate user accounts on Google; none of these requests were granted.[49] Similarly on Facebook, a total of five requests for five different user account information were requested between July 2013 and June 2014, none of which were granted.[50]

Revelations in April 2013 that FinFisher spyware was being used by the partially state-owned Telkom

[43] Jane Duncan, "Monitoring and defending freedom of expression on the internet in South Africa," 2011, https://www.apc.org/en/system/files/SouthAfrica_GISW11_UP_web.pdf.

[44] "Zuma passes 'spy bill,'" *News24*, July 25, 2013, http://www.news24.com/SouthAfrica/Politics/Zuma-passes-spy-bill-20130725.

[45] "Spy Bill passed by National Assembly," Right2Know, April 23, 2013, http://www.r2k.org.za/2013/04/23/spy-bill-passed-by-national-assembly/.

[46] "Spy Bill passed," Polity.org.za, June 21, 2013, http://www.polity.org.za/article/spy-bill-passed-2013-06-21.

[47] Moshoeshoe Monare, "Every Call You Take, They'll Be Watching You," *Independent*, August 24, 2008, http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080824105146872C312228.

[48] Phillip de Wet, "Spy wars: South Africa is not innocent," *Mail & Guardian,* June 21, 2013, http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent.

[49] "South Africa," Google Transparency Report, accessed November 5, 2014, http://www.google.com/transparencyreport/userdatarequests/ZA/.

[50] "South Africa," Facebook government requests report, accessed November 5, 2014, https://govtrequests.facebook.com/country/South%20Africa/2014-H1/.

to intercept private communications have fueled further concerns of government surveillance.[51] In many other countries, such servers have been used to harvest data and user information such as "screenshots, keylogger data, audio from Skype calls, passwords and more" collected by the spyware suite.[52] While Citizen Lab also found evidence of FinFisher being deployed by the authorities in Ethiopia and used against political dissidents in Bahrain,[53] the extent to which FinFisher has been implemented in South Africa and by what entities was unknown as of mid-2014. In January 2014, the government was reported to have funded the South African IT company VASTech to develop unknown surveillance technology with intentions to sell to Libya.[54] According to the Privacy International report, the export of surveillance technologies is not regulated in South Africa.

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital technology users by state authorities or any other actor. Cyberattacks have recently become a growing issue in South Africa, and these are criminalized under the Electronic Communications and Transactions Act of 2002 (ECTA). Government websites have been hacked in the past, with the website of the South African National Road Agency Limited (SANRAL) most recently attacked. SANRAL is responsible for the controversial rollout of an e-tolling road fee system in Gauteng. In the attack, a security flaw was exposed that could give hackers access to the personal details of registered road users. According to SANRAL, the attacks disabled its website's international access.[55] In August 2013, a suspected hacker exposed a security flaw on the website for the City of Johannesburg's online e-statement system.[56] Also in August 2013, MTN was subject to a DDoS attack which had pulled down its servers, affecting its clients for a day.[57]

Cybercrime has long been a challenge in South Africa, with a 2013 Norton Report ranking South Africa as the country with the third-highest number of cybercrime victims, following Russia and China.[58] A National Cyber Security Advisory Council was set up in October 2013 as mandated by the 2012 National Cyber Security Policy Framework, which aims to coordinate business, government, and civil society actions against cyberattacks and crimes. In addition, so-called "cyber inspectors" have been mandated by the ECTA, though these inspectors do not require any specific qualifications (a point of criticism from activists and industry members), and the concept has not been properly implemented, ostensibly due to a skills shortage.[59]

[51] Morgan Marquis-Boire et al., "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, https://citizenlab.org/2013/04/for-their-eyes-only-2/.

[52] Jan Vermeulen, "FinFisher Spyware Servers in South Africa," *BusinessTech*, May 6, 2013, http://bit.ly/17HPbFN.

[53] Morgan Marquis-Boire et al., "For Their Eyes Only."

[54] Kenneth Page, "South African Government still funding VASTech, knows previous financing was for mass surveillance," Unwanted Witness, January 30, 2014, https://unwantedwitness.or.ug/south-african-government-still-funding-vastech-knows-previous-financing-was-for-mass-surveillance/.

[55] Jan Vermeulen, "Sanral E-toll website unavailable overseas due to cyber-attacks," *MyBroadband*, January 14, 2014, http://mybroadband.co.za/news/government/94765-sanral-e-toll-website-unavailable-overseas-due-to-cyber-attacks.html.

[56] "City of Joburg website "hacking" case update," *MyBroadband*, December 23, 2013, http://mybroadband.co.za/news/security/93533-city-of-joburg-website-hacking-case-update.html.

[57] Jan Vermeulen, "Cyber-attack behind Afrihost, MTN Internet problems," *MyBroadband*, August 29, 2013, http://mybroadband.co.za/news/broadcasting/85637-cyber-attack-behind-afrihost-mtn-internet-problems.html.

[58] Gillian Jones, "South Africa neglects alarming effect of cybercrime," *Business Day Live*, January 14, 2014, http://www.bdlive.co.za/business/2014/01/14/south-africa-neglects-alarming-effect-of-cybercrime.

[59] "Skilled 'cyber warriors' wanted to help South Africa fight fraud," *IT News Africa*, October 29, 2013, http://www.itnewsafrica.com/2013/10/skilled-cyber-warriors-wanted-to-help-south-africa-fight-fraud/.