SOUTH AFRICA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	8	7
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	10	11
Total (0-100)	26	26

* 0=most free, 100=least free

POPULATION: 51.1 million
INTERNET PENETRATION 2012: 41 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In May 2012, President Jacob Zuma sought to ban the display of a painting of himself known as "The Spear" from appearing online. Though he failed to win an injunction, the *City Press* newspaper removed a reproduction from its website (see **LIMITS ON CONTENT**).
- The Constitutional Court upheld a 2011 high court judgment ruling controversial 2009 amendments to the Films and Publications Act of 1996 unconstitutional, concluding that prescreening publications, including those online, is an unjustifiable limitation on freedom of expression (see **LIMITS ON CONTENT**).
- The Protection of State Information Bill, which parliament passed in 2013, will criminalize reporting on classified state information and intentionally accessing leaked information online if signed into law (see **VIOLATIONS OF USER RIGHTS**).
- The General Intelligence Laws Amendment Bill, enacted in 2013, authorized state security agencies to intercept "foreign signals intelligence" without a warrant (see **VIOLATIONS OF USER RIGHTS**).
- FinFisher command and control servers were discovered on the Telkom network in April 2013, though the extent to which the spyware has been deployed is unknown (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Digital media freedom is generally respected in South Africa. Political content is not censored, and neither bloggers nor content creators are targeted for their online activities. Access to the internet continued to expand in the past year, facilitated in part by falling costs due to the arrival of the Seacom and the East African Submarine System (EASSy) undersea cables and new fiber-optic cables, though most South Africans access the internet from their mobile phones.

In 2012 and early 2013, internet freedom in South Africa was threatened by two pieces of legislation: the General Intelligence Laws Amendment Bill (GILAB), which aimed to legalize the bulk monitoring of communications known as "foreign signals intelligence" without judicial oversight in its original 2011 version; and the Protection of State Information Bill (POSIB), which makes it illegal to publish and access certain state information, affecting whistleblowers in both traditional and digital media, bloggers, and internet users. In a positive development, the Constitutional Court found the 2009 amendments to the Films and Publications Act of 1996 unconstitutional, concluding that the requirement to prescreen and classify publications, including those online, is an unjustifiable limitation on freedom of expression.

Prior to the Constitutional Court ruling, an art gallery successfully appealed the classification of a controversial painting of President Jacob Zuma known as "The Spear." Zuma and the ANC ruling party had also sought a court injunction to ban the painting and its digital representations from public display and dissemination online, though their failed efforts only led to more widespread circulation of and greater attention paid to the artwork.

OBSTACLES TO ACCESS

The internet is steadily spreading across South Africa, with 41 percent of the South African population having access by the end of 2012, up from 34 percent in 2011, according to the International Telecommunications Union (ITU).[1] Nevertheless, access to the internet is unequal across income lines. A 2012 household and individual survey by Research ICT Africa found that internet users comprise a little over 18 percent of the population at the bottom of the economic pyramid and about 40 percent of the rest of the pyramid.[2]

[1] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. The ITU figures may be an overestimate, as they may not take into account multiple internet subscriptions. Another measure of internet usage is the South African Advertising Research Foundation's All Media Product Survey, which estimated that in December 2012, 15.7 percent of adults had used the internet in the last day, 24.6 percent in the past month, and 27.1 percent in the last year. See, South African Advertising Research Foundation, "AMPS Trended Media Data: Internet," accessed July 24, 2013, http://www.saarf.co.za/amps/internet.asp.

[2] The "bottom of the pyramid" definition uses the 2012 South African National Planning Commission Development Plan poverty datum line, defined as households with income of less than ZAR 432 per month per household member, approximately $52.50, or less than $1.80 per person per day. See, Research ICT Africa and Intelecon, *Mobile Usage at the Base of the Pyramid in South Africa*, World Bank, December 2012: 29, http://www.infodev.org/infodev-files/resource/InfodevDocuments_1193.pdf.

The majority of users access the internet from mobile phones due to the high cost of access, infrastructural limitations, and waiting periods for fixed-line ADSL broadband installation in some areas. Accordingly, mobile phone access in South Africa is much higher than internet access, with an estimated 83 percent of the population identified as mobile phone users and about 74 percent of the population using prepaid mobile services as of July 2012, according to the South African Advertising Research Foundation.[3] The latest ITU data notes over 68 million mobile phone subscriptions in 2012, amounting to a penetration rate of nearly 135 percent.[4] Moreover, access to and usage of mobile phones is more equal across economic strata than internet access, as reported by the 2012 Research ICT Africa study, which found that 75 percent of individuals at the bottom of the economic pyramid own a mobile phone, a rate that is only 14 percent lower than mobile phone ownership in the rest of the pyramid.

South Africa has five mobile phone companies—Vodacom, MTN, Cell-C, Virgin Mobile and 8ta—all of which are privately owned except for 8ta, which is owned by Telkom, a partly state-owned company of which the government has a 39.8 percent share and an additional 10.5 percent share through the state-owned Public Investment corporation. The state previously owned a stake in Vodacom through Telkom, but its shares were relinquished in 2008.[5] The costs of mobile telecommunication services are expensive, with 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.[6]

Fixed-line broadband is also expensive, as documented in a report by the telecom research firm Ovum in 2012 that sampled 20 emerging market countries and found South Africa to have the most expensive broadband tariffs.[7] One gigabyte (GB) of data per month at a speed of 512-1024 Kbps is available for 313 rand ($36),[8] while the cheapest unlimited 1 Mbps connection costs 492 rand ($56) per month.[9] Some mobile broadband packages offering small amounts of data are cheaper than the fixed-line alternatives. The cheapest prepaid mobile data packages are 40 rand ($5) for 100 MB, 120 rand ($13.50) for 500 MB, and 266 rand ($30) for 2 GB.[10] Consequently, there were only 2.2 fixed-line broadband connections per 100 inhabitants in 2012, up from 1.8 connections in 2011,[11] and those with access are generally concentrated in urban areas. South Africa also lags behind other countries in terms of broadband speed, ranking 122 out of 180 countries for download speeds in a test conducted by Ookla.[12]

---

[3] "AMPS Trended Media Data: Cellphone Trends," South African Advertising Research Foundation, accessed February 28, 2012, http://www.saarf.co.za/amps/cellphone.asp.
[4] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions, 2000-2012."
[5] Richard Wray, "Vodafone Offers £1.2bn for Control of Vodacom," *Guardian*, June 2, 2008, http://bit.ly/1dSIGD7.
[6] 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.
[7] Ovum, "Broadband Pricing in Emerging Markets in 2012," cited in Nicola Mawson, "Broadband Still Too Expensive," *ITWeb*, January 8, 2013, http://www.itweb.co.za/index.php?option=com_content&view=article&id=60921.
[8] This package includes ADSL line rental as well as mandatory fixed-line voice rental. For prices see, "1GB ADSL Accounts," *Hellkom*, accessed February 27, 2013, http://hellkom.co.za/1gb-telkom-adsl/.
[9] "1Mbps Uncapped ADSL," *Hellkom*, accessed February 27, 2013, http://hellkom.co.za/uncapped-adsl/1mbps-uncapped-adsl/.
[10] These prepaid data bundles are from the mobile operator 8ta, which is owned by the fixed-line incumbent Telkom. Prices are from http://www.8ta.com/plans/prepaid-data/, accessed February 27, 2013.
[11] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."
[12] "Download Speeds: Mongolia Beats SA," *IOL Scitech*, January 10, 2013, http://bit.ly/11ja0Xh.

There are hundreds of internet access providers (IAPs) in South Africa, with Telkom retaining a monopoly on fixed-line broadband access via ADSL. Although there is competition in the ADSL market and users can choose from hundreds of providers, ADSL lines are only available through Telkom due to its control over the "local loop" or "last mile" of connectivity, which is the copper (or fiber) line that connects to internet users' homes. While other operators and IAPs have been allowed to build their own last mile connectivity since 2008, they have yet to do so, leaving Telkom as the *de facto* consumer choice. It was hoped that the second national operator, Neotel, would enter the broadband market to increase competition, but the telecom has instead 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.

Currently, subscribers cannot enjoy ADSL without also paying for additional voice service, while IAPs selling ADSL access need to pay Telkom for its IPConnect (IPC) service for access to Telkom's local loop. As such, Telkom has been accused of charging twice for the same product by making both Telkom consumers and providers pay for access to the same ADSL network.[13] In February 2013, the Internet Service Providers Association stated that the IPC service fee still comprised up to 70 percent of the total costs for IAPs to provide ADSL internet access. In response, the Independent Communications Authority of South Africa (ICASA) regulatory body acknowledged that the high cost of IPC could be a barrier to competition in the fixed-line sector and announced plans to conduct a study of electronic communications costs in South Africa.[14]

In 2007 the Department of Communications mandated ICASA to implement local loop unbundling by 2011 to open up the local loop between IAPs and their customers to competition. The only measure towards implementing local loop unbundling that has taken place thus far is the reduction in the IPC service price, which is regarded as more of a palliative measure rather than a solution. In April 2012, ICASA promised to implement Bitstream access—a key tool in local loop unbundling—by November 2012, but as of mid-2013, Telkom has not offered any Bitstream products to the local loop, which it still completely controls.[15]

In addition to the market challenges faced by telecom service providers, 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,[16] 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.

[13] Gareth Vorster, "Telkom Charging Twice for the Same Product," *BusinessTech*, March 6 2012, http://bit.ly/wQMZZV.
[14] Bonnie Tubs, "ICASA Mulls Further IPC Cut," *ITWeb*, February 21, 2013, http://bit.ly/1eUVvQk.
[15] Jan Vermeulen, "LLU: A Lost Opportunity," My Broadband, February 11, 2013, http://bit.ly/X2fP57.
[16] 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.

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, ICASA, is protected by the South African constitution, although several incidents involving ministerial policy directives sent to the regulator have called into question the extent of its independence.[17] In addition, the Ministry of Communications has on two different attempts in recent years proposed amendments—one to the Independent Communications Authority Act and another to the Electronic Communications Amendment Act—that would have limited ICASA's independence in various ways. A cabinet reshuffle in June 2012, which saw the replacement of the minister of communications, resulted in the removal of the problematic clauses in both bills.[18]

LIMITS ON CONTENT

Internet content and social media platforms remain free from government censorship and interference in South Africa. In September 2012, 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.[19] 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.

When the 2009 amendments to the Films and Publications Act were passed—ostensibly to regulate child pornography and hate speech—they raised concerns that certain types of controversial content could be subject to prepublication censorship. The amendments required every print and online publication not recognized by the press ombudsman to submit potentially "pornographic" or "violence-inciting" materials to the government's Film and Publications Board (FPB) for approval and imposed criminal penalties for noncompliance.[20] Exemptions were provided for artistic and scientific speech, but the FPB had the discretion to grant or deny these exemptions.[21] Movies and games were classified before their release, though the FPB could not classify publications or websites until it first received a complaint from the public. Before the amendments were overturned in September 2012, appeals could be made to the FPB's Appeals Tribunal, which had been known to rule in favor of freedom of expression online in a few cases.

The most notable case presented to the FBP in 2012 involved a controversial painting by artist Brett Murray known as "The Spear," which depicted President Jacob Zuma in Soviet attire with his

[17] 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.
[18] Nicola Mawson, "ICASA's Power Affirmed by New Bills," *ITWeb,* July 16, 2013, http://bit.ly/12TdmwN.
[19] "Film and Publications Act Amendments Declared Unconstitutional," *BizCommunity*, November 3, 2011, http://www.bizcommunity.com/Article/414/466/66617.html. http://allafrica.com/stories/201209281478.html.
[20] The Film and Publications Board is part of the Ministry of Home Affairs. According to the Film and Publications Amendment Act of 2003, all ISPs are required to register with the board.
[21] Films and Publications Amendment Act, No. 3 of 2009, accessed June 4, 2010, http://bit.ly/18H9bIu.

genitals exposed. Upset by the painting's display in Johannesburg's Goodman Gallery, the African National Congress (ANC) ruling party, Jacob Zuma and his family tried to obtain a high court injunction to ban the display of the painting, arguing that the artwork infringed upon Zuma's dignity both as an individual and as president. The aggrieved parties also sought to have an image of the painting taken down from the website of *City Press* newspaper,[22] in addition to calling for a boycott of the newspaper and pressuring advertisers to withdraw business from the publication.[23] While the May 2012 court case was postponed indefinitely,[24] the Goodman Gallery came to a private agreement with the ANC to remove the painting from display in exchange for dropping charges; the *City Press* newspaper also voluntarily removed the painting's image from its website.[25]

In response to complaints over the artwork's supposedly pornographic nature, the FPB classified the uncensored version of the painting as "16N" in June 2012, effectively proscribing the artwork and its digital reproductions from being exhibited publically or online where it could be viewed by youth under the age of 16.[26] The Goodman Gallery appealed the classification to the FPB's Appeals Tribunal in July 2012, which ultimately overruled it, concluding that the painting was neither pornographic nor harmful to children.[27] The tribunal's decision stripped the artwork's classification, thereby removing all restrictions on access to the painting and its publication online or elsewhere.[28]

Under the Electronic Communications and Transactions Act of 2002 (ECTA), ISPs are required to respond to and implement take-down notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the Internet Service Providers Association are not held liable for third-party content that they do not create or select,[29] though they can lose their protection from liability if they do not respond to take-down 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 take-down notice was requested in bad faith.[30]

Meanwhile, any member of the public can submit a take-down notice, and there are no existing or proposed appeals mechanisms for content creators or providers. The Department of

[22] Karen MacGregor, "A Spear to the Heart of South Africa," *New York Times*, Op-Ed, June 5, 2012, http://nyti.ms/K9Ob5Q.
[23] David Smith, "Zuma Genitals Row Escalates as ANC Calls for Boycott of Newspaper," *Guardian*, May 25, 2012, http://www.guardian.co.uk/world/2012/may/25/zuma-genitals-row-anc-newspaper-boycott.
[24] Erin Conway-Smith, "Jacob Zuma 'The Spear' Painting Case Postponed Indefinitely," *Global Post*, May 24, 2012, http://bit.ly/LId7Bt.
[25] Phillip De Wet, "Boycott Fails, but City Press Agrees to Drop 'The Spear,'" *Mail and Guardian*, May 28, 2012, http://mg.co.za/article/2012-05-28-boycott-fails-but-city-press-agrees-to-drop-the-spear.
[26] Film and Publications Board, "FPB Classification of 'The Spear' Artwork," June 1, 2012, http://bit.ly/LRNwQu.
[27] "'The Spear' Classification Overturned," *Webber Wentzel*, October 15, 2012, http://www.webberwentzel.com/wwb/content/en/ww/ww-most-popular?oid=37612&sn=Detail-2011&pid=32704.
[28] Phillip De Wet, "Appeal Tribunal Shreds Classification of 'The Spear,'" *Mail and Guardian*, October 12, 2012, http://mg.co.za/article/2012-10-12-00-appeal-tribunal-shreds-classification-of-the-spear.
[29] 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.
[30] 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.

Communications has suggested improving this with a new ECTA provision that would allow a service provider to respond to the grounds of the complaint before acting upon the notice. The complainant could then reconsider and decide to withdraw the notice or send a final take-down request that would obligate the service provider to act or lose its protection from liability.[31] This proposed mechanism, however, still falls short of an actual appeals process.

The government does not restrict material on contentious topics such as corruption and human rights. Citizens are able to access a wide range of viewpoints, and there are no disproportionate government efforts to limit or manipulate online discussions. Online content, however, does not match the diverse interests of South Africa's society, especially with respect to the country's 10 other official languages besides English. Radio and television continue to be the main sources of news and information for most South Africans, but there are increasing efforts to extend mainstream news outlets to online platforms. All major media groups now have an online presence.

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 e-mail, instant messaging, chat rooms, and social media, while the South African blogosphere has become highly active in discussing issues such as HIV and 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 throughout 2011 and 2012, though they were unsuccessful in preventing the passage of the controversial bill. Meanwhile, the main political parties have developed online campaigns to attract young voters and are very active in social media.

VIOLATIONS OF USER RIGHTS

The Protection of State Information Bill (POSIB) was passed by parliament in 2013 and, if signed into law, will impose criminal penalties on journalists who report on classified state information and on individuals who intentionally access leaked information, including internet users. Meanwhile, a revised version of the 2011 General Intelligence Laws Amendment Bill (GILAB) was enacted in 2013 that tacitly authorizes the interception of electronic communications known as "foreign signals intelligence" without a warrant. FinFisher command and control servers were discovered on the Telkom network in April 2013, though the extent to which the spyware has been deployed is unknown.

The South African constitution guarantees freedom of the press and other media, freedom of information, and freedom of expression, among other guarantees. However, it also includes constraints, and freedom does not extend to "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that

[31] 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/.

constitutes incitement to cause harm."[32] The judiciary in South Africa is independent and has issued a few rulings protecting freedom of expression online 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.[33]

Current threats to the traditional media in South Africa may have an impact on the internet sphere. Most notably, the Protection of State Information Bill (POSIB)—passed by the lower house of parliament in late 2011 and the upper house in November 2012—imposes sentences on journalists of up to 25 years for reporting on classified information. An amended version that marginally narrowed the definition of "national security" was approved by the National Assembly in April 2013 and was awaiting the president's signature in May 2013. Once signed into law, the bill is expected to have a chilling effect on the media as well as on internet users who could face sentences of up to ten years in prison for intentionally accessing classified South African state information on whistleblower websites. Opponents vowed to challenge the bill at the Constitutional Court before it is signed into law.

Concerning restrictions on anonymous communication, another piece of legislation—the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), in force since 2005—requires mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of a physical address to service providers.[34] An identification number is legally required for any SIM card purchase, and those in possession of an unregistered SIM card are required to register with proof of residence and an identity document.[35] As many people in South Africa do not live in formal housing, this can be an obstacle to mobile phone usage. RICA also requires ISPs to retain customer data for an undetermined period of time and bans any internet system that cannot be monitored, though under the Electronic Communications and Transactions Act of 2002 (ECTA), ISPs do not have an obligation to monitor communications on their network.[36] Internet cafes are also not required to register users or monitor customer communications.

While RICA obligates ISPs to send questionable communications to a designated interception center, it also explicitly prohibits the interception of communications, except with permission from a judge designated to rule on the practice.[37] This is based on the Criminal Procedures Act, which allows law enforcement agencies to apply to a high court judge or regional court magistrate for mobile phone records or the location of a cell phone. RICA also requires judicial oversight and

[32] Constitution of the Republic of South Africa, May 8, 1996, Bill of Rights, Chapter 2, Section 16, http://www.info.gov.za/documents/constitution/.
[33] See: Freedom House, "South Africa," Freedom of the Net 2011, http://www.freedomhouse.org/report/freedom-net/2011/south-africa.
[34] Chapter 7, "Duties of Telecommunication Service Provider and Customer," RICA, http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.
[35] Nicola Mawson, "'Major' RICA Threat Identified," *ITWeb*, May 27, 2010, http://bit.ly/16aWGqe.
[36] Electronic Communications and Transactions Act, 2002, No. 25 of 2002, Article 78, "No general obligation to monitor," http://www.internet.org.za/ect_act.html#No_general_obligation_to_monitor.
[37] 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/19iWT7k.

includes guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards.

Despite explicit legislative provisions, an investigative report by the *Mail and Guardian* in 2011 found that "[s]tate intelligence agencies can—and do—access citizens' private communications illegally," and that "it is a common occurrence, especially in police crime intelligence."[38] According to the news report, the government conducts bulk surveillance of mobile phone conversations, SMS messages, and e-mails through the National Communications Center (NCC)—a government agency that houses interception facilities and operates outside the boundaries of the law because it targets "foreign signals intelligence,"[39] which is not considered under the purview of RICA.[40] According to other reports, the NCC has the technical capability and staffing to monitor both SMS and voice traffic originating outside South Africa.[41] 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 most 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.[42]

To address the concern that the NCC operates without a legislative mandate, the South African government proposed the General Intelligence Laws Amendment Bill (GILAB) in 2011 with the aim of regulating the NCC's activities and legalizing the monitoring and interception of foreign signals intelligence.[43] Known as the so-called "Spy Bill," the 2011 version of GILAB allowed for any electronic communications originating from or passing through a foreign server—such as e-mails on international platforms, Facebook, Twitter, and Voice over IP applications—to be tapped without a warrant.[44] Civil society groups voiced deep concern over the bill's "vast unchecked powers" and its infringement on constitutional rights.[45] Signed into law in July 2013,[46] a revised version of GILAB avoided concerns over the interception of foreign signals intelligence by excluding mention of it altogether, thus leaving its legalization open to vague interpretation.

---

[38] Heidi Swart, "Secret State: How the Government Spies on You," *Mail and Guardian*, October 14, 2010, http://mg.co.za/article/2011-10-14-secret-state/.

[39] "Foreign signals intelligence" is defined as: "intelligence derived from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals, and includes any communication that emanates from outside the borders of the Republic, or passes through or ends in the Republic." General Intelligence Laws Amendment Bill, Government Gazette No. 34747 of 11 November 2011, http://www.info.gov.za/view/DownloadFileAction?id=156569.

[40] Cliffe Dekker Hofmeyr et al., "The General Intelligence Laws Amendment Bill: big "GILA" is watching," Association of Corporate Counsel, March 7, 2012, http://www.lexology.com/library/detail.aspx?g=37a86080-473f-43cc-9037-9398704398ba.

[41] 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.

[42] Moshoeshoe Monare, "Every Call You Take.".

[43] General Intelligence Laws Amendment Bill, Government Gazette No. 34747 of 11 November 2011, http://bit.ly/1eUVUCj.

[44] Drew Forrest and Stefaans Brümmer, "Spooks Bid for New Powers," *Mail and Guardian,* February 3, 2012, http://mg.co.za/article/2012-02-03-spies-bid-for-new-powers/. "R2K Statement of the Final Draft of the 'Spy Bill,'" *Right2Know*, March 27, 2013, http://www.r2k.org.za/2013/03/27/r2k-statement-on-the-final-draft-of-the-spy-bill/.

[45] Cliffe Dekker Hofmeyr et al., "The General Intelligence Laws Amendment Bill: Big "GILA" is Watching," Association of Corporate Counsel, March 7, 2012; "The GILAB (aka the Spy Bill) is Back in Parliament – W You Need to Know," *Right2Know*, February 11, 2013, http://www.r2k.org.za/2013/02/11/gilab-spy-bill-back-in-parliament/.

[46] "Zuma Enacts Five New Bills into Law," *Mail and Guardian*, July 25, 2013, http://bit.ly/172tM7y.

Nevertheless, concerns over the authorities' ability to illegally intercept private communications were further heightened in April 2013 when research conducted by Citizen Lab revealed that two FinFisher command and control servers were discovered on the partially state-owned Telkom network in South Africa.[47] Such servers are used to harvest data and user information such as "screenshots, keylogger data, audio from Skype calls, passwords and more" collected by the spyware suite.[48] While Citizen Lab also found evidence of FinFisher being deployed by the authorities in Ethiopia and used against political dissidents in Bahrain,[49] the extent to which FinFisher has been implemented in South Africa and by what entities was unknown as of mid-2013. Neither Telkom nor government agencies responded to inquiries regarding the Citizen Lab findings when approached by reporters in May 2013.[50]

Meanwhile, ECTA provides for the creation of "cyber inspectors" who are given the responsibility of monitoring and inspecting websites and information systems in the public domain for unlawful activities.[51] No inspectors have been appointed since ECTA's enactment over a decade ago, though in November 2012, the Department of Communications announced that it would soon begin implementing the ECTA provision and appointing cyber inspectors to crackdown against cybercrime.[52] The inspectors are to be trained to "inspect and confiscate computers, determine whether individuals have met the relevant registration provisions, as well as search the internet for evidence of 'criminal actions.'"[53] In addition, the inspectors are not required to have any particular qualifications, and some analysts worry about the potential infringement on individuals' or companies' rights to privacy, though any search and seizure activities do require a warrant.[54]

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital technology users by state authorities or any other actor. In addition, politically-motivated hacking attacks are not significant; however, South African government websites, including the police website, have been hacked from actors outside South Africa a number of times this past year, and some remain unfixed. Meanwhile, spam and malware remain a significant problem in South Africa.

[47] 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/.
[48] Jan Vermeulen, "FinFisher Spyware Servers in South Africa," *BusinessTech*, May 6, 2013, http://bit.ly/17HPbFN.
[49] Morgan Marquis-Boire et al., "For Their Eyes Only."
[50] Jan Vermeulen, "FinFisher Spyware Servers in South Africa," *BusinessTech*, May 6, 2013.
[51] Electronic Communications and Transactions Act, 2002, No. 25 of 2002, Article 80, "Appointment of cyber inspectors," http://www.internet.org.za/ect_act.html#CYBER_INSPECTORS
[52] Thabiso Mochiko, "SA to Get Cyber Inspectors as Cyber Crime Proliferates," *Business Day*, November 14, 2012, http://www.bdlive.co.za/business/technology/2012/11/14/sa-to-get-cyber-inspectors-as-cyber-crime-proliferates.
[53] Privacy International, "South Africa," in *Silenced: An International Report on Censorship and Control of the Internet* (London: Privacy International, 2003).
[54] Shumani L Gereda, "The Electronic Communications and Transactions Act," in Lisa Thornton, Yasmin Carrim, Patric Mtshaulana and Pippa Reburn (eds.) *Telecommunications Law in South Africa*, Johannesburg, STE Publishers: 2006.