Freedom House

South Africa

	2014	2015
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	7	8
Limits on Content (0-35)	8	7
Violations of User Rights (0-40)	11	11
TOTAL* (0-100)	**26**	**27**

* 0=most free, 100=least free

Population:	**53.7 million**
Internet Penetration 2014:	**49 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2015 Status:	**Partly Free**

Key Developments: June 2014 – May 2015

- An active signal jammer was discovered in parliament at the president's annual State of the Nation address in February 2015, which blocked mobile networks and internet signals for at least an hour before the president's speech (see **Restrictions on Connectivity**).
- Concerns over the independence of the telecommunications regulator, ICASA, arose in October 2014 when the minister of communications abruptly dismissed four of ICASA's nine councilors (see **Regulatory Bodies**).
- A March 2015 Equality Court ruled that singer Sunette Bridges should be responsible for moderating and removing hate speech from her public Facebook page, setting a worrying precedent regarding liability for third party comments on websites and social networking platforms (see **Content Removal**).
- The Film and Publications Board introduced the Draft Online Regulation Policy in March 2015 that aims to protect children from harmful online content by allowing the government to pre-censor or take-down existing content that fails to meet the board's new classification requirements (see **Content Removal**).
- Leaked documents known as the "Spy Cables" reported by Al Jazeera in March 2015 led to increasing concerns over the government's surveillance intentions and capabilities (see **Surveillance, Privacy, and Anonymity**).

Introduction

South Africa's digital media environment is generally free and open. A culture of free expression exists online, and the online sphere remains diverse and active. Access is a core concern for both civil society and the private sector, which has led to collaborative efforts between public and private players to expand access to information and communication technologies (ICTs). In 2014-2015, however, ICT development was constrained by the restructuring of the communications ministry into two departments and questions regarding the independence and effectiveness of the communications regulator, the Independent Communications Authority of South Africa (ICASA).

While the South African government under President Jacob Zuma has not proactively restricted access to ICTs or internet content, sporadic incidents in recent years caused concerns. During the president's annual State of the Nation address to parliament in February 2015, an active signal jammer was discovered in parliament, which blocked mobile networks and internet signals for at least an hour before the president's speech. Opposition parties and civil society members suspected deliberate government interference.

Certain types of online content came under judicial or regulatory scrutiny during the coverage period. In March 2015, an Equality Court ruling that Afrikaans folk singer Sunette Bridges should be responsible for moderating and removing hate speech from her public Facebook page led to concerns that the case sets a dangerous precedent regarding liability for third party comments on websites and social networking platforms. Also in March, the Film and Publications Board (FPB) proposed the Draft Online Regulation Policy that aims to protect children from racist, harmful and violent content online by allowing the FPB to pre-censor online content or take-down existing content when it fails to meet certain classification requirements. The FPB regulations, as well as the Equality Court ruling on moderating social media comments, could mean a new stringent regime of intermediary liability and enforcement for South Africa's internet users.

Meanwhile, persistent concerns over government surveillance increased following reporting by Al Jazeera in February 2015 on leaked documents dubbed the "Spy Cables," which detailed the foreign surveillance activities of South Africa's State Security Agency. The government's efforts to deal with the fallout from the leaked documents led to renewed pronouncements to pass the shelved Protection of State Information Bill, which had been vetoed by President Zuma in 2013 due to questions over its constitutionality. The bill contains provisions to criminalize whistleblowers and some journalistic activity, and to allow for the classification of a large degree of state information as state secrets.

Obstacles to Access

An active signal jammer was discovered in parliament at the president's annual State of the Nation address in February 2015, which blocked mobile networks and internet signals for at least an hour before the president's speech. Concerns over the independence of the telecoms regulator, ICASA, arose in October 2014 when the minister of communications abruptly dismissed four of ICASA's nine councilors.

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 49 percent of the South African population in 2014, up from 46 percent in 2013.[1] By contrast, mobile phone penetration reached 150 percent in 2014,[2] with the majority of internet users accessing the internet on their mobile devices.[3] Meanwhile, the country's average internet connection speed is 3.2 Mbps (compared to a global average of 4.5 Mbps), according to Akamai's fourth quarter "State of the Internet" report for 2014.[4]

In a 2014 national household survey, the country's statistics agency reported that 10 percent of South African households had access to the internet at home.[5] Furthermore, according to the ITU, only 3 percent of South African households possess fixed-line broadband subscriptions.[6] Another survey found that internet users were disproportionately white (50 percent), and speak either English (65.5 percent) or Afrikaans (39 percent).[7]

A monopoly in the fixed-line market remains a challenge to reducing overall fixed-line broadband costs, and there remains a general perception that mobile operators overcharge to maximize profits. The passage of South Africa Connect—a new broadband policy that aims to connect 15 under-serviced municipalities, and by 2030, the entire country—as well as a program providing tablets to schools suggest a positive trend in increasing internet access, especially for the poor.[8]

South Africa is one of the few countries in the world that has failed to start the digital broadcasting migration process, missing the deadline of June 17, 2015 set by the ITU. Consequently, South Africans will have to wait much longer to make use of higher quality wireless broadband services such as LTE and WiMax that would be available on the spectrum freed up by the digital migration process.

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 five undersea cables—SAT-3, SAFE, WACS, EASSy, and SEACOM—all of which are owned and operated by a consortium of private companies.[9] Several operators oversee South Africa's national fiber networks, including partly state-owned Telkom and privately-owned MTN, Vodacom, Neotel, and FibreCo, among others.[10] 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.[11]

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2014, http://bit.ly/1cblxxY.

2 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. International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions," 2000-2014, http://bit.ly/1cblxxY.

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 Akamai, "Average Connection Speed," map visualization, *State of the Internet, Q4 2014 Report*, accessed May 29, 2015, http://akamai.me/1LiS6KD.

5 "internet access in South Africa: best and worst provinces," *My Broadband,* May 27, 2015, http://bit.ly/1LlXKdD.

6 International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions," 2000-2014,

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

8 "South Africa Connect: Creating Opportunities, Ensuring Inclusion," *Government Gazette*, November 20, 2013, http://bit.ly/1Llt9s8.

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

10 "This is what South Africa's Internet actually looks like."

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

While the diversity among South Africa's gatekeepers to internet access ensures that the government cannot easily shut-down access to internet or mobile phone networks, the current government under President Zuma recently demonstrated its willingness to restrict access during certain events. In February 2015, an active signal jammer was discovered in parliament at the president's annual State of the Nation address, which blocked mobile networks and internet signals for at least an hour before the president's speech. The jammer would have continued to operate if opposition parliament members did not stage a protest upon discovery of the device. The presidency claimed it was a mistake in the protocol of the State Security Agency (SSA), which had forgotten to turn it off, while the Minister of State Security stated that the jammer was being used to prevent drones from flying above parliament. These explanations were rejected by opposition parties, technical experts, and many members of civil society, who suspected deliberate government interference.[12] Following the incident, a group of media houses petitioned a high court to prevent the further use of jamming, however in May 2015, the Western Cape High court ruled that the state security agency had acted lawfully and was within its rights to use the jammer.[13]

Meanwhile, scheduled power cuts as a result of load-shedding[14] cause near daily interruptions of ICT access for most South Africans. Load-shedding is expected to last another two to three years, though carriers have made contingency plans in order to limit its effects on broadband services.[15]

ICT Market

There are hundreds of ISPs in South Africa, with 174 ISPs belonging to the ISP Association (ISPA).[16] However, the fixed-line connectivity market is still dominated by Telkom,[17] a partly state-owned company of which the government has a 39.8 percent share and an additional 12 percent share through the state-owned Public Investment Corporation.[18] Telkom effectively possesses a monopoly, despite the introduction of a second national operator, Neotel, in 2006.[19] In the mobile market, 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.

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

Regulatory Bodies

The autonomy of the regulatory body, the Independent Communications Authority of South Africa

12 Nicola Mawson, "Jamming excuses won't fly," *ITWeb*, February 20, 2015, http://bit.ly/1ARvzkR.

13 "State security allowed to jam," *ITWeb*, May 29, 2015, http://bit.ly/1NSu2AZ.

14 Load-shedding is the scheduling of electrical outages over the distribution grid to avoid total blackouts due to under-capacity.

15 RDM News Wire, "Load shedding 'to be with us' for the next three years: minister," *Sowetan,* May 15, 2012, http://bit.ly/1LItLOt.

16 Internet Service Providers' Association, "List of Members," accessed June 14 2015, http://ispa.org.za/membership/list-of-members/.

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

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

19 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.

(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.[20] In May 2014, South Africa's ICT ministry was split into two departments—the Department of Communications (DoC) and the Department of Telecommunications and Postal Services (DTPS)— resulting in ICASA being engulfed by the DoC rather than the DTPS, which created confusion and concern that the government was seeking more control over the regulator.[21]

Concerns over ICASA's independence deepened in October 2014 when the minister of communications abruptly dismissed four of ICASA's nine councilors with immediate effect and without the mandatory requirement that councilors remain in office for a period of under 45 days until they have been replaced by a new councilor.[22] As of mid-2015, no replacement councilors have been appointed, leading to speculation that the communications minister intends to reduce the overall number of councilors.[23] Furthermore, ICASA lacks financial control given its dependence on the Financial Treasury for funding and perennially cites poor resources as one of its primary challenges.[24]

The Film and Publications Board (FPB) also regulates media and internet content in South Africa, though it has departed dramatically from the censorship activities of its Apartheid-era predecessor. Today, the FPB focuses solely on content classification. Critics, however, have pointed to the FPB's broadening powers following several amendments 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." In addition, ISPs are required to register with the FPB and must reasonably prevent and report the distribution of child pornography through their services.

Limits on Content

A March 2015 Equality Court ruling that singer Sunette Bridges should be responsible for moderating and removing hate speech from her public Facebook page sets a worrying precedent regarding liability for third party comments on websites and social networking platforms. The Film and Publications Board introduced the Draft Online Regulation Policy in March 2015 that aims to protect children from harmful online content by classifying content and allowing the government to pre-censor or take-down existing content that fails to meet the classification requirements.

Blocking and Filtering

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

20 See: Freedom House, "South Africa," *Freedom on the Net 2012*, http://bit.ly/1LlYOOP; Open Society Initiative for Southern Africa, "South Africa," 2010, http://bit.ly/GzyPq8.

21 Martin Czernowalow, "Industry appalled at Zuma's ICASA edict," *ITWeb*, December 4, 2014, http://bit.ly/1LBbPCa.

22 Bonnie Tubbs, "Four ICASA councillors 'dismissed'," *ITWeb,* October 14 2014, http://bit.ly/1W2z8tx.

23 Sunil Gopal, "Muthambi's first year as minister assessed," *TechCentral,* May 8, 2015, http://bit.ly/1H5vSep.

24 Bonnie Tubbs, "ICASA still fuzzy, one year on," *ITWeb*, May 27, 2015, http://bit.ly/1hQlegv; Siphiwe Hlongwane and Dumisani Moyo, "Regulatory Independence and the public interest," *Journal of African Media Studies* 1, no. 2 (2009) http://bit.ly/1GQSGtM; Bonnie Tubs, "ICASA's independence remains moot," *ITWeb*, July 8, 2015, http://bit.ly/1ZU4uXN.

Content Removal

Non-technical measures such as legal, administrative, or other means have not been used to force the deletion of content from the internet. Access providers and content hosts are not legally responsible for third party content, nor are they are required to censor content transmitted by their users.

Nevertheless, a March 2015 court ruling against a prominent figure in South Africa may set a precedent regarding intermediary liability for third-party comments made on social media and online news platforms. In late 2014, the South African Human Rights Commission took Afrikaans singer Sunette Bridges, known as a propagandist of (the discredited) "white genocide" in South Africa campaign, to the Equality Court on accusations that the singer was hosting hate speech comments on her public Facebook page, in violation of the Equality Act.[25] In ruling that the comments from various fans indeed amounted to hate speech and harassment, the court ordered Sunette Bridges to regularly monitor her Facebook page and remove any content that could be considered hate speech, harassment, or incitement to violence.[26]

The Electronic Communications and Transactions 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. 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 March 2015, the FPB proposed the Draft Online Regulation Policy, which will allow the FPB to pre-censor online content or take-down existing content that fails to meet certain classification requirements. Drafted for the purpose of protecting children from racist, harmful, and violent content online, the proposed policy will regulate commercial content published online, such as games and films, through a classification system managed by the FPB. Problematically, online content to be classified under the proposed policy also explicitly extends to any self-generated content, including Facebook posts, tweets, YouTube videos, or any other user-generated content created in the country.[27]According to the policy, the FBP would have the power to "refer any self-generated video that is found to contain classifiable elements for classification to its classification committee, instruct the distributor to take down the unclassified content and only reinstate it after having complied with the FPB classification decision." All new commercial content (for example, films and games) would be required to apply for classification by the FPB *prior* to publication, which if abused, could lead to the pre-publication censorship of political, social, or religious content.[28] The regulations would also allow for the FPB to grant co-regulatory status to corporations, allowing them to classify their own content, and provides for a large budget for the training and deployment of "classifiers." Public comments

25 South Africa has an equality court, for cases involving discrimination and hate speech. The Equality Court functions in the High Court system, and Equality Courts are High Courts.

26 South African Human Rights Commission, "Equality Courts orders Sunette Bridges to ensure she does not promote hate speech, harassment and violence on her Facebook page," March 31, 2015, http://bit.ly/1GnMjDo; Jenna Etheridge, "Sunette Bridges reaches agreement in Equality Court," News 24, April 1, 2015, http://bit.ly/1KmiuOw.

27 PEN America, "South African Draft Online Regulation Bill Poses Censorship Threat," (blog), June 2, 2015, http://bit.ly/1jyNo19.

28 "General Notice: Notice 182 of 2015," Government Gazettee No. 38531, http://bit.ly/1MS7e2F.

on the draft online regulations were due in mid-July. In August 2015, the South African Cabinet approved the introduction of the draft policy to parliament as the Film and Publications Amendment Bill.[29]

Media, Diversity, and Content Manipulation

Citizens are able to access a wide range of viewpoints and perspectives online. Web-only 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 reliant on the internet and radio for information and are less dependent 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 are being accessed ahead of their print versions.[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.

Online self-censorship is low in South Africa, and the government does not actively try to 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 progovernment bias among prominent media outlets.

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 is uninhibited by government restrictions.

In the past year, citizens actively took to Twitter to cover, respond to, and criticize the State of the Nation address in February 2015, particularly the signal-jamming incident cut off journalists' access to mobile and internet networks during the event (see "Restrictions on Connectivity"). South African netizens also actively used Twitter to share information and revelations about the Al Jazeera "Spy Cables," which reported on leaked documents revealing the government's foreign surveillance and intelligence gathering activities (see "Surveillance, Privacy, and Anonymity").

Violations of User Rights

Persistent concerns over government surveillance increased following reporting by Al Jazeera in February 2015 on leaked documents dubbed the "Spy Cables," which detailed the foreign surveillance activities of South Africa's State Security Agency.

29 Rebecca Kahn, "Scary new Internet censorship law for South Africa," *Huffington Post*, August 9, 2015, www.huffingtonpost.com/rebecca-kahn/south-africa-might-get-th_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.

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.

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."[32] 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] The judiciary in South Africa is regarded as independent.

Prosecutions and Detentions for Online

Aside from the legal proceedings launched against singer Sunette Bridges for hosting hate speech comments on her public Facebook page (see Content Removal), individuals were not prosecuted, detained, or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs during the coverage period.

Surveillance, Privacy, and Anonymity

Persistent concerns over government surveillance increased following reporting by Al Jazeera in February 2015 on leaked documents dubbed the "Spy Cables," which detailed the foreign surveillance activities of South Africa's State Security Agency (SSA).[34] While the leaked documents focused primarily on the SSA's foreign affairs intelligence, one document revealed a secret agreement between the SSA and Zimbabwe's Central Intelligence Agency to monitor and share information about "rogue NGOs" and "media, including social networks," with an eye towards "subversive media."[35]

In response to the Spy Cables scandal, government officials including the minister of state security announced renewed intentions to pass the Protection of State Information Bill (POSIB),[36] which had been vetoed by President Zuma in 2013 based on questions regarding its constitutionality. Provisions in POSIB—also known as the "Secrecy Bill"—pose a threat to freedom of expression, press freedom, and internet freedom. In an effort to regulate state information, POSIB would place 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, could be held criminally liable and face up to 10 years in prison.

Meanwhile, surveillance of domestic communications is regulated by the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), which requires ISPs to retain customer data for an undetermined period of time. RICA also 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 intercep-

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

33 See: Freedom House, "South Africa," *Freedom of the Net 2011*, http://bit.ly/1PEi9Oa.

34 "The Spy Cables," Aljazeera video, 1:58, http://www.aljazeera.com/investigations/spycables.html.

35 Al Jazeera Investigative Unit, "Al Jazeera Investigative Documents," http://bit.ly/1hQx7D2.

36 David Smith, "South Africa scrambles to deal with fallout from leaked spy cables," *The Guardian*, February 24, 2015, http://bit.ly/1DQJnwn.

tion.[37] 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.[38]

RICA also compromises users' right to anonymous communication, requiring 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] 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 June 2013, an investigative report by the *Mail & Guardian* revealed that the NCC monitors mobile phone conversations, SMS, and emails, "largely unregulated and free of oversight."[41]According to the *Mail & Guardian*, 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.[42]

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.[43] 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-2015, after which point companies will have one year to begin compliance with the law.

Intimidation and Violence

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

37 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.

38 "Zuma passes 'spy bill,'" *News24*, July 25, 2013, http://bit.ly/1hQxVIf.

39 Chapter 7, "Duties of Telecommunication Service Provider and Customer," RICA, http://bit.ly/1W2EbKc.

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

41 Phillip de Wet, "Spy wars: South Africa is not innocent," *Mail & Guardian,* June 21, 2013, http://bit.ly/1jRPVD9.

42 Moshoeshoe Monare, "Every Call You Take, They'll Be Watching You," *Independent*, August 24, 2008, http://bit.ly/1RmaimM.

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

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.[44] Most of the hacks are perpetrated by amateur hackers with no apparent political motivations other than to advertise their skills, and consist of minor website defacements rather than incidents of data theft.

44 Through the use of a simple Google search trick, it is evident that a large number of websites have previously been "hacked" in some way or another. This can be emulated by googling the following: "hacked by" site:gov.za, or "hacked by" site:org.za. This will reveal the presence of the term "hacked by" in either governmental or NGO domains. The term is often used in the defacements. The search trick does not reveal up-to-date data, and many sites revealed have been fixed since their indexing.