



ZIMBABWE

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	17	16
Limits on Content (0-35)	14	14
Violations of User Rights (0-40)	23	24
Total (0-100)	54	54

POPULATION: 12.6 million
INTERNET PENETRATION 2012: 17 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

* 0=most free, 100=least free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- There were no reports of internet content being blocked or filtered during the coverage period, though various ruling party officials publicly expressed the desire to increase control over ICTs, particularly in the lead-up to the July 2013 general elections (see **LIMITS ON CONTENT**).
- An anonymous Facebook user with the pseudonym “Baba Jukwa” became a social media sensation for his posts exposing supposed secrets from within the ZANU-PF ruling party, in addition to his naming and shaming campaign against corrupt party officials (see **LIMITS ON CONTENT**).
- Two mobile phone users were arrested for allegedly sending text messages that insulted the president (see **VIOLATIONS OF USER RIGHTS**).
- An investigative report in early 2013 uncovered evidence of a “massive” cyber training program for Zimbabwean security agents facilitated by Iranian intelligence organizations (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

Zimbabwe's 2013 internet freedom status reflects developments in the country from May 1, 2012 to April 31, 2013, which are covered in this report. However, the July 2013 general elections entailed a number of events that directly impacted the country's internet freedom landscape.

The 2013 political contestations in Zimbabwe were likely the most internet-fueled elections to date, as various parties took to social media to campaign and promote their platforms in advance of the general elections that occurred on July 31, 2013. All major political parties had a presence on Facebook and Twitter,¹ and leading political figures used the internet to engage with citizens both in Zimbabwe and the diaspora on a daily basis. Social media was also widely used to encourage citizens to vote and counter electoral corruption, among other issues, while numerous websites were launched to monitor election irregularities²

At the time of writing in August 2013, there were no reports of internet content being blocked, or of online users arrested for their activities related to the elections, though the sensational popularity of the anonymous Facebook user, Baba Jukwa, elicited a desire by the ruling party to crackdown against individuals using social media to express criticism against the government (see "Limits on Content").³

Despite the lack of internet censorship, in the week leading up to the July 31 elections, the telecommunications regulator POTRAZ reportedly issued a directive to the private mobile phone provider, Econet, to block the dissemination of bulk SMS messages sent through its international gateway.⁴ Meanwhile, the independent community radio station, Radio Dialogue, reported frequent internet disconnections in its office, and internet café owners reported slow internet connectivity.⁵ While the government's hand behind the disruptions could not be confirmed, state control over two of the country's five international gateways, as well as the state's ability to issue directives to private telecom providers, increase the likelihood of deliberate government interference.

INTRODUCTION

Zimbabwe has witnessed an upsurge in internet use, and despite the country's recent history of political instability and economic volatility, the past two years have seen a sizeable investment in the ICT sector, which had largely been stagnant over the previous decade. In 2012 and early 2013, access to ICTs remained nominally free from direct government interference with the exception of

¹ Free & Fair Zimbabwe Election's Facebook page, accessed August 1, 2013, http://www.facebook.com/zimbabweelection?hc_location=stream.

² "In Heavy Zimbabwe Voting, No Repeat of Disastrous 2008 Events," *New York Times*, July 31, 2013, <http://nyti.ms/1aFwwvn>.

³ Cris Chinaka, "Cat-and-Mouse in Zimbabwe's Election Cyber War," Reuters, July 26, 2013, <http://www.reuters.com/article/2013/07/26/us-zimbabwe-elections-internet-idUSBRE96POSU20130726>.

⁴ Brandon Gregory, "Zimbabwe Authorities Block Award Winning SMS Service for 'Political Reasons,'" *Humanipo*, July 30, 2013, <http://www.humanipo.com/news/7611/Zimbabwe-authorities-block-award-winning-SMS-service-for-political-reasons/>.

⁵ George Mpofu and Nicolette Zulu, "FFZE: Zim Internet, Phones 'Jammed' Day Ahead of Vote," Free & Fair Zimbabwe Election, July 30, 2013, <http://zimbabweelection.com/2013/07/30/ffze-zim-internet-phones-jammed-day-ahead-of-vote/>.

the July 2013 elections period, though the relative openness is more likely due to a lack of resources to affect control than a lack of intention.

As Zimbabwe's internet community, both local and in the diaspora, has become more assertive in discussing socioeconomic and political issues online, the Zimbabwean African National Union–Patriotic Front (ZANU-PF) ruling party under President Robert Mugabe has become increasingly concerned about the internet's ability to mobilize political opposition, particularly the Movement for Democratic Change (MDC) under Morgan Tsvangirai. Accordingly, ZANU-PF officials made several public demands to stop what it calls the “abuse” of information and communication technologies (ICTs) in 2012.⁶ Meanwhile, two citizens were arrested in the past year for sending text messages on their mobile phones that allegedly insulted the president.

Zimbabwe's new constitution was enacted in May 2013, giving freedom of expression a boost both on and offline through its provisions on freedom of the press, access to government information, as well as protection for sources of information. Such guarantees, however, are likely to be nominal, given the ruling party's trend of taking extralegal actions against Zimbabwean citizens. Further, state security officials continue to have the authority to monitor and intercept ICT communications at will, and an investigative report revealed in early 2013 that Zimbabwean security agencies have been receiving cyber training assistance from Iranian intelligence organizations since 2007.

OBSTACLES TO ACCESS

Internet access has continued to expand in Zimbabwe, growing from a penetration rate of nearly 16 percent in 2011 to over 17 percent in 2012, according to the International Telecommunications Union (ITU).⁷ This figure, however, may not reflect the growing number of users who are accessing the web on their mobile devices. Research from June 2012 indicated that about 70 percent of Zimbabwean internet users are logging online via mobile phones,⁸ which likely accounts for the rapid spike in mobile phone penetration from 72 percent in 2011 to nearly 97 percent in 2012.⁹

Similar to most countries in Africa, Zimbabwe benefits from low-cost, internet-enabled imitation mobile phones from Asia. Internet access on mobile phones has been further facilitated by the introduction of 3G, 4G and EDGE technology in the past few years.¹⁰ The decreasing price of mobile internet access—which dropped from \$1.50 per megabyte (MB) in 2011 to \$1 per MB as of May 2013—has also facilitated increased access. Subscription fees for 3G services have gone down

⁶ Everson Mushava, “Technology a Security Threat: Sekeremayi,” *Newsday*, May 9, 2013, <http://www.newsday.co.zw/2013/05/09/technology-a-security-threat/>.

⁷ International Telecommunication Union, “Percentage of Individuals Using the Internet, 2000-2012,” <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

⁸ Brian Gondo, “Insights into Zim Internet Usage,” *Techzim*, June 12, 2012, <http://www.techzim.co.zw/2012/06/insights-into-zim-internet-usage/>.

⁹ International Telecommunication Union, “Mobile-Cellular Telephone Subscriptions, 2000-2012.”

¹⁰ EDGE is a faster version of the globally used GSM mobile standard.

to \$30 per month for 10 GB, and other services providers are offering 3G services on a pay-as-you-go basis for as little as \$0.10 per MB.

While mobile access to the internet has become increasingly affordable, fixed-line internet subscriptions cost \$30-\$40 per month (including installation fees) and remain expensive for many Zimbabweans who earn an average monthly wage of approximately \$180.¹¹ Nevertheless, market competition among service providers is slowly bringing down prices. For example, the cost of wireless 3G modems has decreased from \$60 to \$30 and is accessible on prepaid wireless access devices. Computer prices have also declined from an average of \$600 in 2011 to between \$350 and \$450 in 2012.

Although competition has decreased the cost of broadband internet access, effective broadband for home and individual users has not been realized due to the poor infrastructure of the state-owned fixed-line operator, TelOne. Nonetheless, both the public and private sectors have invested in expanding coverage to other parts of the country. Presenting the 2013 budget in late 2012, Finance Minister Tendai Biti stated that \$26 million had been spent on Zimbabwe's fiber-optic cable system since 2009, which included the Harare-Bulawayo fiber-optic link that was completed in 2012.¹² TelOne was also connected to Namibia Telcom's fiber cable near the border towns of Victoria Falls and Katima Mulilo in 2012. Meanwhile, other licensed data carriers are continually rolling out fiber-optic networks across the country and establishing links to international undersea cables, leading to expanding penetration.¹³ By the end of 2012, Zimbabwe's largest private telecoms provider, Econet, reported that it had expanded its broadband customer base by 75 percent, with its GSM and WiMAX (voice and data) services covering nearly 80 percent of the country.¹⁴

Most Zimbabweans access the internet in cybercafes, which have experienced a resurgence since 2010 when the country's economic situation began to improve. Recent ICT investments have also encouraged the reopening of cybercafes in the country's urban centers, in addition to the rising demand for cheaper communication tools such as Voice over Internet Protocol (VoIP) applications,¹⁵ which has been fueled by the growing expatriate population of Zimbabweans seeking to stay in touch with friends and family back home.

Despite the expanding penetration of ICTs across the country, there remains a significant urban-rural divide in access to both internet and mobile technologies, particularly as a result of major infrastructural limitations in rural areas, such as poor roads and electricity distribution. A Zimbabwe All Media Products and Services Survey released in September 2012 found that 41

¹¹ "Survey to Assist Policymakers: Zimstat," *The Herald* via *AllAfrica*, April 19, 2013, <http://allafrica.com/stories/201304190669.html>.

¹² Tonderai Rutsito, "Fibre Optic: 2012 Newsmaker," *The Herald*, January 9, 2013, <http://www.herald.co.zw/fibre-optic-2012-newsmaker/>.

¹³ BuddeComm, "Zimbabwe – Telecoms, Mobile and Broadband," accessed July 31, 2013, <http://www.budde.com.au/Research/Zimbabwe-Telecoms-Mobile-and-Broadband.html>.

¹⁴ Tawanda Karombo, "Econet Revenue and Broadband Users Surge," *ITWebAfrica*, October 26, 2012, <http://www.itwebafrica.com/telecommunications/154-zimbabwe/230183-econet-revenue-and-broadband-user-numbersurge>.

¹⁵ "Econet Wireless launches VoIP," *TeleGeography*, January 26, 2012, <http://www.telegeography.com/products/commsupdate/articles/2012/01/26/econet-wireless-launches-voip/>.

percent of adults living in urban centers are using the internet,¹⁶ with 83 percent of users accessing the web at least once a month. By contrast, an official government report estimates rural internet penetration to be 22 percent, though this figure is likely inflated given the national penetration rate of 17 percent according to the latest ITU data.

The government has endeavored to transform rural postal centers into ICT access points where internet services would be provided, but this initiative has yet to be fully realized. Even in urban areas, electricity is regularly rationed for six to seven hours a day, leading to uneven access to the internet and mobile phone service. Power outages affect not only households but also business entities such as cybercafes, while prolonged power blackouts often affect mobile telephony signal transmission equipment, resulting in cut-offs of both mobile networks and internet connections.

Zimbabwe currently has 28 licensed internet access providers (IAPs) and 128 internet service providers (ISPs),¹⁷ the former of which offer only internet access while ISPs may provide additional services. However, ISP connections are constrained by the limited infrastructure of IAPs through which they must connect. As set by the telecoms regulator, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), the license fees for IAPs and ISPs range from \$2-4 million, depending on the type of service to be provided, and must be vetted and approved by the regulator prior to installation.¹⁸ Providers must also pay 3.5 percent of their annual gross income to POTRAZ. Application fees for operating a mobile phone service in Zimbabwe are also steep, and in 2013, the regulator increased the license fees for mobile networks from \$100 million to \$180 million.¹⁹ There are no stringent fees or regulations that hinder the establishment of cybercafés.

While POTRAZ handles the official licensing process for telecoms, insider reports have revealed that the Zimbabwean military may be involved in screening and approving license applications, demonstrating that ICTs are regarded as a security matter for the state. There nevertheless have been no reports of harassment or license denials on the basis of political affiliation. Otherwise, internet access prices in Zimbabwe are set by ISPs and cybercafe owners and have thus far been free from state intervention. Individual ISPs submit tariff proposals to POTRAZ, which approves proposals on a per case basis.

Zimbabwe currently has five international gateways for internet and voice traffic, two of which are operated by the state-owned fixed network, TelOne, and mobile network, NetOne. The private mobile operators—Econet, TeleCel and Africom—operate the other three international

¹⁶ Zimbabwe All Media Products Survey, Research International Bureau, Harare September, Third Quarter Report, 2012.

¹⁷ Zimbabwe Internet Service Providers Association membership list, <http://www.zispa.org.zw/members.html>.

¹⁸ L.S.M Kabweza, "Zimbabwe Raises Telecoms Licence Fees, Migrates to Converged Licensing," *TechZim*, March 12, 2013, <http://www.techzim.co.zw/2013/03/zimbabwe-raises-telecoms-licence-fees-migrates-to-converged-licensing/>.

¹⁹ M. Kadzere, "Mobile License Fees Raised," *The Herald* via *AllAfrica*, March 12, 2013, <http://allafrica.com/stories/201303130892.html>.

gateways.²⁰ There are also two trunk switches for the TelOne fixed network and nine mobile switching centers,²¹ set up by the country's three mobile operators.²²

ISPs and mobile phone companies are regulated by the telecommunications regulatory body, POTRAZ, whose leaders are appointed by the president in consultation with the minister of transport and communication. POTRAZ has been widely accused of partisanship and politicized decision-making, such as demanding Econet to reconnect the state-owned mobile phone service provider NetOne after Econet had cut NetOne's service in August 2012 for defaulting on its interconnection fee payments.²³

LIMITS ON CONTENT

In 2012 and early 2013, there were no reports of internet content being blocked or filtered, though various ruling party officials publicly expressed a desire and intent to increase control over ICTs. Civic engagement on social media platforms increased in the last year, fueled in large part by debates and discussions surrounding the general elections that took place in July 2013, during which bulk SMS text messaging via the international gateway was blocked while internet connections were reportedly slow. An anonymous Facebook user with the pseudonym Baba Jukwa became a social media sensation for its frequent posts that exposed alleged secrets from within the ZANU-PF ruling party, in addition to its naming and shaming campaign against corrupt party officials.

Several incidents in previous years hint at the extent to which the authorities are capable of filtering web content and their intent to do so. The most recent instance of online censorship was reported in 2006, when the Zimbabwean Reserve Bank had installed an e-mail content filtering system that blocked e-mails containing the words "Morgan Tsvangirai" or "MDC" and other political content.²⁴ It is uncertain whether this practice is still ongoing. There was also a case reported in 2005 in which the authorities had traced anti-government e-mail content and arrested its suspected senders.²⁵

²⁰ Econet Wireless, "Statement on the Operation and Management of International Gateways," via *Kubatana*, October 3, 2006, http://www.kubatana.net/html/archive/inftec/061002econet.asp?sector=inftec&year=2006&range_start=1.

²¹ A "trunk switch" is a system that provides network access to many clients by sharing a set of lines or frequencies instead of providing them individually. A "mobile switching center" (MSC) connects calls by switching the digital voice data packets from one network path to another (also called routing). The MSC also provides information that is needed to support mobile service subscribers, such as user registration and authentication information.

²² L.S.M Kabweza, "An Overview of Zimbabwe's Telecommunications—POTRAZ Presentation Download," *TechZim*, March 5, 2010, <http://www.techzim.co.zw/2010/03/zimbabwe-telecoms-overview/>.

²³ "Zimbabwe's Econet Cuts Off Operator Over Fees," Reuters, August 23, 2012, <http://www.reuters.com/article/2012/08/23/zimbabwe-econet-netone-idUSL6E8JN94C20120823>; "Econet Reverses Decision to Terminate NetOne Interconnection," *The Herald* via *AllAfrica*, August 24, 2012, <http://allafrica.com/stories/201208240359.html>.

²⁴ Anonymous interviews with state media journalists at Zimpapers and Zimbabwe Broadcasting Holdings in January 2013; Clapperton Mavhunga, "The Glass Fortress: Zimbabwe's Cyber-Guerrilla Warfare," *Concerned Africa Scholars*, Bulletin 80 – Winter 2008, <http://concernedafricascholars.org/docs/acasbulletin80-4.pdf>.

²⁵ Open Net Initiative, "Country Profile: Zimbabwe," 2009, <http://opennet.net/research/profiles/zimbabwe>.

The last attempt by the authorities to implement a more systematic internet censorship regime occurred in 2004 when the government proposed a contract for all ISPs requiring them to block “objectionable” content and communications that were “inconsistent with the laws of Zimbabwe” as well as report “malicious messages” to the authorities.²⁶ Some ISPs agreed to comply with the proposed contract before it was declared unconstitutional by the Supreme Court a few months later.²⁷ No other such attempts to impose systematic restrictions on ICTs have been reported since.

Nevertheless, the government has routinely exhibited a desire to control digital communications, particularly during times of high political tension, such as elections or other potentially volatile situations. These efforts have been made primarily through intimidation and threats. Around the time of ZANU-PF’s December 2009 party congress, for example, the authorities issued a warning to operators against allowing subscribers to use their networks for political purposes, which came in response to a mass circulation of text messages that had castigated the ruling party. The private telecom provider, Econet, in turn warned its subscribers that their service would be cut off if they sent political messages.²⁸

Similarly in 2010, after the MDC announced that it would be using an Econet line to send bulk SMSs to keep in contact with its supporters, a column appeared in the government-controlled *Herald* newspaper that threatened to cancel Econet’s operating license.²⁹ In response, Econet openly complained about the MDC’s use of the network for political purposes and announced that it was installing software to identify and block problematic messages. These threat tactics from the authorities remain to this day and serve as a constant reminder to service providers of the need to remain in government favor. Mass SMS texting of apolitical nature is largely approved, but mobile service providers often refrain from carrying bulk messages sent by the MDC. To bypass such restrictions, the civic organization Kubatana, an online community of Zimbabwean activists and NGOs, uses an international gateway to send bulk text messages in the country, though this strategy failed in July 2013 when the regulator POTRAZ blocked international gateway bulk messaging in advance of the general elections.³⁰

State employees, including those working for state-owned media, exercise self-censorship when sharing politically sensitive information. The pronounced lack of anonymity on social media platforms coupled with the attendant fear of repercussions tends to limit politically oriented statements, since they can be traced back to their authors. Although many journalists contribute to

²⁶ “MWeb ‘Will Obey’ Zim E-mail Snooping Laws,” *New Zimbabwe*, June 2, 2004, <http://www.newzimbabwe.com/pages/e-mail4.11921.html>.

²⁷ “Supreme Court Bars Mugabe E-mail Snooping,” *New Zimbabwe*, March 16, 2004, <http://www.newzimbabwe.com/pages/email3.1537.html>.

²⁸ “Zanu PF Texts Sent from Sweden: Econet,” *New Zimbabwe*, December 17, 2009, <http://www.newzimbabwe.com/news-1491-Zanu+PF+texts+sent+from+Sweden/news.aspx>.

²⁹ The column was written under the pseudonym “Nathaniel Manheru,” who is believed to be President Mugabe’s spokesperson. See, Beth Jones, “Zimbabwe - ZANU-PF Threatens to Close Econet for Carrying a Political Campaign,” *Zimbio*, June 19, 2010, <http://www.zimbio.com/Zimbabwe/articles/r4ouXmtsT5e/Zimbabwe+ZANU+PF+threatens+close+Econet+carrying>.

³⁰ Gareth van Zyl, “Zimbabwean Regulator ‘Blocks’ Bulk SMS as Election Nears,” *ITWebAfrica*, July 29, 2013, <http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/231381-zimbabwean-regulator-blocks-bulk-sms-as-election-nears>.

online news platforms, quite a number use pseudonyms when writing about sensitive issues for fear of harassment, and citizens are increasingly using pseudonyms online to discuss political topics.³¹ Debates on the country's political and socioeconomic issues as well as reactions to online articles about Zimbabwe are mostly confined to chat rooms and feedback sections of online news sites. Concerns over state surveillance has also led to increasing self-censorship, and journalists and human rights defenders who feel threatened often resort to secure e-mail platforms such as Hush-Mail for correspondence out of concern that the Zimbabwe domain name .co.zw is an open book for state security.

There is a sense that the dominant political elite are losing the online battle. With the growing use of digital and social media tools, the ruling party has identified ICT-based communication platforms as a threat to its hold on power and has accordingly grown more intent on regulating and influencing online content.³² For example, at its December 2012 party conference, a ZANU-PF official expressed the broad intention to invest at least \$5 million in ICT and social media development to "fight cyber warfare."³³ Also in December 2012, during a meeting with the Chinese deputy minister of the State Counsel Information Office who was visiting Zimbabwe at the time, a ZANU-PF cabinet minister was quoted as stating that "there should be some form of control of the internet and other social media platforms because they [have] the potential to cause strife."³⁴

Meanwhile, Facebook, Google, Yahoo, and YouTube, are among the most popular websites among Zimbabwean internet users. Media surveys indicate a declining readership of newspapers coinciding with the rising use of ICT-based platforms for news and other information.³⁵ In keeping with this shift, traditional media outlets are increasingly resorting to Facebook, Twitter, and other social media platforms to enhance their engagement with readers and listeners, receive feedback, and crowd-source news on various issues.³⁶ Due to the restrictive communications space in the country, blogs have become an important alternative platform for community organizations, minorities, individuals and online journalists to express their views. New blogs hosted by Blogspot and WordPress are on the rise, though as with journalists, some bloggers use pseudonyms out of fears of reprisal.

³¹ Vladimir Mzaca, "What Online News Means for Zimbabwe," *Free African Media*, April 5, 2011, <http://www.thezimbabwemail.com/opinion/7745.html>; Tendai Chari, "Ethical Challenges Facing Zimbabwean Media in the Context of the Internet," *Global Media Journal - Africa Edition*, Zimbabwe, 2009, Vol 3 (1), <http://globalmedia.journals.ac.za/pub/article/download/19/51>; Committee to Protect Journalists, "Sweeping Surveillance Law to Target 'Imperialist-Sponsored Journalists,'" press release, August 9, 2007, <http://allafrica.com/stories/200708090943.html>; Barbara Borst, "African Journalists Struggle to Find their Role in Building Democracies," *Perspectives on Global Issues*, Volume 2, Issue 2, spring 2008, <http://www.perspectivesonglobalissues.com/0301/borst.htm>.

³² Everson Mushava, "Technology a Security Threat: Sekeremayi," *Newsday*, May 9, 2013, <http://www.newsday.co.zw/2013/05/09/technology-a-security-threat/>.

³³ Tawanda Majoni, "ZANU PF Resolves to Jam Private Radio Stations," *Nehanda Radio*, December 11, 2012, <http://nehandaradio.com/2012/12/11/zanu-pf-resolves-to-jam-private-radio-stations/>.

³⁴ Everson Mushava, "Shamu Attacked over Internet Control," *Newsday*, December 20, 2012, <http://www.newsday.co.zw/2012/12/20/shamu-attacked-over-internet-control/>.

³⁵ Zimbabwe All Media Products Survey, Research International Bureau, Harare September, Third Quarter Report, 2012.

³⁶ The Newsday's Facebook page, <http://www.facebook.com/pages/NewsDay-Zimbabwe/215170571826981> and ZiFM's Twitter account, <https://twitter.com/ZiFMStereo>.

Independent news websites and other digital media outlets based overseas have emerged as an important source of alternative information for those able to access them. The websites of outlets such as *New Zimbabwe* and Nehanda Radio publish information often obtained from stringers or other contacts based inside Zimbabwe, at times generating news that is later picked up by mainstream media outlets. There is no concrete evidence of government manipulation of online content, though there is some concern over the quality of the news in online publications that often re-publish content from state-owned sources.

Civil society groups use social media platforms to support imprisoned political activists and human rights defenders by providing instant updates on the country's human rights situation and other political developments.³⁷ Radio stations such as Star and ZiFM are also increasingly using social media as a tool to facilitate listener feedback and participation in their programs. Meanwhile, Zimbabwean journalists, long divided across state-owned and independent media lines, have found space on social media platforms to discuss current affairs and share information, contacts, and tips on story ideas.³⁸ Nevertheless, the growing use of social media platforms has yet to manifest in concrete social, political, or economic change in Zimbabwe.

In March 2013, a self-proclaimed disaffected ZANU-PF member created a Facebook page under the moniker Baba Jukwa, which had drawn a following of over 300,000 Facebook users (compared to the 100,000 followers both Mugabe and Tsvangirai have each) by July 2013. Characterizing himself as a "Concerned father, fighting nepotism and directly linking community with their Leaders, Government, MPs, and Ministers,"³⁹ Baba Jukwa quickly became a social media sensation for daily posts that named and shamed politicians for alleged corruption and informed on the ruling party's supposed secrets. Most notably, the anonymous informant was credited with predicting the death of a ZANU-PF member of parliament, Edward Chindori Chininga, who died in a suspicious car accident in June 2013, nine days after Chininga had released a report on widespread corruption in the country's diamond mines.⁴⁰ Threatened by the Facebook page's growing influence, Mugabe reportedly offered a \$300,000 reward for Baba Jukwa's identity.⁴¹ While the whistleblower's efforts on Facebook have yet to affect concrete change on the country's political and social reality, Baba Jukwa's popularity has been described as representing "the Zimbabwean people's growing appetite for information and transparency, which will only be fuelled by increasing access to information technology."⁴²

³⁷ "Free Cynthia Manjoro and 23 Other Glen View Residents NOW!" Facebook group, <http://www.facebook.com/groups/212089078834518/?fref=ts>; Crisis Coalition Twitter page, <https://twitter.com/crisiscoalition>.

³⁸ Newsroom Lingo's Facebook page that brings Zimbabwe journalists from state and independent media, <http://www.facebook.com/groups/390978400932282/?fref=ts>.

³⁹ Baba Jukwa's Facebook page, accessed July 31, 2013, <https://www.facebook.com/pages/Baba-Jukwa/232224626922797>.

⁴⁰ "The Spirit of Wrath is Upon Us," *Economist*, June 19, 2013, <http://www.economist.com/news/middle-east-and-africa/21580163-mysterious-facebook-character-predicting-murder-and-mayhem-spirit>.

⁴¹ Mary Ann Jolley, "Mugabe Offers \$300,00 for Outing of Anonymous Whistleblower Baba Jukwa," ABC News, July 17, 2013, <http://www.abc.net.au/news/2013-07-17/mugabe-offers-243002c000-for-outing-of-anonymous-whistleblower/4824498>.

⁴² Rebecca Regan-Sachs, "Baba Jukwa vs. Mugabe – the Man On Facebook Standing Up to Zimbabwe's President," Think Africa Press via *All Africa*, July 24, 2013, <http://allafrica.com/stories/201307241382.html?viewall=1>.

VIOLATIONS OF USER RIGHTS

A new constitution came into force in May 2013 that included provisions for freedom of expression and of the press. Nevertheless, legal restrictions that contradicted the new constitutional guarantees remained in place and were frequently used against journalists, particularly for violations in the traditional media in the lead-up to the July 2013 general elections. Two mobile phone users were arrested during the coverage period for sending text messages that allegedly insulted the president. An investigative report in early 2013 uncovered evidence of a “massive” cyber training program for Zimbabwean security agents facilitated by Iranian intelligence organizations.

In 2013, Zimbabwe adopted a new constitution that was approved by parliament in May and signed into law by the president shortly thereafter.⁴³ Sections 60, 61, and 62 of the constitution guarantees freedom of expression, press freedom, access to information, protection of sources of information as well as the editorial independence of state-owned media. While these provisions are focused on the traditional media, it is expected that the new rights will also extend online. Accordingly, online journalists, bloggers, and citizens using social media platforms to share information can potentially seek protection under the new constitution.

Nevertheless, there are no laws that specifically protect online modes of communication, and bloggers are not recognized as eligible for accreditation as journalists. While the judiciary has sometimes demonstrated a degree of autonomy through rulings that are not necessarily favorable to the state, some in freedom of expression cases, the government often ignores such decisions. An appointment process that allows for high levels of executive interference further compromises judicial independence.

Meanwhile, the country’s civil and criminal defamation laws, the Interception of Communications Act of 2007, and the Criminal Law Codification and Reform Act (CODE) remain on the books and apply equally to reporters in the traditional media and online. The CODE punishes anyone who publicly undermines the authority of the president or insults him in any printed or electronic medium with a sentence of up to 20 years in prison.⁴⁴ In addition, Zimbabwe maintains restrictive access to information and media laws, which include the Access to Information and Protection of Privacy Act, the Criminal Codification Act, the Public Order and Security Act, and the Officials Secrets Act, among others. Combined with the extrajudicial actions of both state and non-state actors, these laws severely limit Zimbabweans’ ability to access and share information.⁴⁵

Since the signing of the Global Political Agreement at the end of 2008 that brokered a power-sharing deal between Robert Mugabe and Morgan Tsvangirai, violations against journalists have decreased significantly, though the improvement has not entailed a change in the dominant political

⁴³ Cris Chinaka, “Mugabe Signs Zimbabwe Constitution, Paving Way for Vote,” Reuters, May 22, 2013, <http://www.reuters.com/article/2013/05/22/us-zimbabwe-constitution-idUSBRE94L0RT20130522>.

⁴⁴ Criminal Law (Codification and Reform) Act [Chapter 9:23], Act 23/2004, Government Gazette, June 3, 2005, http://www.kubatana.net/docs/legisl/criminal_law_code_050603.pdf.

⁴⁵ Constitution of Zimbabwe, <http://www.gta.gov.zw/index.php/documents/constitution-of-zimbabwe>.

elite's attitude against the independent media. Arrests,⁴⁶ verbal attacks, and harassment against traditional media journalists, including expulsion from press conferences, still continue.⁴⁷

Penalties for online activities, however, have been less common. In one recent case, a South African-based Zimbabwean man, Benias Madhakasi, was thrown in police custody in April 2012 and held for three months for insulting the president after it was discovered that he had an image and inscription on his mobile phone that read, "Happy 87th Birthday (Operation Matibili)," referring to the president's nickname. The prosecutor opposed bail until the High Court threw out the charges in July 2012.⁴⁸ In a second case, Bulawayo resident Shantel Rusike was arrested on December 24, 2012 and held for four days after she was reported to the police for sending an image depicting President Mugabe in a nude state via WhatsApp on her mobile phone.⁴⁹ Rusike, out on \$100 bail, faces charges of "causing hatred, contempt or ridicule of the president," as delineated in the CODE.⁵⁰ As of mid-2013, her case was still before the courts.

Website owners, bloggers, and internet users are not required to register with the government, though mobile phone users must register their SIM cards by submitting personal identity details to the mobile operator, ostensibly to combat crime and curtail threatening or obscene communications.⁵¹ POTRAZ reported that approximately two million subscribers were disconnected in mid-2011 as a result of non-compliance,⁵² though the number of registered mobile telephone users increased thereafter.

Meanwhile, POTRAZ has maintained a September 2011 ban—reportedly enacted for security reasons—on the use of the BlackBerry messenger service that enables users to send free messages.⁵³ The ban went into effect in response to unfounded fears that the service had facilitated the 2011 Arab uprisings as well as the violent protests that took place in England in August of the same year.⁵⁴ In mid-2011, POTRAZ director general Charles Manzi Sibanda announced that the regulator was examining the compliance of BlackBerry's encryption technology with the Interception of Communications Act, which requires that all telecommunication services allow

⁴⁶ "Police Charge Zimind Editor, Reporter," *Newsday*, May 8, 2013, <http://www.newsday.co.zw/2013/05/08/police-charge-zimind-editor-reporter/>.

⁴⁷ Ndakaziva Majaka, "Mudede gags Media," *Daily News*, accessed 7 January 2013, <http://www.dailynews.co.zw/mobi/article/News/7ae212a6-d66b-490c-927d-a75af2da46ce>.

⁴⁸ "Court Frees Man Found with 'Nude' Mugabe Pictures," *Nehanda Radio*, July 25, 2012, <http://nehandaradio.com/2012/07/25/court-frees-man-found-with-nude-mugabe-pictures/>.

⁴⁹ Alex Bell, "'Naked' Mugabe Picture Lands Woman in Court," *Nehanda Radio*, January 9, 2013, <http://nehandaradio.com/2013/01/09/naked-mugabe-picture-lands-woman-in-court/>.

⁵⁰ Section 33(2)(a)(ii) of the Criminal Law (Codification and Reform) Act/CODE Chapter 9:23.

⁵¹ "POTRAZ Issues Mobile Phone Registration Reminder," *Technology Zimbabwe*, January 31, 2011, <http://www.techzim.co.zw/2011/01/potraz-registration-reminder/>.

⁵² Tawanda Musarurwa, "Zimbabwe: Tele-Density Rate takes Dip," *The Herald via AllAfrica*, May 10, 2011, <http://allafrica.com/stories/201105110010.html>, cited in L.S.M Kabweza, "ICT Policy and New Media Cultures in Southern Africa – Zimbabwe Report, Internal report for the Department of Media Studies" (South Africa: University of the Witwatersrand, 2011).

⁵³ BlackBerry formerly operated as Research in Motion. "BlackBerry Messenger a Dream," *The Zimbabwean*, June 5, 2012, <http://www.thezimbabwean.co.uk/technology/58636/blackberry-messenger-a-dream.html>.

⁵⁴ "Mugabe Vetoes Blackberry Service," *The Zimbabwean*, September 28, 2011, <http://www.thezimbabwean.co.uk/news/zimbabwe/53208/mugabe-vetoes-blackberry.html>.

official interception.⁵⁵ The POTRAZ decision was still outstanding as of October 2012.⁵⁶ Other encrypted communication applications, such as Skype, remain accessible.

The Post and Telecommunications Act of 2000 allows the government to monitor communications, including e-mail, and requires ISPs to supply information to government officials upon request.⁵⁷ The act also obligates ISPs to report any e-mail with “offensive” or “threatening” content. Meanwhile, the Interception of Communications Act of 2007 established a Monitoring of Interception of Communications Center with the powers to oversee traffic in all telecommunications services and to intercept phone calls, e-mails, and faxes under the pretext of national security.⁵⁸ The Act further requires telecommunications operators and ISPs to install necessary surveillance technology at their own expense and to intercept information on the state’s behalf.⁵⁹ Failure to comply is punishable with a fine and sentence of up to three years in prison.

Warrants allowing the monitoring and interception of communications are issued by the minister of information at his discretion; consequently, there is no substantial judicial oversight or other independent safeguard against abuse. The extent and frequency of monitoring therefore remains uncertain. There are also reports that the Central Intelligence Organization monitors all networks connected to the IP world’s routing system through the Interception of Communications Unit, which is administered by a top ZANU-PF politician.⁶⁰

Following the passage of the ICA in 2007, there were unconfirmed reports that Zimbabwe’s government had received surveillance technology and training from China,⁶¹ and suspicions of Chinese technical assistance in controlling ICTs remain strong.⁶² More recently in March 2013, the news and internet radio station, Nehanda Radio, reported that it had confirmed a “massive” cyber training program that had begun in 2007 with assistance from Iranian intelligence organizations.⁶³ According to the report, personnel from the Zimbabwean armed forces and the CIO have been undergoing intensive cyber training in “technological warfare techniques, counter-intelligence and methods of suppressing popular revolts among others, every six months.”

⁵⁵ Section 12 (1) (a) of the Act reads: “Notwithstanding any other law, a telecommunication service provider shall provide a telecommunication service which has the capacity to be intercepted.”

⁵⁶ BlackBerry Zimbabwe’s Facebook post, October 14, 2012, <https://www.facebook.com/BlackBerry.Zimbabwe>.

⁵⁷ Postal and Telecommunications Act, http://www.potraz.gov.zw/files/Postal_Act.pdf.

⁵⁸ Reporters Without Borders, “All Communications Can Now be Intercepted Under New Law Signed by Mugabe,” news release, August 6, 2007, http://en.rsf.org/zimbabwe-all-communications-can-now-be-06-08-2007_17623.html. The law is available at *Kubatana*, http://kubatana.net/docs/legisl/icb_070508.pdf.

⁵⁹ Nqobizitha Khumalo, “Zim Internet Service Providers Struggle to Buy Spying Equipment,” *ZimOnline*, August 10, 2007, http://www.kubatana.net/html/archive/inftec/070810zol1.asp?spec_code=060426commdex§or=INFTEC&year=0&range_start=1&intMainYear=0&intTodayYear=2010.

⁶⁰ “Mugabe Vetoes BlackBerry Service,” *The Zimbabwean*, September 28, 2011, <http://www.thezimbabwean.co.uk/news/zimbabwe/53208/mugabe-vetoes-blackberry.html>.

⁶¹ Lance Guma, “Too Much to Monitor for Snooping Squads,” *SW Radio Africa*, August 7, 2007, <http://www.swradioafrica.com/news070807/snoop070807.htm>; Reporters Without Borders, “All Communications Can Now Be Intercepted under New Law Signed by Mugabe,” news release, August 6, 2007; “Zimbabwe’s bugging bill condemned,” *BBC News*, June 15, 2007, <http://news.bbc.co.uk/2/hi/africa/6755753.stm>.

⁶² Amber Will, “Peeking Behind the Curtain: Analyzing Chinese Aid and Influence in Zimbabwe,” *The First Tranche* (blog), AidData, July 30, 2013, <http://blog.aiddata.org/2013/07/updated-peeking-behind-curtain.html>.

⁶³ Itai Mushekwe, “Iran Helping Zimbabwe Snoop on Internet,” *Nehanda Radio*, March 27, 2013, <http://bit.ly/YKatMQ>.

There have been no reported cases of attacks against bloggers and online journalists, despite concerns over potential violence and unrest surrounding the 2013 elections in July and its aftermath. In the first half of 2013, there was an explosion of political content on social media platforms, with bold and unrestrained political discussions taking place, such as on the Facebook page of the anonymous informant, Baba Jukwa (see “Limits on Content”).⁶⁴ These activities, particularly those linked to the July 2013 elections, have purportedly alarmed the security and political sector, and reports indicate that the ruling party and its security agencies are increasingly focusing on attacking and uncovering the identities of anonymous social media activists.⁶⁵ What technology the Zimbabwean authorities do have to monitor internet users has nonetheless failed to expose the true identity of Baba Jukwa,⁶⁶ though the whistleblower’s Facebook and Twitter accounts have reportedly been subject to several hacking attacks, resulting in the deletion of some of Jukwa’s damaging posts.⁶⁷

The government has reportedly used Chinese assistance to hack into websites of independent newspapers, although this also cannot be confirmed. In December 2011, for example, the website of the *Daily News*, one of Zimbabwe’s private newspapers, experienced a series of attacks on its website, which the *Daily News*’s information technology department blamed on Chinese hackers working in conjunction with the Zimbabwean authorities.⁶⁸ Meanwhile, government websites are increasingly the target of hacking attacks, with the website of the Ministry of Mines most recently hacked in March 2013.

⁶⁴ Everson Mushava, “Baba Jukwa distresses ZANU PF,” *Newsday*, April 30, 2013, <http://www.newsday.co.zw/2013/04/30/baba-jukwa-distresses-zanu-pf/>.

⁶⁵ “Baba Jukwa: Legion of Malicious Engagement,” *The Herald* via *All Africa*, May 14, 2013, <http://allafrica.com/stories/201305140292.html>.

⁶⁶ “Should Africa Be Worried About Chinese Cyber-Espionage?” ICT Africa, June 2, 2013, <http://ictafrica.info/FullNews.php?id=9480>.

⁶⁷ “Julian Assange, Baba Jukwa and Cyberpunks,” ICT Africa, May 4, 2013, <http://ictafrica.info/FullNews.php?id=9002>.

⁶⁸ “Chinese Cyber Spooks Intensify Zimbabwe Media Attacks, The Zimbabwe Mail targeted,” *The Zimbabwe Mail*, December 30, 2011, https://groups.google.com/forum/#!topic/InfoAccessNow/PD-F_uU-5Uk.