REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
HCCHRPET/ 276 /2025

INTERNATIONAL COMMISSION OF JURISTS
KENYA SECTION (ICJ KENYA) .....1ST PETITIONER
BLOGGERS ASSOCIATION OF KENYA (BAKE).....2ND PETITIONER
KENYA UNION OF JOURNALISTS (KUJ).....3RD PETITIONER
COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA (CIPESA).....4TH PETITIONER

AND

COMMUNICATIONS AUTHORITY OF KENYA (CA).....1ST RESPONDENT
ATTORNEY GENERAL.....2ND RESPONDENT
CABINET SECRETARY INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY.....3RD RESPONDENT
SAFARICOM LTD.....4TH RESPONDENT
AIRTEL KENYA LTD.....5TH RESPONDENT
PARADIGM INITIATIVE (PIN).....1ST INTERESTED PARTY
LAW SOCIETY OF KENYA.....2ND INTERESTED PARTY
KATIBA INSTITUTE.....3RD INTERESTED PARTY

CERTIFICATE OF URGENCY

I Ochiel Dudley, Advocate, certify this matter urgent because:

1. The internet enables the enjoyment of rights and freedoms while enhancing transparency and accountability in public and private spheres. Therefore, internet shutdowns are powerful markers of sharply deteriorating human rights situations. Internet shutdowns also have major economic costs for all sectors, disrupting for example financial transactions, commerce and industry.
2. Yet, in Kenya, internet freedom is increasingly imperilled by emerging digital authoritarianism. First, Respondents have, during the 2023 and 2024 national examinations routinely shut down Telegram. Then, on 25 June 2024, during the **#RejectFinanceBill** protests, the Respondents illegally shut down the internet. The June shutdown coincided with an unprecedented attack on fundamental rights and freedoms in which nearly 60 Kenyans were killed by state agents.
3. Fearing repeat internet shutdown including during the 2027 General Elections, exams or protests, Petitioners file this case. Petitioners seek appropriate reliefs for the 25 June 2024 shutdown and aim to deter future violations. The matter is urgent because of the **harmful effect of internet shutdowns** on human rights, the economy and democracy.

Dated at Nairobi on 13 May 2025

OchielJD
Bond Advocates LLP
Advocates for the Petitioners

Drawn and filed by:
Bond Advocates LLP
Top Plaza, 2nd Floor,
Kindaruma Road
P. O. Box 37551-00100 Nairobi
0112318576
bond@bondadvocates.com
ochieljd@bondadvocates.com

REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
HCCHRPET/ 276 /2025

INTERNATIONAL COMMISSION OF JURISTS
KENYA SECTION (ICJ KENYA) .....1ST PETITIONER
BLOGGERS ASSOCIATION OF KENYA (BAKE).....2ND PETITIONER
KENYA UNION OF JOURNALISTS (KUJ).....3RD PETITIONER
COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA (CIPESA).....4TH PETITIONER

AND

COMMUNICATIONS AUTHORITY OF KENYA (CA).....1ST RESPONDENT
ATTORNEY GENERAL.....2ND RESPONDENT
CABINET SECRETARY INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY.....3RD RESPONDENT
SAFARICOM LTD.....4TH RESPONDENT
AIRTEL KENYA LTD.....5TH RESPONDENT
PARADIGM INITIATIVE (PIN).....1ST INTERESTED PARTY
LAW SOCIETY OF KENYA.....2ND INTERESTED PARTY
KATIBA INSTITUTE.....3RD INTERESTED PARTY

NOTICE OF MOTION

Take notice that this court will be moved on the day of 2025 at 9:00am or per the cause list for hearing of the petitioners' application for orders that:

a) This application is certified urgent.
b) Pending hearing of this application inter partes, a conservatory order does issue, prohibiting the Respondents and their agents from unlawfully directing, enforcing, or implementing any internet shutdown in Kenya during protests, exams, elections, or other civic action.
c) Pending hearing and determination of the Petition a conservatory order does issue, prohibiting the Respondents and their agents from unlawfully directing, enforcing, or implementing any internet shutdown in Kenya during protests, exams, elections, or other civic action.

Which application is based on the affidavit of Eric Mukoya and on the grounds:

1. The internet enables the enjoyment of rights and freedoms while enhancing transparency and accountability in public and private spheres. Therefore, internet shutdowns are powerful markers of sharply

deteriorating human rights situations. Internet shutdowns also have major economic costs for all sectors, disrupting for example financial transactions, commerce and industry.

2. Yet, in Kenya, internet freedom is increasingly imperilled by emerging digital authoritarianism.
3. First, Respondents have, during the 2023 and 2024 national examinations routinely shut down Telegram. Then, on 25 June 2024, during the **#RejectFinanceBill** protests, the Respondents illegally shut down the internet. The June shutdown coincided with an unprecedented attack on fundamental rights and freedoms in which nearly 60 Kenyans were killed by state agents.
4. No law or court order sanctioned the June 2024 internet shutdown or the 2023 and 2024 suspension of Telegram. However, the June 2024 internet shutdown lasted several days causing daily GDP losses of $6.3 million and disproportionately affecting small businesses and women.
5. Fearing repeat internet shutdown including during the 2027 General Elections, exams or protests, Petitioners file this case. Petitioners seek appropriate reliefs for the 25 June 2024 shutdown and aim to deter future violations.
6. The matter is urgent because of the **harmful effect of internet shutdowns** on human rights, the economy and democracy.

Dated at Nairobi on 13 May 2025

OchielJD

Bond Advocates LLP
For the Petitioners

Drawn and filed by:
Bond Advocates LLP
Top Plaza, 2nd Floor, Kindaruma Road
P.O. Box 37551-00100 Nairobi,
0112318576
bond@bondadvocates.com
ochieljd@bondadvocates.com

REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
HCCHRPET/ 276 /2025

KENYA SECTION OF THE INTERNATIONAL COMMISSION OF JURISTS (ICJ KENYA) .....1ST PETITIONER
BLOGGERS ASSOCIATION OF KENYA (BAKE).....2ND PETITIONER
KENYA UNION OF JOURNALISTS (KUJ).....3RD PETITIONER
COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA (CIPESA).....4TH PETITIONER

AND

COMMUNICATIONS AUTHORITY OF KENYA (CA).....1ST RESPONDENT
ATTORNEY GENERAL.....2ND RESPONDENT
CABINET SECRETARY INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY.....3RD RESPONDENT
SAFARICOM LTD.....4TH RESPONDENT
AIRTEL KENYA LTD.....5TH RESPONDENT
PARADIGM INITIATIVE (PIN).....1ST INTERESTED PARTY
LAW SOCIETY OF KENYA.....2ND INTERESTED PARTY
KATIBA INSTITUTE.....3RD INTERESTED PARTY

PETITION

A. INTRODUCTION

1. The internet enables the enjoyment of rights and freedoms while enhancing transparency and accountability in public and private spheres. Therefore, internet shutdowns are markers of deteriorating human rights situations. Internet shutdowns also have major economic costs for all sectors, disrupting for example financial transactions, commerce and industry. Economic shocks of shutdowns are felt over long periods, greatly exacerbating pre-existing social and economic inequalities.
2. Yet, in Kenya, internet freedom is increasingly imperilled by emerging digital authoritarianism. First, Respondents have, during the 2023 and 2024 national examinations routinely shut down Telegram. Then, on 25 June 2024, during the **#RejectFinanceBill** protests, the Respondents illegally shut down the internet. The June shutdown coincided with an unprecedented attack on fundamental rights and freedoms in which nearly 60 Kenyans were killed by state agents.

3. Fearing repeat internet shutdown including during the 2027 General Elections, exams or protests, Petitioners file this case. Petitioners seek appropriate reliefs for the 25 June 2024 shutdown and aim to deter future violations. The matter is urgent because of the **harmful effect of internet shutdowns** on human rights, the economy and democracy.

B. PARTIES

(i) Petitioners

4. Founded in 1952, the Kenyan Section of the International Commission of Jurists-Kenya (ICJ Kenya), the First Petitioner, is an international, non-partisan, and non-profit registered professional society with long-established and well-recognised expertise in the rule of law.
5. The, Second Petitioner, Bloggers Association of Kenya (BAKE) is a community organisation representing Kenyan online content creators. BAKE seeks to empower online content creation and improve the quality of web content in Kenya.
6. Kenya Union of Journalists, the Third Petitioner, is a professional organisation dedicated to improving the working conditions of journalists in Kenya. KUJ focuses on protecting and promoting media freedom, professionalism and ethical standards within the media industry.
7. Collaboration on International ICT Policy For East and Southern Africa (CIPESA), Fourth Petitioner, is a network of collaborators working to promote effective and inclusive ICT policy and practice for improved governance, livelihoods, and human rights in Africa.

(ii) Respondents

8. The Communication Authority of Kenya (CA), the First Respondent, is a regulatory authority responsible for the information and communications sectors under the Kenya Information and Communications Act, Cap 411A. CA is sued for directing internet shutdowns contrary to its mandate under

83c(1)(g) section of KICA to promote and facilitate the efficient management of critical internet resources.

9. The Second Respondent is the Attorney General whose office is established under Article 156 of the Constitution of Kenya. The AG represents the national government in legal proceedings.
10. The Third Respondent is the Cabinet Secretary for Information, Communications and the Digital Economy responsible for the impugned decision.
11. Safaricom and Airtel are Kenyan network providers sued for acting on the unconstitutional directives of the First to Third Respondents to effect the unjustified, deliberate and illegal disruption of Internet access.

(iii) Interested Parties

12. Paradigm Initiative (PIN), the First Interested Party, is a pan-African non-profit organisation which advocates for an Internet that is open, accessible, and affordable to all.
13. Law Society of Kenya (LSK) the Second Interested Party, is Kenya's premier bar association. LSK is mandated by the Law Society of Kenya Act, 2014, to uphold the Constitution of Kenya and to assist the courts and protect the public in legal matters.
14. Katiba Institute, the Third Interested Party, is a constitutional research, policy, and litigation institute formed to further the implementation of Kenya's 2010 Constitution.

C. FOUNDING FACTS

15. In Kenya, internet freedom is increasingly imperilled by emerging digital authoritarianism.
16. First, Respondents suspended Telegram during the 2023 and 2024 national examinations. Then, on 25 June 2024, during the **#RejectFinanceBill** protests, the Respondents illegally shut down the internet. The June 2024 internet shutdown coincided with an

unprecedented attack on fundamental rights and freedoms in which nearly 60 Kenyans were killed by state agents.

17. No law or court order sanctioned the June 2024 internet shutdown or the 2023 and 2024 suspension of Telegram. Even so, the June 2024 internet shutdown lasted several days causing daily GDP losses of $6.3 million and disproportionately affecting small businesses and women.

18. Fearing repeat internet shutdown including during the 2027 General Elections, during exams, or in protests, Petitioners file this case. Petitioners seek appropriate reliefs for the 25 June 2024 internet shutdown and the 2023 and 2024 exam-time suspension of Telegram. They aim to deter future violations.

D. LEGAL GROUNDING

(a) Constitution of Kenya 2010

19. The preamble to the Constitution of Kenya 2010 recalls Kenyans' aspiration for a government based on the essential values of human rights, democracy and the rule of law.

20. Article 2(1) of the Constitution proclaims the supremacy of the Constitution declaring it the supreme law of the Republic that binds all persons and all state organs at both levels of the government.

21. Under Article 2(4) of the Constitution any law, any act or omission in contravention of the Constitution is invalid. Under Article 2(6) treaties ratified by Kenya form part of the laws of Kenya.

22. Article 3 of the Constitution subjects the Respondents like all Kenyans and State organs to the requirement to respect, uphold and defend the Constitution.

23. The national values and principles of governance in Article 10 bind all State organs, State officers, public officers, and all persons whenever any of them applies or interprets the Constitution or enacts, applies, or interprets any law. The national values and principles of governance

relevant to this petition include the rule of law, social justice, democracy, public participation, and human rights.

24. The Bill of Rights under Article 19(3)(b) does not exclude other rights and fundamental freedoms not in the Bill of Rights, but recognised or conferred by law.

25. Article 22 (1) and (2) and 258(1) and (2) of the Constitution entitle the Petitioners to institute these court proceedings claiming that rights or fundamental freedom in the Bill of Rights and the Constitution itself is violated, or infringed, or threatened.

26. Article 20(1) of the Constitution provides that the Bill of Rights applies to all law and binds all State organs and all persons while Article 20(2) of the Constitution provides that every person will enjoy the rights and fundamental freedoms in the Bill of Rights to the greatest extent consistent with the nature of the right or fundamental freedom.

27. Article 21(1) of the Constitution provides that it is a fundamental duty of the State and every State organ to observe, respect, protect, promote and fulfil the rights and fundamental freedoms in the Bill of Rights.

28. Article 20(3) of the Constitution provides that in applying a provision of the Bill of Rights, a court shall (a) develop the law so much so that it does not give effect to a right or fundamental freedom; and (b) adopt the interpretation that most favors the enforcement of a right or fundamental freedom.

29. Article 23 (1) of the Constitution vests jurisdiction on this Court, in under Article 165, to hear and determine applications for redress of a denial, violation or infringement of, or threat to, a right or fundamental freedom in the Bill of Rights as sought in the present proceedings. Article 23(3) allows the court to grant the orders sought in these proceedings.

30. Article 24 of the Constitution provides in part that a right or fundamental freedom cannot be limited except by law, for a legitimate aim, and proportionately. A limitation is therefore justifiable only if it meets the

three-part test of being: by law; pursuing a legitimate purpose; and the least restrictive measure.

31. Under Article 32, every person has the right to freedom of conscience, thought, belief, and opinion extending to the expression of beliefs and opinions online.

32. Article 33 guarantees every person the right to freedom of expression, which includes: freedom to seek, **receive or impart information or ideas**; freedom of artistic creativity; and academic freedom and **freedom of scientific research.**

33. Article 34 of the constitution guarantees freedom and independence of electronic, print and all other types of media. The State shall not exercise control over or interfere with any person engaged in broadcasting, the production or circulation of any publication or the dissemination of information by any medium; or penalise any person for any opinion or view or the content of any broadcast, publication or dissemination. Broadcasting and other electronic media have freedom of establishment, subject only to licensing procedures that are necessary to regulate the airwaves and other forms of signal distribution; and are independent of control by government, political interests or commercial interests. All State-owned media shall—be free to determine independently the editorial content of their broadcasts or other communications; be impartial; and afford fair opportunity for the presentation of divergent views and dissenting opinions. Parliament shall enact legislation that provides for the establishment of a body, which shall—be independent of control by government, political interests or commercial interests; reflect the interests of all sections of the society; and set media standards and regulate and monitor compliance with those standards.

34. Article 35 of the Constitution provides that every citizen has the right of access to information held by the state and information held by another person and required for the exercise or protection of any right or

fundamental freedom. The State must publish and publicise any important information affecting the nation.

35. Every person has the right, under Article 36, to freedom of association, which includes the right to form, join or participate in the activities of an association of any kind.

36. Under Article 37 every person has the right, peaceably and unarmed, to assemble, to demonstrate, to picket, and to present petitions to public authorities.

37. Article 38 frees every citizen to make political choices, which includes the right, including online, to: (a) form, or participate in forming, a political party; (b) to participate in the activities of, or recruit members for, a political party; or (c) to campaign for a political party or cause.

38. Article 46 gives consumers the right: to goods and services of reasonable quality; the information necessary for them to gain full benefit from goods and services;(c)to the protection of their health, safety, and economic interests; and compensation for loss or injury arising from defects in goods or services.

(b) International Law and Instruments

i. African Charter on Human and People's Rights

39. Article 2 of the Banjul Charter entitles every individual to enjoy the rights and freedoms recognised and guaranteed in the Charter without distinction of any kind such as race, ethnic group, color, sex, language, religion, political or any other opinion, national and social origin, fortune, birth, or other status.

40. Article 9 of the Banjul Charter entitles individuals to receive information and to express and disseminate their opinion within the law.

ii. International Covenant on Civil and Political Rights

41. Article 2(1) of the ICCPR obligates states to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights

recognized in the Covenant. Under Article 2(3)(a) to (c) of the ICCPR, state parties must afford effective remedy to any person whose rights or freedoms in the ICCPR are violated, notwithstanding that the violation has been committed by persons acting in an official capacity.

42. Article 19(1) and (2), everyone has the right to hold opinions without interference. Everyone has the right to freedom of expression; this right includes freedom **to seek, receive, and impart information and ideas of all kinds**, **regardless of frontiers,** either orally, in writing or in print, in the form of art, or **through any other media of their choice**.

iii. General Comment No. 34: Article 19 ICCPR on the Freedoms of Opinion and Expression

43. The General Comment in para 1 explains that freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society. They constitute the foundation stone for every free and democratic society. The two freedoms are closely related, with freedom of expression providing the vehicle for the exchange and development of opinions. In that regard, freedom of expression is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights.

44. Further, para 11 explains that states parties must guarantee the right to freedom of expression, including the **right to seek, receive and impart information and ideas of all kinds regardless of frontiers**. This right includes the expression and receipt of communications of **every form of idea and opinion capable of transmission to others**. It includes political discourse, commentary on one's own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse. It may also include commercial advertising.

45. The entitlement protects **all forms of expression and the means of their dissemination**. Such forms include spoken, written, and sign

language and nonverbal expressions such as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress, and legal submissions. They include all forms of audiovisual as well as electronic and **internet-based modes of expression**.

46. Para 15 indicates:

> States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.

47. Para 43 explains that any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are permissible only if they are compatible with Article 19(3) of the ICCPR. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible Article 19(3) of the ICCPR. It is also inconsistent with article (19)3 to prohibit a site or an information dissemination system from publishing material solely because it may be critical of the government or the political social system espoused by the government.

iv. ACHPR Declaration on Freedom of Expression and Access to Information in Africa, 2020

48. The ACHPR Declaration on Freedom of Expression and Access to Information in Africa, 2020, which establishes or affirms the principles for anchoring the rights to freedom of expression and access to information

under Article 9 of the African Charter guaranteeing the right to receive information and the right to express and disseminate information.

49. Principle 37 on access to the internet obligates states to facilitate the rights to freedom of expression and access to information online and the means necessary to exercise the rights. The principle further requires states to recognise that universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information, and the exercise of other human rights.

50. Principle 38 on non-interference stipulates:

> 1. States shall not interfere with the right of individuals to seek, receive and impart information through any means of communication and digital technologies, through measures such as the removal, blocking or filtering of content, unless such interference is justifiable and compatible with international human rights law and standards.
> 2. States shall not engage in or condone any disruption of access to the internet and other digital technologies for segments of the public or an entire population.
> 3. States shall only adopt economic measures, including taxes, levies and duties, on internet and information and communication technology service end-users that do not undermine universal, equitable, affordable and meaningful access to the internet and that are justifiable and compatible with international human rights law and standards.

51. Principle 39 on internet intermediaries compels states to require internet intermediaries enable access to all internet traffic equally without discrimination based on the type or origin of content or the means used to transmit content. Internet intermediaries must not interfere with the free flow of information by blocking or giving preference to particular internet traffic.

52. Nor shall States require the removal of online content by internet intermediaries unless such requests are:

a. clear and unambiguous;

b. imposed by an independent and impartial judicial authority, subject to sub-principle 5;

c. subject to due process safeguards;

d. justifiable and compatible with international human rights law and standards; and

e. implemented through a transparent process that allows a right of appeal.

v. Report of the Office of the United Nations High Commissioner for Human Rights - Internet shutdowns: trends, causes, legal Implications and impacts on a range of Human Rights

53. The report defines "internet shutdowns" as:

> measures taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online. They include actions that limit the ability of a large number of people to use online communications tools, either by restricting Internet connectivity at large or by obstructing the accessibility and usability of services that are necessary for interactive communications, such as social media and messaging services. Such shutdowns inevitably affect many users with legitimate pursuits, leading to enormous collateral damage beyond the scope of their intended purposes…

54. According to the report, shutdowns often include complete blocks of Internet connectivity or accessibility of the affected services. However, governments increasingly resort to throttling bandwidth or limiting mobile service to 2G, which, while nominally maintaining access, renders it extremely difficult to make meaningful use of the Internet. In particular, bandwidth throttling interferes with the ability to share and watch video footage and live streams.

55. Another way is limiting the availability of some websites and services, restricting access to certain communications channels while continuing to shutdown access to the rest of the internet. Some governments have also blocked the use of virtual private networks to prevent people from circumventing shutdown measures. In some cases, shutdowns of entire telephone networks accompany Internet shutdowns, leaving no channel of direct electronic communication.

56. Internet shutdowns can affect all Internet connections in a country or region, but are often limited to certain forms of Internet access, in particular mobile networks. In countries where the Internet is overwhelmingly accessed through mobile devices and broadband Internet is affordable only for the affluent, this may amount to a complete Internet blackout for the majority of the population. As technology develops, the modalities for disrupting access to, and the use of, online space will evolve, and the definition of shutdowns and responses to them must change as well.

57. The report notes that access to the Internet is widely recognised as an indispensable enabler of a broad range of human rights. It is not only essential for freedom of expression, but, as digitalization advances, it is also central to the realization of the rights to education, to freedom of association and assembly, to participate in social, cultural and political life, to health, to an adequate standard of living, to work and to social and economic development, to name just a few.

58. Further, given the positive obligation of States to promote and facilitate the enjoyment of human rights, States should take all steps necessary to ensure that all individuals have meaningful access to the Internet. On the same grounds, States should refrain from interfering with access to the Internet and digital communications platforms unless such interference is in full compliance with the requirements of the applicable human rights instruments.

59. While Internet shutdowns deeply affect many human rights, they most immediately affect freedom of expression and access to information – one of the foundations of free and democratic societies and an indispensable condition for the full development of the person. It is a touchstone for all other rights guaranteed in the International Covenant on Civil and Political Rights and other human rights instruments. Any restriction on freedom of expression constitutes a serious curtailment of human rights.

vi. The promotion, protection and enjoyment of human rights on the Internet : resolution / adopted by the Human Rights Council (2012)

60. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which applies regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Right.

vii. UN Guiding Principles on Business and Human Rights

61. Article 11 of the UN Guiding Principles on Business and Human Rights Business demand that enterprises should respect human rights and must avoid infringing on the human rights of others and address adverse human rights impacts with which they are involved.

62. Besides, under para 13, the responsibility to respect human rights requires that business enterprises: (a) avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; (b) seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

63. In turn, under para 14, the responsibility of business enterprises to respect human rights applies to all enterprises regardless of their size, sector, operational context, ownership and structure.

viii. Universal Declaration of Human Rights

64. Article 19 of the UDHR provides the right "to seek, receive, and impart information and ideas through any media and regardless of frontier". While the UDHR is not a legally binding document, it can be considered customary international law by its role as a global standard in international human rights law.

ix. Resolution on Internet Shutdowns and Elections in Africa - ACHPR.Res.580 (LXXVIII)2024

65. The Commission calls on State Parties to:

(i) Ensure compliance with the African Charter, the African Charter on Democracy, Elections and Good Governance and relevant regional and international human rights instruments during the electoral process;
(ii) Take the necessary legislative and other measures to ensure open and secure internet access before, during and after elections, including ensuring that telecommunications and internet service providers take adequate steps to provide unrestricted and uninterrupted access
(iii) Refrain from ordering the interruption of telecommunications services, shutting down the internet, and/or disrupting access to any other digital communication platforms before, during or after the elections;
(iv) Require telecommunications and internet service providers to inform users of potential disruptions and exercise due diligence to resolve any disruptions expeditiously.

x. Guidelines on Access to Information and Elections in Africa,

66. Article 26 of the Guidelines stipulates that "The body responsible for regulating the broadcasting media as well as other public or private bodies responsible for national security and associated with the provision of telecommunications services shall refrain from blocking access to the Internet or any other media during the electoral process.

xi. Joint Declaration on Freedom of Expression and the Internet

67. The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom jointly declared:

General Principles

a. Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognised under international law (the 'three-part' test).
b. When assessing the proportionality of a restriction on freedom of expression on the Internet, the impact of that restriction on the ability of the Internet to deliver positive freedom of expression outcomes must be weighed against its benefits in terms of protecting other interests.
c. Approaches to regulation developed for other means of communication – such as telephony or broadcasting – cannot simply be transferred to the Internet but, rather, need to be specifically designed for it.
d. Greater attention should be given to developing alternative, tailored approaches,

which are adapted to the unique characteristics of the Internet, for responding to illegal content, while recognising that no special content restrictions should be established for material disseminated over the Internet.

e. Self-regulation can be an effective tool in redressing harmful speech, and should be promoted.

f. Awareness raising and educational efforts to promote the ability of everyone to engage in autonomous, self-driven and responsible use of the Internet should be fostered ('Internet literacy).

68. On filtering and blocking, the joint declaration states that mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can be justified only in accordance with international standards, for example where necessary to protect children against sexual abuse.

69. On access to the internet the declaration indicates:

a. Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.

b. Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.

(c) Statutory Basis

i) Fair Administrative Actions Act, 2015

70. Section 4(1) of the Fair Administrative Action Act, 2015 guarantees every person the right to administrative action that is expeditious, efficient, lawful, reasonable and procedurally fair.

71. Section 2 of the Act defines "administrative action" as "powers, functions and duties exercised by authorities"; or "any act, omission or decision of any person, body or authority that affects the legal rights or interests of any person affected by the action".

72. Under section 7 of the Fair Administrative Action Act, 2015 this court is entitled to review administrative action where:

The administrator—

a. denied the person to whom the administrative action or decision relates, a reasonable opportunity to state the person's case

The administrative action:

a. did not comply with a mandatory and material procedure or condition prescribed by an empowering provision;
b. was materially influenced by an error of law;
c. Is unfair or procedurally unfair;
d. Is unreasonable or not informed by the reasons given for it.

73. In turn, Article 23 and section 11 of the FAA empower the present day judicial review courts to grant any order that is just and equitable, including an order: declaring the rights of the parties in respect of any matter to which the administrative action relates; prohibiting the administrator from acting in a particular manner; or compelling the performance by an administrator of a public duty owed in law and in respect of which the applicant has a legally enforceable right.

ii) Kenya Information and Communication Act, 2009

74. Section 83C(1)(g) of KICA directs CA to promote and facilitate the efficient management of critical internet resources.

E. PARTICULARS OF UNCONTITUTIONALITY

75. First, although there is no express right to the internet in Kenya's Constitution, the Bill of Rights under Article 19(3)(b) does not exclude other rights and fundamental freedoms not in the Bill of Rights but recognised or conferred by law. To that end, Article 20(3) of the Constitution tasks Kenyan court to develop the law to give effect to rights or fundamental freedoms and to adopt the interpretation that most favours the enforcement of right or fundamental freedom.

76. In that regard, Article 33 of the Constitution entitles one to seek, receive or impart information or ideas and freedom of scientific research including through the internet. Article 32 equally entitles one to express their opinion through the internet, while Article 34 and 35 equally guarantee the right of the media to disseminate, and the citizen to receive information through internet.

77. Therefore, internet shutdown and suspension of Telegram or other social media sites violates the right of access to the internet inherent in Kenya's Constitution.

78. In the alternative, even if internet access were not strictly a fundamental right, it is a "derivative right" that enhances the exercise of freedom of expression. As such, internet access is integral to the right to freedom of expression that requires protection by law and makes its violation actionable. Any interference with this right must therefore be reasonable and justifiable under Article 24 of the Constitution.

79. Further, violation of the right of access to the internet compounds other violations because access to the internet is an enabler of a broad range of human rights. It is not only essential for freedom of expression, but, as digitalization advances, it is also central to the realization of the rights to education, to freedom of association and assembly, to participate in social, cultural and political life, to health, to an adequate standard of

living, to work and to social and economic development, to name just a few.

80. Second, internet shutdown and suspension of Telegram or other social media sites violate Articles 32, 33, 34, 35, 36, 37, and 38 (on opinion, expression, media, information, association, assembly, and political rights).

81. In that regard, Article 9 of the Banjul Charter and Article 19 of the ICCPR guarantee the right to freedom of expression without interference. Article 19 of ICCPR creates a derivative right that allows a person to enjoy the right using whatever medium of choice. The rights under Articles 32, 33, 34, 35, 36, 37, and 38 could be enjoyed through several media, including social media platforms like Telegram, Twitter, Facebook, or Instagram. Access to Telegram is one a derivative right that is complimentary to the enjoyment of the right to freedom of expression under Article 9(1) & (2) of the Banjul Charter, Article 19 of the ICCPR, and Article 33 of the of the Constitution.

82. Third, Respondents failure to acknowledge the internet shutdowns or their decision to provide minimal or no explanation for the measures, including their legal basis and underlying grounds, violates Article 10 on openness and transparency. The opacity further violates Article 35(5), obligating the state to publish and publicise any important information affecting the nation. And for lacking reasons, the shutdowns violated Article 47 of the Constitution requiring *reasonable* administrative action.

83. Fourth, internet shutdown and the suspension of Telegram by the CA violates the rule of law under Article 10. The decision is ultra vires section 83C(1)(g) of the Kenya Information and Communication Act, 2009 requiring CA to promote and facilitate the efficient management of critical internet resources.

84. Fifth, internet shutdowns violate the right to associate, assemble, and to enjoy political rights under Article 36, 37, and 38 of the Constitution.

Shutdowns obscure the right to participate in the activities of associations, limit the freedom to assemble and to present petitions to public authorities, and impair the right to participate in the activities of, or recruit, or campaign for a political party or cause online.

85. Contrary to Article 37, blocking internet access during protests makes it harder for protesters to communicate and organise without the existence of formal organisations. Injured protestors cannot call for help or get medical attention. Besides, citizens are more likely to protest ill governance if they perceive that others are also willing to stand up against the challenge. protests, which now have both offline and online manifestations, cannot be carried out when access to the Internet is shut, which impacts on the right to freedom of assembly and association.

86. Sixth, internet shutdowns violate Article 46 by denying consumers of internet services and others generally the right to: goods and services of reasonable quality, information necessary for them to gain full benefit from goods and services, and protection of their health, safety, and economic interests.

87. Seventh, internet shutdowns threaten the right under Article 81 to free and fair elections. For example, mobile (smart) phones provide individuals with an efficient tool for monitoring electoral malpractice. Pictures and other pieces of information can instantly be shared with broader networks, documenting incidences of violence and enabling opposition actors to send assistance to affected polling stations. On the other hand, disrupting internet connection can prevent voters from effectively using ICT to challenge electoral malpractice, while obscuring the use of violent state repression. Iin turn, the government can commit violence without risking denunciation of their actions if Internet access is disrupted during elections. By banning access to widely used online platforms, governments hinder the opposition from documenting state violence and effectively challenging their use of coercive force.

88. Further, according to social movement theory, to become active in antiregime mobilization, citizens need to have a sense of the extent to which their grievances are shared with others. Voters are more likely to challenge electoral malpractice if they perceive the elections as fraudulent and if they know that others are also willing to stand up against it.

89. That said, voters in authoritarian regimes are often confronted with the problem of 'preference falsification'. Even if they secretly favour the opposition, for example, citizens may deny their preferences in public due to the threat of punishment and uncertainty about broader public opinion. So-called 'islands of separateness' – places in which people express and mobilise for their antiregime opinions – tend to be scarce in the authoritarian offline world. In the context of elections, citizens may lack information about the extent to which others share their disapproval of the regime and, hence, be reluctant to engage in mobilization challenging election malpractice. The alleged anonymity on the Internet can encourage individuals to share their 'true' preferences, especially in places where the public sphere is heavily restricted

90. Eighth, the internet plays a critical role in trade and commerce, and some businesses are completely dependent on the internet. In Kenya, every hour of total internet shutdown results in the country losing about Sh1.8 billion of its GDP, according to NetBlock's cost of internet shutdown calculator. The June 2024 internet shutdown lasted several days causing daily GDP losses of $6.3 million and disproportionately affecting small businesses and women.

91. Internet shutdown not only affect the country's financial stability but also have broader implications for businesses and individuals who rely on the internet for their livelihood violating the right to life and livelihood under Article 26 and 43. Given the increasing reliance of businesses and trade

on digital technologies, mandated disruptions of communications services have serious repercussions for all economic sectors.

92. Shutdowns may lead to the disruption of financial transactions, commerce, industry, labour markets and the availability of platforms for the delivery of services. Moreover, shutdowns create a climate of uncertainty for investment, which can prove disastrous for companies and for start-up ecosystems in particular. Economic shocks provoked by shutdowns are felt over long periods of time, greatly exacerbating pre-existing social economic inequalities contrary to Article 10 and 27 of the Constitution.

93. Again, on socio-economic rights, particularly of the youth reliant on technologies for finding and maintaining employment, internet shutdowns illegally and illegitimately restrict their enjoyment of the right to work under Article 41. The youth particularly use the internet as one of their primary modes of business, political participation, and for other legitimate purposes. Shutting Internet access therefore actively violates socio-economic rights under Article 43 including the right to education online, sexual and reproductive health, online and even access to online financial services

94. Ninth, under Article 43, essential services that provide education, health care and social assistance increasingly rely on digital tools and communications. Consequently, drastic disruptions or slowdowns of communications services negatively affect the enjoyment of economic, social and cultural rights, with immediate and long-term repercussions. Contrary to Article 43 and 53. Shutdowns' can undermine pedagogical outcomes and interfere with education planning and communication among teachers, school administrators and families. Restrictions on connectivity endangers the education of students relying on remote education, due to restricted access to pedagogical materials and online classes.

95. Equally, communication delays and impediments provoked by shutdowns also compromise the effectiveness of health-care and public health policies, with impacts that accumulate over time. Shutdowns, contrary to Article 43, have negative impact on health systems, including on mobilizing urgent medical care, disrupting the delivery of essential medicines and maintenance of equipment, limiting the exchange of health information between medical personnel and disrupting essential mental health assistance.

96. Shutdowns also undermine access for women and girls to critical support and protection, exacerbating the gender divide and violating Article 27. For example, shutdowns hamper access to emergency health support and to information for reproductive health under Article 43.

97. Tenth, the limitation of rights by the impugned internet shutdowns is neither reasonable nor justifiable under Article 24 of the Constitution. The shutdowns fail the three-part test cumulatively requiring any limitation to be: lawful, legitimate, and proportionate. No law permits Respondents to shut down the internet or to suspend Telegram or any social media site. Shutting down internet is a disproportionate action on part of the state, which has a damaging impact on economic activities and the livelihood of millions of citizens, and also denies access to the internet which facilitates various other rights including of communication, information, commerce and expression and speech.

F. RELIEFS

98. As a result, invoking Article 23 of the Constitution Petitioner prays for the following or other appropriate reliefs:

(a) A declaration in Kenya, the right of access to the internet is, under Article 19(3)(b), a right not in the Bill of Rights, but recognised or conferred by law. The right of access to the internet is inherent in Kenya's Constitution and Bill of

Rights. Internet shutdowns violate the fundamental right of access to the internet.

(b) A declaration that the impugned internet shutdowns violate Articles 32, 33, 34, 35, 36, 37, 38, and 46 (on opinion, expression, media, information, association, assembly, political rights, and consumer rights).

(c) A declaration that by failing to acknowledge internet shutdowns or providing minimal or no explanation for the measures, including their legal basis and underlying grounds, violate Article 10 on openness and transparency and Article 35 on information. A further declaration does issue that the state must make public any law or court order restricting fundamental rights unless there is a countervailing public interest reason for secrecy.

(d) Prohibition restraining the Respondents and their agents from unlawfully directing, enforcing, or implementing any internet shutdown in Kenya during protests, exams, elections, or other civic action.

(e) A declaration that the 4th and 5th Respondents are liable and violated their consumers' rights by effecting, enforcing, or implementing CA's unconstitutional directives on internet shutdown or Telegram suspension, in 2023 and 2024 outside the law and without a court order.

(f) An order does issue directing the 4th and 5th Respondents to, within 7 day of the order, publicly apologise to their consumers for the inconvenience caused by the internet shutdowns in 2023 and 2024.

(g) Damages for violation of the Petitioners' rights.

Dated at Nairobi on 13 May 2025

OchielJD

Bond Advocates LLP
Advocates for the Petitioners

Drawn and filed by:
Bond Advocates LLP
Top Plaza, 2nd Floor, Kindaruma Road
P. O. Box 37551-00100
Nairobi
0112318576
bond@bondadvocates.com
ochieljd@bondadvocates.com

REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
HCCHRPET/ 276 /2025

INTERNATIONAL COMMISSION OF JURISTS
KENYA SECTION (ICJ KENYA) .....1ST PETITIONER
BLOGGERS ASSOCIATION OF KENYA (BAKE).....2ND PETITIONER
KENYA UNION OF JOURNALISTS (KUJ).....3RD PETITIONER
COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA (CIPESA).....4TH PETITIONER

AND

COMMUNICATIONS AUTHORITY OF KENYA (CA).....1ST RESPONDENT
ATTORNEY GENERAL.....2ND RESPONDENT
CABINET SECRETARY INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY.....3RD RESPONDENT
SAFARICOM LTD.....4TH RESPONDENT
AIRTEL KENYA LTD.....5TH RESPONDENT
PARADIGM INITIATIVE (PIN).....1ST INTERESTED PARTY
LAW SOCIETY OF KENYA.....2ND INTERESTED PARTY
KATIBA INSTITUTE.....3RD INTERESTED PARTY

AFFIDAVIT ON THE MOTION AND PETITION

I Eric Mukoya of ICJ Kenya House, Off Silanga Road, Karen, P. O. Box 59743 – 00200 Nairobi make oath and state as follows:

1. I am the Chief Executive Officer of the Kenya Section of the International Commission of Jurists (ICJ Kenya). I am duly authorised, familiar with the facts, and competent to swear this affidavit on behalf of the petitioners.
2. ICJ has studied the existence and impact of internet shutdowns in Kenya. *I annex the Internet Outage and Detection Analysis (IODA), Open Observatory of Network Interference (OONI), Cloudflare, and the ICJ reports marked* **EM-1 to EM-4.**
3. The internet enables the enjoyment of rights and freedoms while enhancing transparency and accountability in public and private spheres. Therefore, internet shutdowns are powerful markers of sharply deteriorating human rights situations. Internet shutdowns also have major economic costs for all sectors, disrupting for example financial transactions, commerce and industry. Economic shocks of shutdowns are

felt over long periods, greatly exacerbating pre-existing social and economic inequalities

4. Yet, in Kenya, internet freedom is increasingly imperilled by emerging digital authoritarianism.
5. First, Respondents suspended Telegram during the 2023 and 2024 national examinations.
6. Then, on 25 June 2024, during the **#RejectFinanceBill** protests, the Respondents illegally shut down the internet. The June 2024 internet shutdown coincided with an unprecedented attack on fundamental rights and freedoms in which nearly 60 Kenyans were killed by state agents.
7. No law or court order sanctioned the June 2024 internet shutdown or the 2023 and 2024 suspension of Telegram. However, the June 2024 internet shutdown lasted several days causing daily GDP losses of $6.3 million and disproportionately affecting small businesses and women.
8. Access to the internet is an indispensable enabler of a broad range of human rights. It is not only essential for freedom of expression, but, as digitalization advances, it is also central to the realization of the rights to education, to freedom of association and assembly, to participate in social, cultural and political life, to health, to an adequate standard of living, to work and to social and economic development, to name just a few.
9. Hospitals being unable to contact their doctors in cases of emergency, voters being deprived of information about candidates, handicraft makers being cut off from customers, and potentially facing imminent economic ruin, peaceful protesters who fall under violent attack being unable to call for help, students missing entrance exams for academic programmes and refugees being unable to access information on the risks that they face are just some of the situations confronted when an Internet and telecommunications services shutdown occurs.

10. However, the Kenyan government has ordered shutdowns, unaware of, or oblivious to, the harsh impacts that they can cause or calculating that the factors motivating the shutdown outweigh those harms.

11. The dramatic real-life effects of shutdowns on the lives and human rights of millions of people are vastly underappreciated and deserve much greater attention from the court.

12. When implementing the shutdowns, the Respondents fail to publication of important information affecting the nation. acknowledge them or provide minimal or no explanation for the measures, including their legal basis and underlying grounds, thus violating Article 10 on openness and transparency and Article 35 on

I annex swered requests for information from 2023 and 2024 marked **EM-5** and **EM-6**

13. Fearing repeat internet shutdown including during the 2027 General Elections, exams or protests, Petitioners file this case. Petitioners seek appropriate reliefs for the 25 June 2024 shutdown and aim to deter future violations. The matter is urgent because of the **harmful effect of internet shutdowns** on human rights, the economy and democracy

14. I swear this affidavit from facts within my knowledge believing it to be true and per the Oaths and Statutory Declarations Act, Cap 15.

Sworn at Nairobi by Eric Mukoya on 13 May 2025)

DANIEL OMORO ACHACH
ADVOCATE
& COMMISSIONER FOR OATHS
P. O. Box 51340 - 00100
NAIROBI

Before me) .....
) Deponent
)
)
)
Commissioner for Oaths)

Drawn and filed by:
Bond Advocates LLP
Top Plaza, 2nd Floor,
Kindaruma Road
P. O. Box 37551-00100 Nairobi
0112318576
bond@bondadvocates.com
ochieljd@bondadvocates.com

The Kenya June 25, 2024 Internet Disruption: Subsea Cable Cut or Shutdown?

In this analysis, we investigate the temporal nature of the June 25, 2024 Internet disruption in Kenya by comparing it to two previous subsea cable outages in 2024 and comparing it to our findings from the first longitudinal analysis of shutdowns and spontaneous outages.

June 25th Internet Disruption -

Political Context

In the afternoon of June 25, 2024, Kenya experienced a severe Internet disruption. This disruption occurred seven days into a protest over the Kenya Finance Bill. The bill was widely condemned for imposing new and higher taxes on essential goods and services, such as bread, fuel, mobile money transfers, and digital products, which critics argued disproportionately impacted low-income households, vulnerable people and small businesses. The bill sparked unprecedented, largely youth-led protests, with demonstrators organizing under hashtags like #RejectFinanceBill2024 and #OccupyParliament, reflecting deep frustration with the government's approach to taxation and economic management. Protesters expressed anger with the government by ignoring public input and prioritizing debt repayment over citizens' welfare. On June 25, the peaceful protests culminated in a deadly clash between police and protesters, when protesters stormed the parliament. Twenty-two people were killed. Kenyan President Ruto bowed to the pressure of protesters and dropped the bill on June 27, 2024. Due to pressure from civil society, the Communications Authority in Kenya issued a press release on June 24, stating they had no intention of shutting down the Internet. This report further examines this declared intention by looking at IODA's measurements and comparing the June 25th disruption to previous

outages due to subsea cable damage and to IODA's groundbreaking research comparing spontaneous outages to shutdowns.

June 25th Internet Disruption

According to IODA data, a disruption to Internet connectivity began ~4:30 PM local time on June 25th, 2024 (see Image 1 below). Looking at IODA's Active Probing and Routing Announcement signals, we see a clear, abnormal drop in Internet connectivity signals in Kenya. At its lowest levels, 50% of previously responsive network addresses in Kenya stopped responding to IODA's Active Probing signals and were no longer connected to the global Internet. Routing Announcements (BGP) which is normally stable signal measuring at 100%, also abnormally dropped. . Most networks began to recover at 8:30 PM local time. At the same time, IODA picked up outages in Uganda, Burundi, Rwanda, and Tanzania. The multi-country nature of the event's impact on Internet connectivity is indicative of disruptions to critical Internet infrastructure connecting several countries like a terrestrial cable, subsea cable, or a cable landing station.

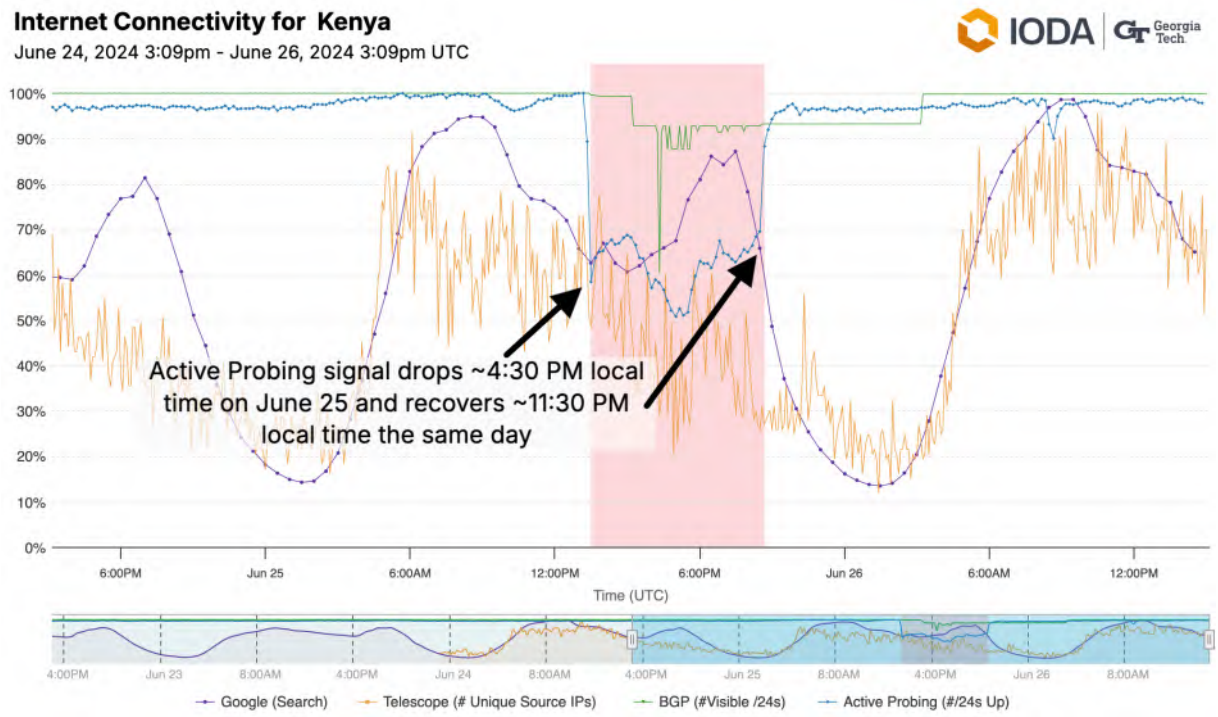


Image 1. This IODA time series data provides a view of Kenya's Internet disruption on June 25, 2024 from IODA

When investigating Internet disruptions, it is routine to look for announcements made by Internet Service Providers (ISPs). As measurement groups further investigated the disruption on June 25, 2024, two announcements were found by Airtel and Safaricom informing their customers that the disruption was due to an undersea cable outage.

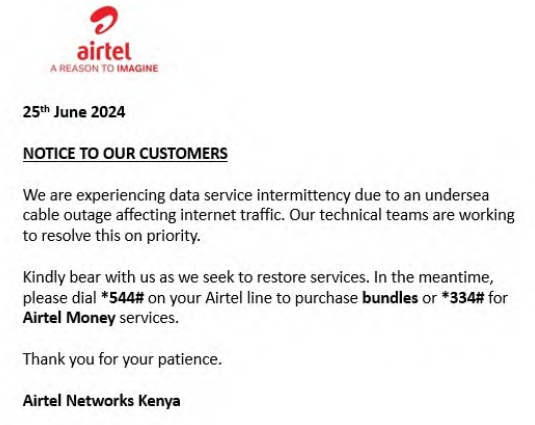


Image 2. Airtel post on X made on June 25th, 2024, at 3:13 PM local time

Image 3. Safaricom post on X made on June 25th, 2024, at 1:54 PM local time

These announcements spurred further investigation into which subsea cables were impacted. Notably, no definitive announcement was made by providers or the Kenyan government on which cables were impacted. One report on LinkedIn by the Co-Founder and Director of a company that provides fiber optic cable transmission service in Kenya mentioned two subsea cables, “PEACE” and “DARE”.

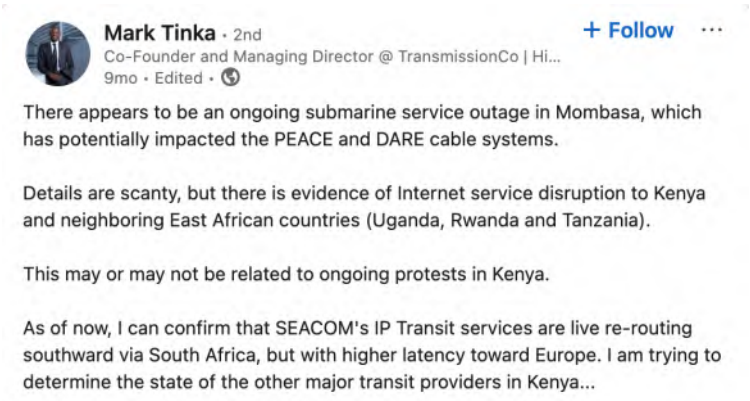


Image 4. Mark Tinka post, June 25th, 2024, on LinkedIn referencing a potential impact on PEACE and DARE cable systems.

The PEACE and DARE-1 cables both have landing stations in Kenya. These cables do not land in Tanzania, Uganda, Rwanda and Burundi but spillover effects from Kenya could conceivably cause a disruption in Internet connectivity in these neighboring countries due to the cross-boarder links between Kenya and Tanzania and cross-boarder links between Tanzania and Uganda, Rwanda, and Burundi. Having a retrospective view of the June 25th disruption allows us to compare the outage severity and duration to previous subsea cable outages. In the next section we compare this disruption to a subsea cable outage in May of 2024. Notably, the May 2024 subsea cable outage had a less severe impact on Kenya's connectivity signals but lasted longer. Additionally, the ISPs and Kenyan government's communications following the subsea cable outage were, more frequent, much more descriptive of what cables were affected, and included actions being taken to reduce the impact on connectivity. The following section outlines the May 2024 subsea cable outage.

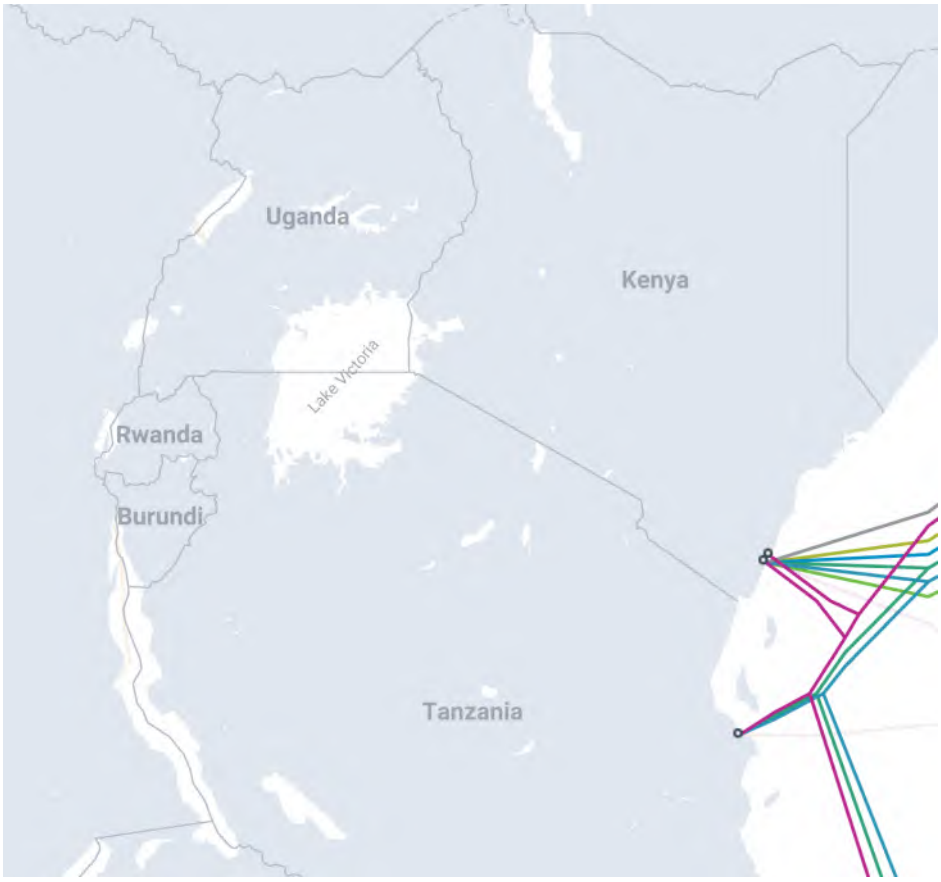


Image 5. Submarine cable map showing cables with landing stations in Mombasa, Kenya. (https://www.submarinecablemap.com/landing-point/mombasa-kenya)

The June 2024 Disruption Response compared to May 2024 Subsea Cable Outage Response

Kenya is connected to 8 subsea cables and has experienced subsea cable cuts before. On May 12th 2024, Kenya experienced an Internet disruption due to a legitimated subsea cable outage. In this section we compare the impact to connectivity, as seen in the IODA dashboard, and the response to the outage by the Communications Authority in Kenya (CA of Kenya) and the Internet Service Providers, Airtel and Safaricom.

On May 12th, 2024 Kenya experienced an Internet disruption due to a subsea cable outage. IODA data shows that this disruption lasted longer but had a less severe impact on Internet connectivity in Kenya, compared to the June 25th disruption.

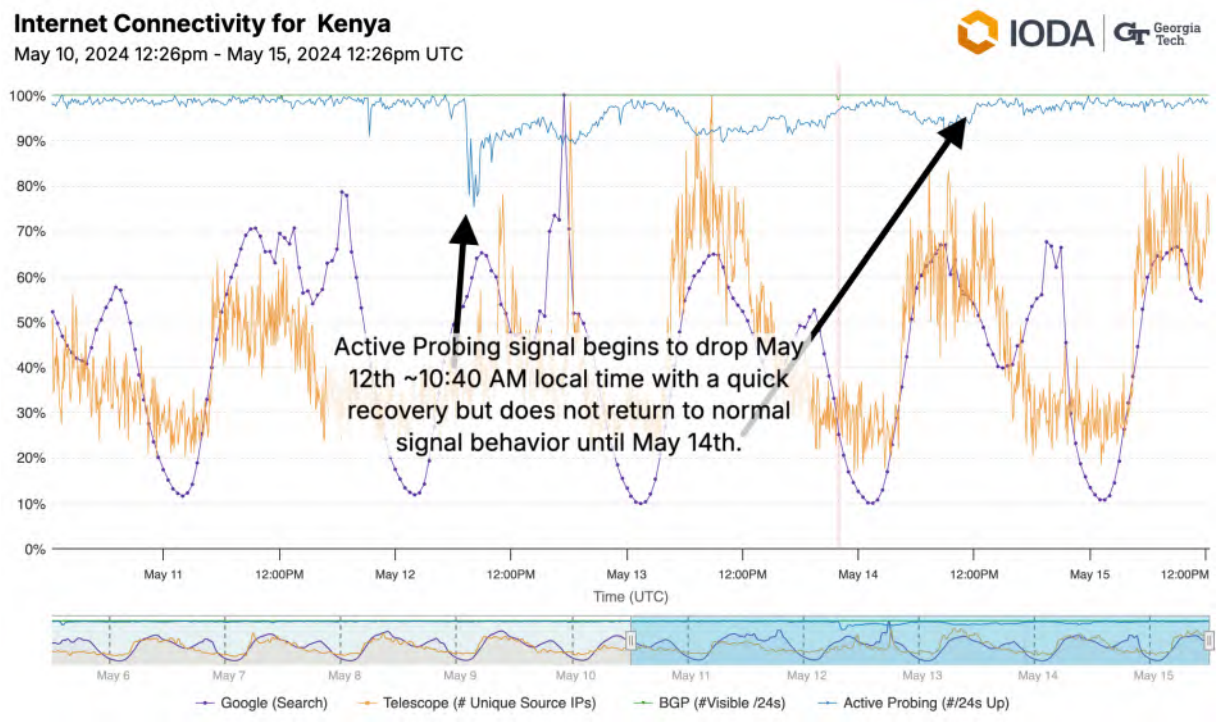


Image 6. IODA Internet connectivity for Kenya during the Internet disruption May 12 - 14th, 2024, due to a subsea cable outage.

According to IODA data, the Active Probing signal dropped at most 20% on May 12th compared to previous levels and recovered quickly but did not return to normal levels until two days later. In a blog post reviewing the May 2024 subsea

cable outage, Cloudlfare Radar noted, “In Kenya, the impact may have been nominal due to steps taken by providers like Safaricom and Airtel Kenya.” Additionally, we note that BGP and Telescope did not show an abnormal drop during this time, only Active Probing.

On May 13th, the CA of Kenya issued a press release made after the subsea cable outage. This press release includes details of the outage by noting which cables and stations were affected as well as the proactive steps being put in place to reroute Internet traffic. After searching the website press release section and their social media, we did not find any subsequent press release from the CA of Kenya that acknowledged any subsea cable outage on June 25, 2024. Additionally, both Safaricom and Airtel issued initial and subsequent social media posts updating how they had implemented measures to restore Internet connectivity in May. No such updates were made in June.

COMMUNICATIONS AUTHORITY OF KENYA

PRESS RELEASE

DEEP SEA FIBRE CUTS AFFECT INTERNET SERVICES IN KENYA

13th May, 2024: Yesterday, the Authority received reports on intermittent data outages and traffic jam on the submarine cable Internet traffic flow into the country.

Upon engaging the relevant industry players, the Authority has established that a deep-sea fibre cut had occurred on the Mtunzini teleport station, affecting a number of submarine cables serving Kenya, including Seacom and the East African Submarine System (Eassy).

We wish to inform individual and corporate consumers that the recovery process has since commenced but Internet intermittency and slow speeds may remain in the coming few days before services are fully restored.

Meanwhile, the Authority has directed service providers to take proactive steps to secure alternative routes for their traffic and is monitoring the situation closely to ensure that incoming and outbound internet connectivity is available.

The East Africa Marine System (TEAMS) cable, which has not been affected by the cut, is currently being utilised for local traffic flow while redundancy on the South Africa route has been activated to minimize the impact.

David Mugonyi EBS
Director-General & CEO

For more information, please contact:
Director/Corporate Communications
Email: info@ca.go.ke

Image 7. Press release from Communications Authority of Kenya on May 13th, 2024, explaining which cables were damaged and actions being taken for repair.

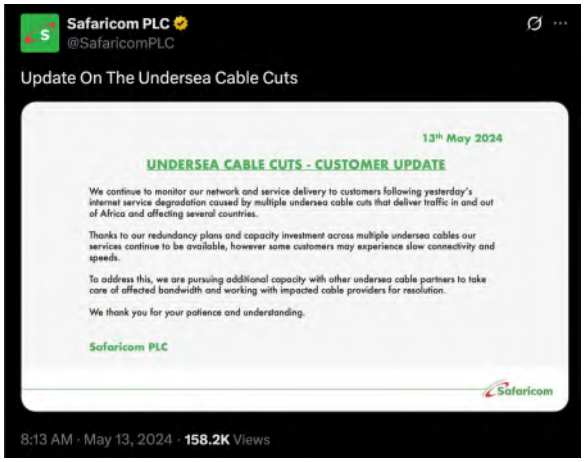


Image 8. Post on X from Safaricom after May 13th subsea cable outage.

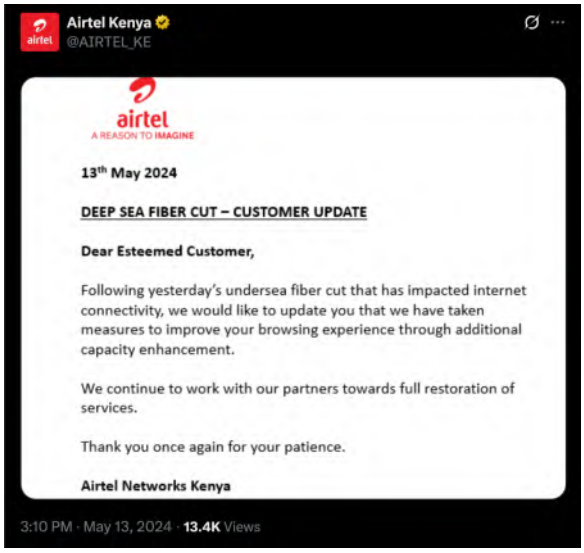


Image 9. Post on X from Airtel after May 13th subsea cable outage.

Image 10. Follow-up post X from Airtel on May 16th, 2024.

ISPs often have important information during outages and shutdowns as they are either closest to the actions taken to improve service delivery during an outage or they are the ones implementing a government-directed shutdown. Internet

measurement sources like IODA or Cloudlfare make use of these announcements to help us interpret cause and context when looking at our Internet measurement data. It is notable how different Safaricom and Airtel's communications are in May compared to June. In May, they published several subsequent updates assuring customers that measures had been taken to improve service delivery. No such update was made for June 25th. Even more odd was the lack of a press release from the CA of Kenya, especially when compared to the detailed press release on May 13th.

Comparison to March 2024 Subsea Cable Outage Length of Repair Time

In the previous section, we compared the June 25, 2024, Internet disruption to the May 2024 subsea cable outage that affected Kenya. In this section, we compare the June 25, 2024 outage to the March 2024 West Africa subsea cable damage that affected 13 countries with the most heavily affected being Cote d'Ivoire, Benin, and Cameroon. This comparison will further demonstrate the length of repair time for a subsea cable outage.

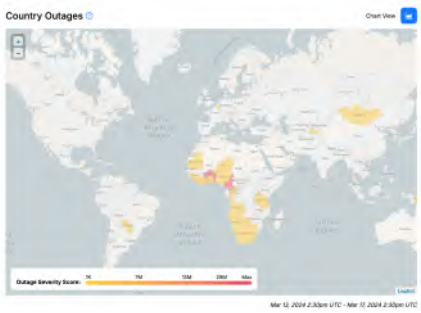


Image 11. The County Outage Severity Overview for March 13 - 17, 2024 shows how many countries in West Africa were impacted by the subsea cable outage.

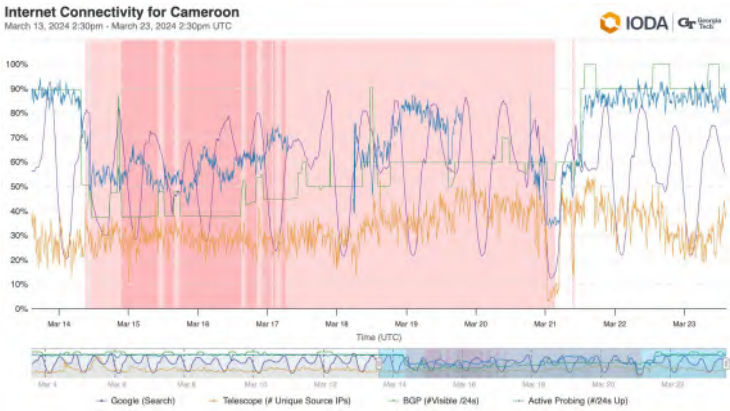


Image 12. IODA connectivity signals from a 7-day outage in Cameroon in March 2024 due to a subsea cable cut.

This comparison demonstrates that repairs to subsea cable outages take weeks to implement, as there are limited number of repair vessels globally that may not be in the vicinity to make a repair. Additionally, our research shows that impact of a

subsea cable outage on both connectivity and latency will last days. This was seen when the ACE, SAT-3, WACS, MainOne subsea cables were damaged due to a suspected underwater rock slide. As mentioned, this damage greatly impacted Internet connectivity in Cote d'Ivoire, Benin, and Cameroon. In particular for Cameroon, the Internet disruption related to this subsea cable outage lasted 7 days, from March 14 - 21, 2024 (see Image 10 above). Internet connectivity recovery for Cote d'Ivoire took over three days.

If we look at TeleGeography's reporting on number of days to repair an August 2023 subsea cable cut, we see the following repair durations: ACE - 37 days, SAT-3/WASC - 43 days, WACS - 30 days. Again, this demonstrates that subsea cable outages can require significant repair time. Accordingly, it is not likely that officials notified crews, an available crew navigated to the repair location, and then completed the repair within the ~7 hours of the June 25, 2024 disruption in Kenya.

Temporal Signatures of Shutdowns versus Spontaneous Outages

Additionally, we would like to provide an analysis of the time signatures of spontaneous outages (not government-directed, e.g. a subsea cable outage) versus shutdowns (government-directed), based on our longitudinal study comparing shutdowns and spontaneous outages, *Destination Unreachable: Characterizing Internet Outages and Shutdowns*. While the article explores various potential correlates with shutdowns and spontaneous outages, here we focus on the temporal signatures.

First, this Internet disruption co-occurred with a protest. In our analysis, we found that shutdowns are 9 times more likely to co-occur with protests than spontaneous outages.

Second, shutdowns (87.4%) are more likely to start on the hour or half hour compared to spontaneous outages (39.6%). Internet measurement data provided the following start times: 4:25 PM by Kentik, 4:30 PM by Coudlfare Radar, and 4:30 PM by IODA. The start time, according to Cloudflare Radar and IODA, aligns more with a shutdown than a spontaneous outage.

Our research also found that shutdowns are more likely to last longer than spontaneous outages. Specifically, the median length of shutdowns is 5.5 hours and the median length of spontaneous outages is 2 hours. Internet measurement data shows the June 25 Kenya Internet disruption lasted ~7 hours, which is closer to the duration of a shutdown, per our historical analysis.

We also found that 55% of shutdowns compared to 15% of spontaneous outages last for multiples of 30 minutes (e.g. 1 hour, 1.5 hours, 2 hours, etc). Kentik reported a duration of 7 hours and 20 minutes. Cloudflare Radar reported 7 hours and 15 minutes. IODA reported ~7 hours. Accordingly, based on these estimated durations, this aligns more with a spontaneous outage.

In our analysis we also found that 67.7% of shutdowns reoccur over the next 1,2,3,4 days; however, we do not find this was the case in Kenya.

Finally, we looked at the number of IODA signals that drop during a shutdown versus a spontaneous outage. 94.5% of shutdowns show visible drops in all three of IODA's signals, while only 55.3% of spontaneous outages show visible drops in all three of IODA's signals. For the Internet disruption on June 25, 2024, we found that the loss in connectivity was most visible in Active Probing and BGP. IODA's Telescope signal in Kenya is too low to reliably detect an abnormal drop.

Table 1. Temporal signatures of spontaneous outages versus shutdowns

Temporal Signatures	Spontaneous Outage	Shutdown	Kenya Internet Disruption June 25-26, 2024	Aligns with Outage or Shutdown
Co-occur with a protest		9 times more likely	Finance Bill Protest	Shutdown
Start time - on the hour or half hour	39.6%	87.4%	1:30 PM UTC / 4:30 PM EAT	Shutdown
Length - duration	2	5.5	~7 hours	Shutdown
Length - multiple of 30	15%	55%	7 hours and 20 minutes. Cloudflare Radar reported 7 hours and 15 minutes.	Spontaneous Outage

Temporal Signatures	Spontaneous Outage	Shutdown	Kenya Internet Disruption June 25-26, 2024	Aligns with Outage or Shutdown
			IODA reported ~7 hours	
Recurrence - likely to reoccur in 1,2,3,4 days	17%	67.7%	no recurrence	Spontaneous Outage
Number of IODA signals that show a drop in connectivity	55.3% show drop in all three signals	94.5% show drop in all 3 signals	Visible in Active Probing and BGP. Telescope signal is too low to be conclusive	Inconclusive

When looking at co-occurrence with a protest, start time, and length, the Internet disruption in Kenya shows signatures of a shutdown. When looking at duration lasting multiples of 30 and reoccurrence, this Internet disruptions aligns more with a spontaneous outage.

Conclusion

According to this analysis, it is unlikely that the June 25, 2024, Internet disruption in Kenya was caused by a subsea cable outage. Internet measurement data cannot show cause of a disruption, but we hope this analysis provides further details regarding:

- How Kenya Internet connectivity and the Kenyan government and ISPs responses in June 25th 2024 were importantly different from the legitimated May 12-14th 2024 subsea cable outage.
- The expected length for repair of a subsea cable outage is days, not hours. We demonstrate this by showing that the May 2024 subsea cable outage that lasted 3 days and the ACE, SAT-3, WACS, MainOne subsea cables that caused an outage that lasted up to 7 days, from March 14 - 21, 2024.
- How this disruption aligns with several indicators of shutdowns based on our longitudinal statistical analysis of shutdowns and spontaneous outages.

Witness Statement

Expertise

The above report was researched and written by Dr. Zachary Bischof, Senior Research Scientist, and Internet Measurement expert; and Dr. Amanda Meng, Senior Research Scientist, and International Affairs, Science, and Technology expert.

Impacts of Shutdowns on Rights and Freedoms

The Internet has been enshrined as a human right by the United Nations since 2012. The Internet is seen as critical infrastructure, providing access to both information and communication technologies that support an array of human activity from access to life-saving services to enabling dissemination of information supporting democratic mobilization. Government-directed shutdowns impede on this human right, restricting access to information, communication technologies and services reliant on the Internet.

Methodology of the Study

Internet Outage Detection and Analysis (IODA) is a system that monitors the connectivity of Internet infrastructure, in near-real time, to identify Internet outages affecting networks, nations, and subnational regions. It is run out of the Internet Intelligence Lab at Georgia Tech's College of Computing, in the School of Computer Science.

IODA generates three signals, Border Gateway Protocol (BGP) aka Routing Announcements, Active Probing, and Telescope. We used these three signals to report on Internet connectivity in Kenya. These three signals are described below.

IODA generates the BGP signal by analyzing data from RouteViews and RIPE RIS collectors using BGPStream with BGPView. For each time bin, IODA calculates the total number of "full-feed" peers that observe each routable prefix. A peer is considered full-feed if it has more than 400k IPv4 prefixes and/or more than 10k IPv6 prefixes. A prefix is considered visible if it is observed by at least 50% of the full-feed peers. IODA uses this data to calculate the total number of visible /24s per country, region, and Autonomous System every 5 minutes.

For the Active Probing signal, IODA conducts active measurements using a technique similar to Trinocular, probing approximately 4.2M /24 blocks at least once every 10 minutes via ICMP packets. Using the Trinocular measurement and inference technique, IODA labels each /24 block as up, down, or unknown. After each 10-minute cycle, IODA calculates the number of /24s that are considered active for each country, subnational region, and Autonomous System.

To obtain the Telescope signal, IODA analyzes traffic received by a network telescope. IODA applies multiple antispoofing heuristics and noise reduction filters to the raw traffic to create a set of valid packets. For each valid packet, IODA uses IP geolocation databases and Autonomous System lookups to map a packet's source IP address to a geographic location and Autonomous System. For each country, region, and Autonomous System view, the IODA dashboard displays the number of unique source IP addresses observed in each 5 minute bin. Though IODA currently uses the Merit Network Telescope, prior to January 2022, IODA used the UCSD Network Telescope.

In addition to the measurement methodology of IODA, we employ a comparative case study analysis to compare the June 24, 2025 Internet disruption to previous ligitimated Internet disruptions caused by subsea cable outages. Finally, we draw from our longitudinal study comparing spontaneous outages to government-ordered shutdowns, which leveraged multiple analytical methods to characterize and identify relationships between the occurrence government-ordered shutdowns across multiple social, political, economic, and technical indicators.

Findings of the Study

IODA data indicates a ~7 hour disruption of the Internet in Kenya that had spillover effects in Uganda, Burundi, Rwanda, and Tanzania. The multi-country nature of the event's impact on Internet connectivity is indicative of disruptions to critical Internet infrastructure connecting several countries like a terrestrial cable, subsea cable, or a cable landing station.

Internet Service Providers and the Communications Authority of Kenya provided very little information on which cables were impacted and what actions were being taken in response to the June 24, 2025 Internet disruption in Kenya in comparison to the subsea cable outage affecting Kenya on May 12th-14th Internet disruption. The difference in how the outage and response was communicated is

stark and notable and raises questions as to whether there was really a subsea cable outage on June 24, 2025 affecting Kenya.

Based on repair times reported for previous legitimated subsea cable outages, it is unlikely that officials notified crews, an available crew embarked and navigated to the repair location, and then completed the repair within the span of the ~7 hours of the June 25, 2024 disruption in Kenya.

Comparing the temporal signatures of the June 24, 2025 Kenya Internet disruption to our longitudinal study comparing spontaneous outages to government-directed shutdowns, we find that the Internet disruption in Kenya shows 3 signatures of a government-directed shutdown and 2 signatures of a spontaneous outage.

Expert Opinion on the Blocking of Telegram in Kenya During the 2023 and 2024 KCSE Exams

By the Open Observatory of Network Interference (OONI) Foundation

April 2025

Table of Contents

Introduction

Access to Telegram was blocked in Kenya during the Kenya Certificate of Secondary Education (KCSE) national exams in both November 2023 and November 2024. This document provides an Expert Opinion by the Open Observatory of Network Interference (OONI) Foundation on these blocks.

OONI is a nonprofit organization with global expertise on Internet censorship, having built free software tools for measuring Internet censorship since 2012. OONI hosts the world's largest open dataset on Internet censorship of its kind, consisting of more than 2 billion measurements collected from 28,000 unique networks across 242 countries and territories. Since OONI measurements are collected from the edge of the network, they provide unique insights into the accessibility or blocking of Internet services and can serve as evidence of Internet censorship.

The following sections of this document share further information about OONI, their measurement methodologies, and OONI measurement coverage in Kenya. More importantly, the following sections share relevant OONI data and technical analysis that serves as evidence of the blocking of Telegram on networks in Kenya during the November 2023 and November 2024 KCSE exams.

Summary of Findings

2023 KCSE exams: Blocking of Telegram

Between 8th to 24th November 2023 (which correlates with the dates of the 2023 KCSE exams), OONI data shows that access to Telegram was **intermittently blocked** on Safaricom (AS33771 and AS37061) and Airtel (AS36926), and **persistently blocked** on Jambonet (AS12455).

More specifically, during the 2023 KCSE exams, OONI data shows:

- **Blocking of the Telegram website (telegram.org).**
  - **TLS interference.** On the Safaricom (AS33771) and Airtel (AS36926) networks, OONI data shows the timing out of the session after the ClientHello message during the TLS handshake.
  - **DNS tampering.** On the Jambonet (AS12455) network, OONI data shows that DNS resolution for the domain name telegram.org returned an IP address in local IP space (192.168.7.222), instead of the actual IP address for telegram.org. OONI data shows that this behavior persists even outside of the exam hours.
- **Blocking of Telegram Web (web.telegram.org).**
  - **TLS interference.** OONI data shows TLS level blocks affecting the IP address 149.154.167.99 (which is the IP of the Telegram web application) on the Safaricom (AS33771 and AS37061) and Airtel (AS36926) networks.
- **Blocking of the Telegram app endpoints.**
  - **IP level blocks on Jambonet.** Of all tested networks, OONI data shows that only Jambonet (AS12455) seems to have implemented IP level blocking of Telegram endpoints. On this network, all tested Telegram endpoints consistently presented timeout errors between 8th November 2023 to 24th November 2023. Similarly to the blocking of telegram.org, OONI data shows that Jambonet continued to block access to Telegram endpoints outside of the time period of the 2023 KCSE national exams (such as during the weekend and outside of exam hours).
- **Unblocking of Telegram.** OONI data shows that the blocking of Telegram was lifted by 25th November 2023, which correlates with the end of the 2023 KCSE exams.

2024 KCSE exams: Blocking of Telegram

In November 2024, during the 2024 KCSE exams, OONI data shows that access to Telegram was blocked on Safaricom (AS33771 and AS37061), Jambonet (AS12455), and on Jamil Telecommunications (AS36866).

More specifically, during the 2024 KCSE exams, OONI data shows:

- **Blocking of the Telegram website (telegram.org).**
  - **IP blocking on Safaricom.** OONI data shows TCP/IP timeout errors on two Safaricom networks (AS33771 and AS37061), suggesting that access to telegram.org was blocked at an IP level. On AS33771, the block persisted outside of the exam hours and throughout the weekend, even though ISPs were only instructed to block access to Telegram on weekdays during the exam hours. On AS37061, the block was lifted during the weekend (9th and 10th November 2024).
- **Blocking of Telegram Web (web.telegram.org).**
  - **IP blocking.** OONI data shows that access to Telegram Web (web.telegram.org) was restricted by means of IP blocking on Safaricom (AS33771 and AS37061) and Jambonet (AS12455).
  - **TLS interference.** On Jamil (AS36866), OONI data suggests that the blocking of web.telegram.org was implemented at the TLS level because the connection was reset after the ClientHello message during the TLS handshake. However, very few measurements are available that overlap with the 2024 KCSE exam hours, limiting this finding.
- **Blocking of the Telegram app endpoints.**
  - **IP level blocks.** Between 7th to 22nd November 2024, OONI data shows that access to Telegram app endpoints was blocked on the Jambonet (AS12455) and Safaricom (AS33771 and AS37061) networks.
    - On Jambonet (AS12455), OONI data shows that *all* tested Telegram endpoints were blocked, and that the block was limited to exam hours.
    - On Safaricom networks (AS33771 and AS37061), OONI data shows the blocking of most Telegram endpoints, except for two (149.154.175.100 and 149.154.175.50), and that the block persisted outside of the hours of the national exams.
- **Unblocking of Telegram Web *after* the 2024 KCSE exams.** While the blocking of Telegram app endpoints was lifted by 23rd November 2024 (at the end of the 2024 KCSE exams, as instructed by the Communications Authority of Kenya), OONI data suggests that access to Telegram Web (web.telegram.org) remained blocked on Safaricom networks (AS33771 and AS37061) until 29th November 2024.

About OONI

This Expert Opinion on the blocking of Telegram in Kenya during the 2023 and 2024 KCSE exams is provided by the Open Observatory of Network Interference (OONI) Foundation (hereafter referred to as "OONI"). OONI is a nonprofit organization, legally registered in Rome, Italy, with global operations and extensive global expertise in Internet censorship.

Having pioneered crowdsourced methods for measuring Internet censorship, OONI is a leader in the network measurement world. OONI won the 2012 Access Now Freedom of Expression Tech Prize for actionable ideas on how to use information technology to promote and enable human rights and deliver social good. More recently, OONI received the Free and Open Communications on the Internet (FOCI) 2023 Community Award.

Since 2012, OONI has developed OONI Probe, a free and open source software designed to measure various forms of Internet censorship, including the blocking of the Telegram app. Each month, volunteers run OONI Probe in around 170 countries, including Kenya, where users have contributed more than 9 million network measurements from 94 local networks since 2016. By default, OONI automatically publishes network measurements submitted by OONI Probe users worldwide as open data in real-time. With over 2 billion network measurements collected from 28,000 unique Autonomous Systems (ASes) across 242 countries and territories since 2012, OONI maintains the world's largest open dataset on Internet censorship of its kind.

More specifically, OONI works on the following:

- **Free and open source tools for measuring internet censorship.** Since 2012, OONI has developed free and open source software designed to measure various forms of Internet censorship. Through their OONI Probe app, anyone can measure the blocking of websites and instant messaging apps (including Telegram) and collect network measurement data in real-time that can serve as evidence.
- **Real-time open data on internet censorship.** OONI maintains the largest open dataset on Internet censorship to date. As soon as anyone runs OONI Probe anywhere around the world, their test results are automatically published by OONI as open data in real-time. To enable researchers to investigate Internet censorship, OONI provides an API for downloading the raw data in JSON format, a web platform ("OONI Explorer") for searching through OONI measurements, and a Measurement Aggregation Toolkit (MAT) for generating charts based on aggregate views of OONI data.
- **Research on internet censorship based on OONI data.** OONI has published more than 75 reports documenting Internet censorship around the world based on the analysis of OONI data. Notably, these include a technical multi-stakeholder research report on Internet shutdowns in Iran, facilitated by the European Commission and the United States government. OONI presented this report to members of the Trade and Technology

Council (TTC) and to EU Member States of the High Level Group on Internet Governance (HLIG).

- **Partnerships on the study of Internet censorship.** Since 2016, OONI has established more than 50 partnerships with leading digital rights organizations worldwide to study Internet censorship. These include research collaborations with academic institutions like the Oxford Internet Institute at the University of Oxford and Georgia Tech, as well as with prominent global nonprofits such as the Internet Society (ISOC).

Over the past decade, OONI data has supported third-party research on Internet censorship in Iran, Egypt, Malaysia, the Philippines, India, Venezuela, Rwanda, Uganda, Lebanon, Myanmar, Azerbaijan, Ukraine, Russia and Crimea (among many other countries). Freedom House has cited OONI data in many of their annual Freedom on the Net country reports. OONI data has also supported academic papers, such as research on China's DNS censorship, global CDN geoblocking, global I2P censorship, and on the deployment of network censorship filters at a global scale.

Harvard's Berkman Klein Center integrated OONI data into their AccessCheck project. Internet Society (ISOC) includes OONI data in their Pulse Internet Shutdowns project, which provides a timeline of blocking events and internet shutdowns around the world. Journalists worldwide also rely on OONI data when reporting on emerging censorship events. For example, OONI data is cited in articles by major news outlets such as Wired, BBC, CNN, CBC News, CNET, The Intercept, Wall Street Journal, Deutsche Welle, Taggesspiegel, Mada Masr, Al Araby, Time, and Africa Times, among many others.

OONI's Internet Measurement Methodology

Overall, OONI measures Internet services in a crowdsourced way through network-level experiments run by OONI Probe app users in around 170 countries each month. Each of these experiments has a different methodology, all of which are publicly documented. Since these experiments are run from local network vantage points, they offer **unique insights into the accessibility or blocking of Internet services at the edge of the network**. OONI publishes OONI Probe test results ("measurements") from around the world as open data in real-time.

To examine the reported blocking of Telegram in Kenya, OONI analyzed measurements collected from the OONI Probe testing of Telegram in the country. Specifically, OONI analyzed measurements from two OONI Probe experiments that are relevant to the testing of Telegram:

- Telegram experiment
- Web Connectivity experiment

The following sections explain how each of these two experiments work.

Telegram experiment

The OONI Probe Telegram experiment is designed to measure the reachability of Telegram's app and web version within a tested network. More specifically, the test attempts to establish a TCP connection to the endpoints of the Telegram app (DCs) and perform an HTTP POST request, as well as an HTTPS GET request to Telegram's web version (web.telegram.org) over the vantage point of the user. The test results are automatically annotated as "OK" if the experiment succeeds in all of these steps. If they fail, the test results are automatically annotated as "anomalous", indicating potential blocking.

Based on OONI's methodology, Telegram's app is considered likely blocked if TCP connections on ports 80 and 443 to all tested Telegram access point IPs fail, and/or if HTTP POST requests to Telegram's access points do *not* send back a response to OONI's servers. Telegram's web version (web.telegram.org) is likely blocked if the TLS handshake fails or if the HTTPS GET requests to web.telegram.org do *not* send back a consistent response to OONI's servers. However, false positives can occur due to a number of reasons, such as due to transient network failures, or if Telegram makes changes to their infrastructure that affect how the OONI Probe Telegram experiment runs.

Web Connectivity experiment

OONI's Web Connectivity experiment is designed to measure the blocking of the websites included in the public, community-curated Citizen Lab test lists, which include telegram.org.

Specifically, OONI's Web Connectivity test is designed to measure the accessibility of URLs by performing the following steps:

- Resolver identification
- DNS lookup
- TCP connect to the resolved IP addresses
- TLS handshake to the resolved IP addresses
- HTTP(s) GET request following redirects

The above steps are automatically performed from *both* the local network of the user, and from a control vantage point. If the results from both networks are the same, the tested URL is annotated as accessible. If the results differ, the tested URL is annotated as anomalous, and the type of anomaly is further characterized depending on the reason that caused the failure (for example, if the TCP connection fails, the measurement is annotated as a TCP/IP anomaly).

Anomalous measurements may be indicative of blocking, but false positives can occur. The likelihood of blocking is therefore greater if the overall volume of anomalous measurements is

high in comparison to the overall measurement count – compared on an AS level within the same date range for each OONI Probe experiment type.

Each Web Connectivity measurement provides further network information (such as information pertaining to TLS handshakes) that helps with evaluating whether an anomalous measurement presents signs of blocking. OONI therefore disaggregates based on the reasons that caused the anomaly (e.g. connection reset during the TLS handshake) and if they are consistent, they provide a stronger signal of potential blocking.

Based on their heuristics, OONI is able to automatically confirm the blocking of websites based on fingerprints if a block page is served, or if DNS resolution returns an IP known to be associated with censorship. These blocking fingerprints enable OONI to automatically confirm website blocks in countries like Russia, Italy, Kazakhstan, Iran, and Indonesia where ISPs implement blocks with these techniques. For other countries (such as Kenya) where ISPs implement blocks differently, OONI analyzed anomalous measurements with their data analysis tool to determine whether those anomalies are symptomatic of blocks.

Data analysis

OONI analyzed measurements for test_name = telegram and those for test_name = web_connectivity and hostname = telegram.org on each tested network during the date range of interest. The analysis was further restricted to networks (ASes) which had a sufficient number of measurements to have a high enough confidence in the findings. The notebook used by OONI to perform the data analysis is available **here**.

In order to perform the analysis more effectively, the raw OONI measurement JSONs were converted into observations and the interpretation of the anomaly from the perspective of the probe (the value of the `blocking` key in web_connectivity and the keys telegram_http_blocking, telegram_tcp_blocking, telegram_web_status for the telegram test) is discarded. In doing so, OONI is able to adjust the analysis to the specificity of the blocking patterns seen and improve the accuracy of the findings.

Observations are generated from raw OONI measurement JSONs using OONI Pipeline v5 and, generally, a given OONI measurement will correspond to multiple observations. An observation is the outcome of a particular network operation towards a specific target (e.g. “When attempting to perform a TCP handshake to IP address 123.45.67.8 on port 443, we got a connection refused”). These observations are then aggregated by a specific time window (mostly hourly) and disaggregated by network (probe_asn) and/or target (IP address or domain name).

As outlined in previous sections, the measurement collection logic differs between the Web Connectivity and Telegram experiments and, therefore, the analysis will vary slightly.

For the Web Connectivity measurements, OONI looks at the observations for each distinct IP address which was resolved for the domain name telegram.org. OONI excludes IPv6 addresses, since they noticed that IPv6 connectivity on all tested networks in Kenya was not working reliably. OONI also exclude IP addresses which are bogons (i.e. IPs that should not appear on the public internet), which leaves us with a single Telegram IP address: 149.154.167.99. OONI then inspects the outcome of the TCP connect and TLS handshake operation to assess whether these operations are failing consistently in the same way on the same network.

For the Telegram measurements, OONI analyzes separately the observations targeting the Telegram app endpoints (for which only a TCP connect operation is performed) from those targeting Telegram Web (web.telegram.org). The Telegram Web measurements – since they also include a TLS handshake – are analyzed in a way that is very similar to that of Web Connectivity measurements.

For the Telegram app endpoint tests on the other hand, OONI only looks at the TCP connect outcome and again checks for consistent failures across the same network. When OONI notices some inconsistencies in the failures, they will then manually inspect the inconsistent measurements to determine why they may not be consistent. One important limitation of the test, however, is that it does not actually speak the Telegram MTProto protocol once a TCP connection is established to the endpoint. This means that there is the risk of reporting the application as functional, while it in fact does not work due to protocol level blocks that only occur after the initial TCP handshake.

Each of the time series charts shared in this report contain an overlay of the times in which the national KCSE exams were occurring to identify a correlation between the time of the blocks and the ongoing exam times.

Acknowledgement of limitations

The OONI findings of this Expert Opinion present several limitations:

- **Date range of analysis.** The findings are limited to OONI network measurement data collected from Kenya in November 2023 and November 2024, when the blocking of Telegram was reported in the country during the KCSE exams.
- **Measurement coverage.** The availability of OONI data depends on whether, on which networks, and when an OONI Probe user ran tests in Kenya. As OONI Probe is used on a voluntary basis, OONI has no control over the availability measurements. As a result, OONI measurement coverage in Kenya varies over time.

- **Tested ASes.** While OONI Probe tests are regularly performed on multiple ASes in Kenya, not all networks are tested equally. Rather, the availability of measurements depends on which networks OONI Probe users were connected to when performing tests. As a result, OONI measurement coverage varies across ASes over time in Kenya. Moreover, the findings are limited to the ASes which received the largest measurement coverage and which presented the strongest blocking signals during the analysis period.
- **Blocking signals.** As part of their data analysis, OONI limited their findings to signals that they considered more reliable and indicative of government-commissioned censorship, while excluding cases viewed as presenting weak signals (due to limited measurement coverage and inconsistent failure types).

OONI measurements from Kenya

Since 2012, the Open Observatory of Network Interference (OONI) has built free software apps (OONI Probe) which include experiments designed to measure various forms of internet censorship, including the blocking of Telegram. These experiments are run by OONI Probe users in around 170 countries (including Kenya) every month, testing their networks to detect the blocking of websites and apps. To increase transparency of Internet censorship, OONI publishes OONI Probe test results ("measurements") from around the world as open data in real-time.

Since 2016, OONI Probe users in Kenya have contributed more than 9 million measurements from 94 local Autonomous Systems (ASes). Every day, OONI Probe users in Kenya continue to contribute new measurements, which OONI publishes in real-time. These longitudinal network measurements – spanning from 2016 to date – provide insight into the accessibility of tested websites and apps on tested networks in Kenya.

Over the past decade, OONI data suggested that Kenya was a leader in defending Internet freedom, with almost no blocks detected or reported. In fact, OONI even published a short report in December 2016 (titled "Kenya: Censorship-free internet?") documenting that almost no signs of Internet censorship had been detected in Kenya based on the analysis of OONI data. This stood in sharp contrast to other East African countries, such as Ethiopia and Uganda, where access to major social media platforms was blocked.

However, Kenya's record of maintaining access to Internet services declined during the November 2023 and November 2024 KCSE exams, when access to Telegram was allegedly blocked. To examine whether Telegram was blocked in Kenya, it is necessary to first evaluate whether there was OONI measurement coverage from the country during those time periods (leading up to, during, and after November 2023 and November 2024). In general, the greater the availability of network measurement data, the more likely it is to derive statistically meaningful conclusions.

The following two charts illustrate overall OONI measurement coverage (including results from all OONI Probe experiments), aggregated from all tested networks in Kenya throughout 2023 and 2024.

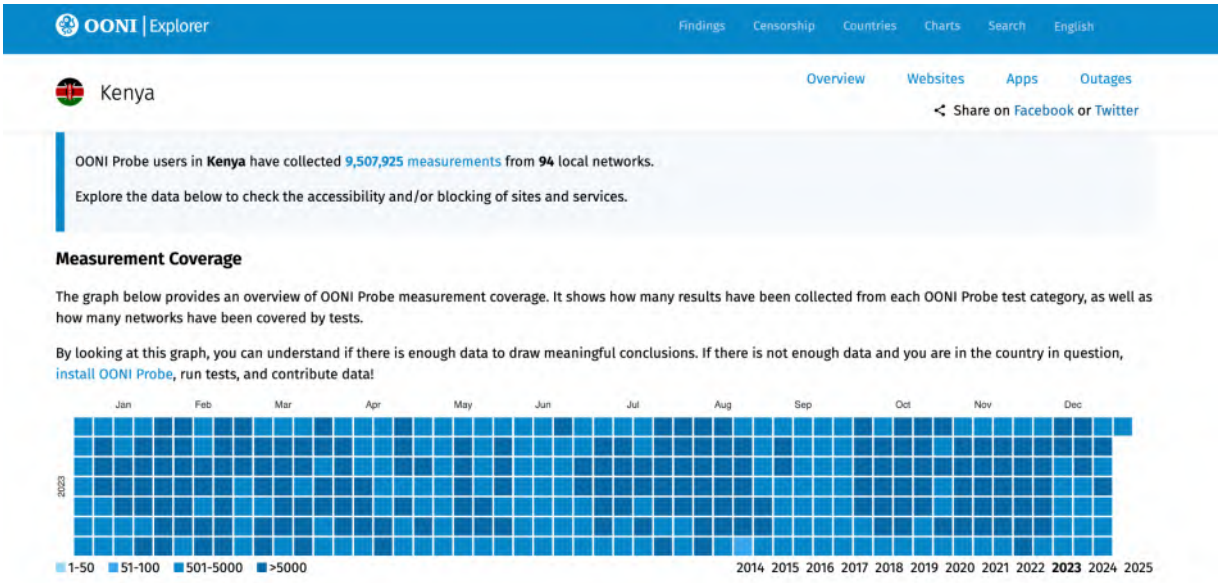


Chart: Overall OONI measurement coverage aggregated from all tested networks in Kenya between January 2023 to December 2023 (source: OONI Explorer).

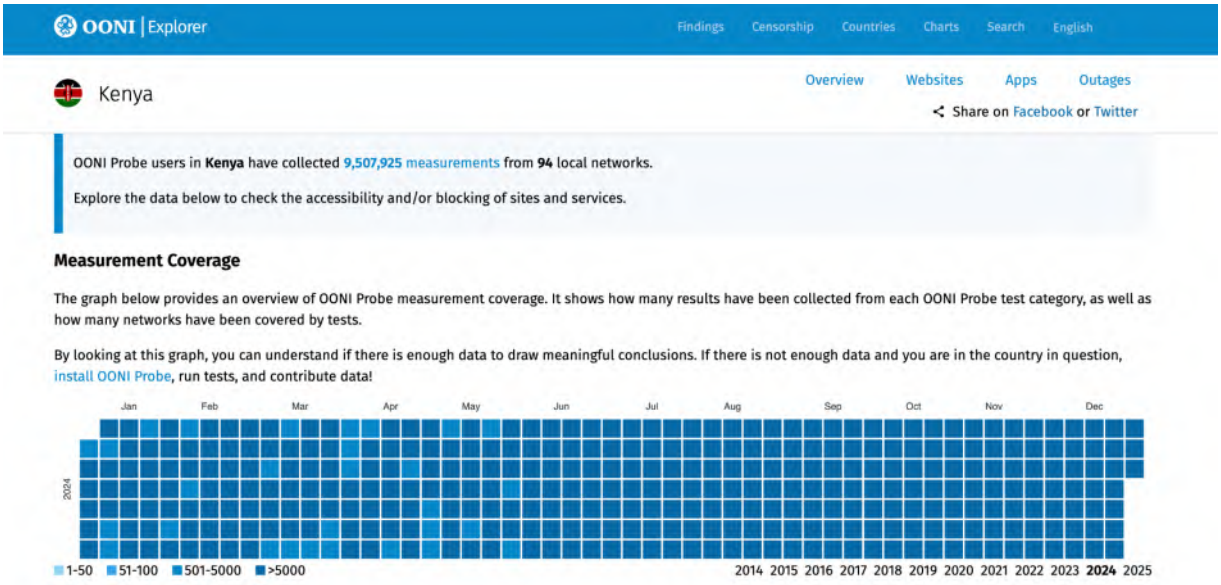


Chart: Overall OONI measurement coverage aggregated from all tested networks in Kenya between January 2024 to December 2024 (source: OONI Explorer).

The charts above show stable OONI measurement coverage throughout both years, with a notable increase in coverage in 2024 compared to 2023. The stable and relatively high volume of measurements during the periods of interest helps instill confidence in the blocking findings, as it statistically reduces the likelihood of false positives caused by transient network failures.

Findings: Blocking of Telegram in Kenya during 2023 and 2024 KCSE exams

Access to Telegram was intermittently blocked in Kenya in November 2023 amid the Kenya Certificate of Secondary Education (KCSE) national exams. As examination papers were allegedly leaked on Telegram, access to Telegram may have been blocked in an attempt to prevent exam cheating. The timing of the disruption was reportedly limited to daytime hours (when exams were in session), as Telegram was accessible at night (outside of exam hours) during this period. Kenya's Communications Authority (CA) does not appear to have publicly acknowledged or verified this disruption.

Similarly, access to Telegram was blocked again in Kenya the following year during the 2024 KCSE exams. The block was reportedly requested by the Communications Authority of Kenya (CA) to prevent cheating during the national exams. An order by the Communications Authority of Kenya (dated 31st October 2024) specifies that while other social media platforms operating in Kenya took steps to address misuse, Telegram remained non-responsive and continued to host "offending forums and channels" in breach of Kenyan laws and data protection principles, and in interference with the integrity of the national examinations. In response, the Communications Authority of Kenya directed all mobile network operators to suspend Telegram services between 7am to 10am, and between 1pm to 4pm from Monday until Friday up until 22nd November 2024 – all of which coincided with the dates and timings of the 2024 KCSE exams.

The following sections share OONI data on the blocking of Telegram during the 2023 KCSE exams and 2024 KCSE exams.

2023 KCSE exams: Blocking of Telegram in Kenya

In November 2023, OONI data presented signs of Telegram blocking in Kenya for the first time. Even though OONI data has been collected from Kenya since 2016, the data had not shown strong signals pertaining to the blocking of social media or instant messaging apps in the country before. In fact, OONI even published a report in the past documenting that they had found almost no signs of Internet censorship in Kenya.

Telegram was tested in Kenya with both the OONI Probe Web Connectivity experiment (designed to measure the blocking of websites) and with the dedicated OONI Probe Telegram experiment (designed to measure the blocking of the Telegram app and web version). OONI measurements collected from both experiments present signs of Telegram blocking on some tested networks in Kenya in November 2023.

The hypothesis that Telegram was down globally – as opposed to being blocked locally in Kenya by ISPs – is ruled out because global OONI measurement coverage pertaining to the testing of Telegram shows that the Telegram app was mostly accessible on tested networks in most countries globally between 1st October 2023 to 31st December 2023 (which includes the November 2023 KCSE exam period), as illustrated below.

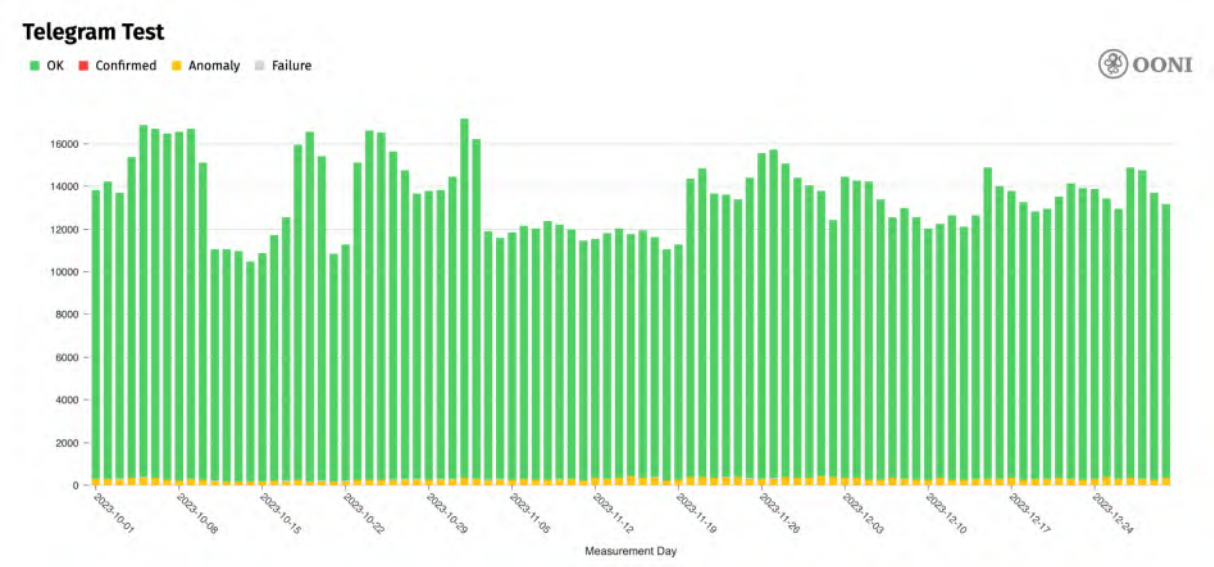


Chart: Global OONI Probe testing of Telegram between 1st October 2023 to 31st December 2023 (source: OONI data).

The above chart shows global OONI measurement coverage pertaining to the testing of Telegram app endpoints and Telegram Web (web.telegram.org). If Telegram were down globally, the above chart would have presented a large volume of measurements annotated as "anomalous" because attempted TCP connections to the Telegram app endpoints would have failed globally. Instead, the above chart shows that most measurements were "OK", meaning that it was possible to successfully establish TCP connections to Telegram app endpoints from thousands of networks in most countries around the world. Telegram therefore seemed to work globally during the 2023 KCSE exams, suggesting that any restrictions were imposed locally.

Blocking of Telegram website

The following chart aggregates OONI measurement coverage from the OONI Probe Web Connectivity testing of Telegram's website (telegram.org) on multiple networks in Kenya between 15th October 2023 to 15th December 2023.

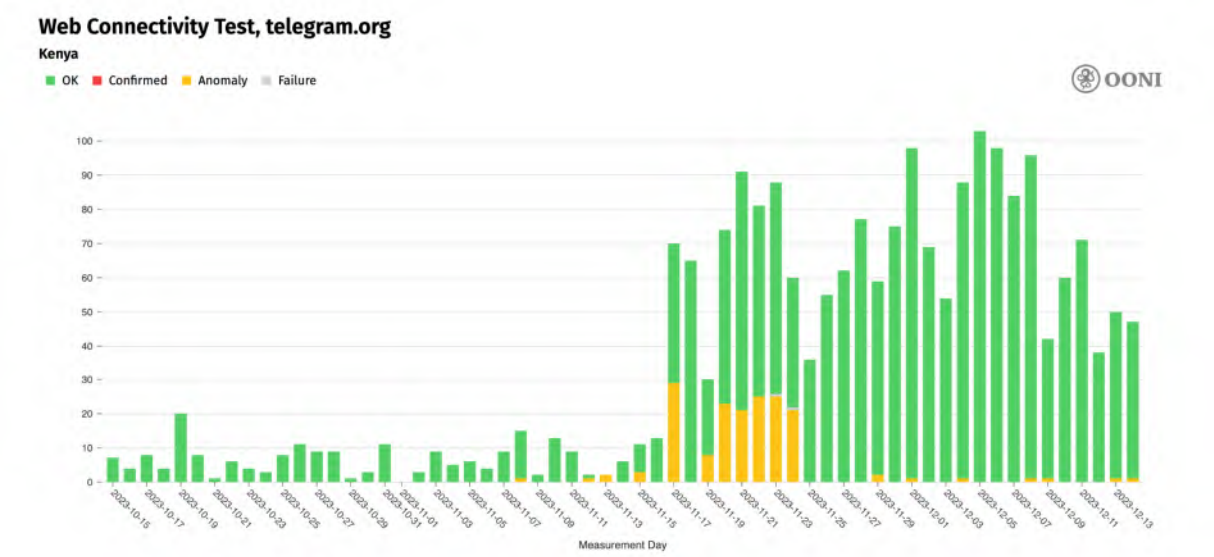


Chart: OONI Probe Web Connectivity testing of telegram.org on multiple networks in Kenya between 15th October 2023 to 15th December 2023 (source: OONI data).

As is evident from the above chart, most OONI measurements between October 2023 to December 2023 showed that telegram.org was accessible on tested networks in Kenya (as annotated in green), while measurements mainly presented anomalies (annotated in orange) between 17th November 2023 to 24th November 2023. While those anomalous measurements could present signs of Telegram blocking, it's worth highlighting that the availability of successful measurements during the same dates (between 17th to 24th November 2023) suggest that if access to telegram.org was blocked, it was *not* blocked continuously, and/or that it was *not* blocked on all networks.

A similar pattern is observed when looking at OONI measurements collected from the OONI Probe Telegram experiment on multiple networks in Kenya during the same period (15th October 2023 to 15th December 2023), as illustrated below.

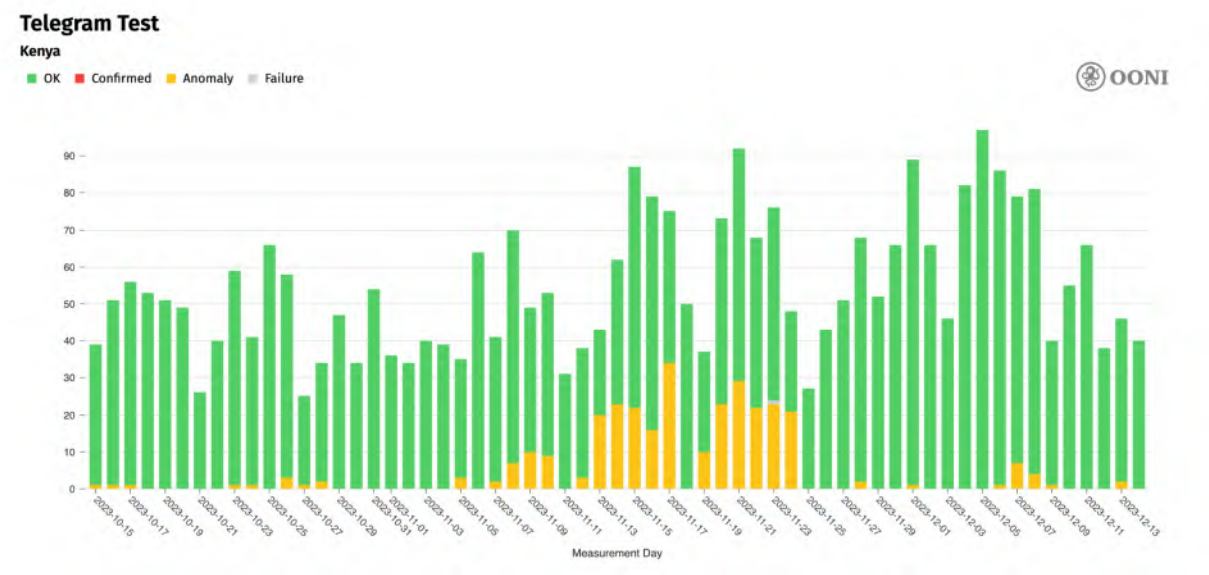


Chart: OONI Probe testing of Telegram on multiple networks in Kenya between 15th October 2023 to 15th December 2023 (source: OONI data).

In both cases demonstrated in the above two charts, there is a spike in anomalous measurements during the same period, but those anomalies are not persistent, as many measurements during the same period were successful. OONI therefore analyzed these anomalous measurements to determine what caused them, and if they were symptomatic of censorship.

The following chart illustrates the results of OONI's analysis of the Web Connectivity testing of telegram.org in Kenya, demonstrating that most anomalous measurements presented timeout errors after the ClientHello message during the TLS handshake.

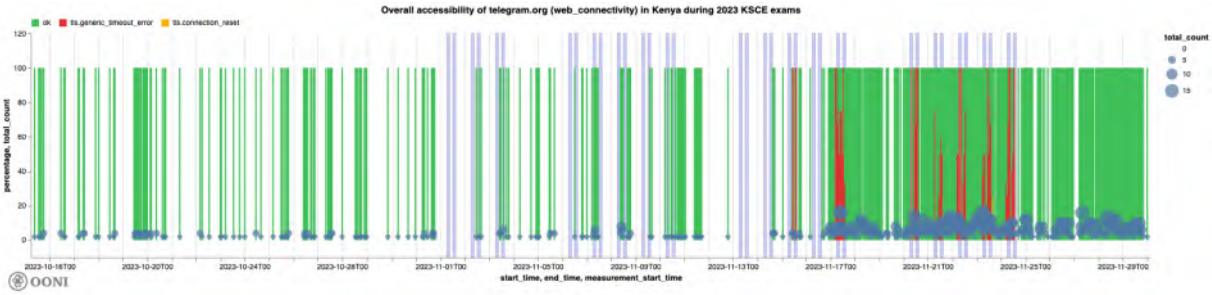


Chart: Aggregated results from the OONI Probe Web Connectivity testing of telegram.org on multiple networks in Kenya between 16th October 2023 to 29th November 2023 (source: OONI data).

While the first anomalous measurement is from 8th November 2023, this signal was quite weak given the relatively limited measurement coverage and presence of successful measurements. OONI therefore focused their analysis of Web Connectivity measurements from 10th November 2023 onwards (two days prior to the first case of true blocking).

OONI measurements during this period were collected on a total of 19 networks, listed below.

Probe ASN	Probe AS organization name	Observation count
33771	Safaricom Limited	1050
36866	Jamii Telecommunications Limited	646
30844	Liquid Telecommunications Ltd	284
37061	Safaricom Limited	264
15808	ACCESSKENYA GROUP LTD is an ISP serving	160
15399	Wananchi Group (Kenya) Limited	156
12455	Jambonet Autonomous System	150
329014	Vilcom Networks Limited	140
329183	FLINK TECHNOLOGIES LTD	80
329211	Novia East Africa Ltd	36
36926	Airtel Networks Kenya Limited	34
328993	Click Fiber Communications Limited	30
37305	Frontier Optical Networks Ltd	22
329205	VUMA FIBER LIMITED	16
328977	Wavex Internet Service Provider LTD	8
328856	VIJIJI CONNECT LIMITED	6
328475	AFRIQ NETWORK SOLUTIONS LIMITED	4
13335	Cloudflare Inc	4
329044	Surf Net Solutions Limited	4

OONI decided, however, to limit their analysis to measurements collected from networks that provided sufficient coverage for the relevant time period.

In the following charts, OONI placed an overlay on top of the rate of anomalous measurements which indicates the times at which the 2023 KCSE exams occurred based on the official government issued timetable. While the official government letter requesting ISPs in Kenya to block access to Telegram in 2023 does not appear to be publicly available, the leaked letter from 2024 mentions that all ISPs in Kenya should block access to Telegram between 7am to 10am, and between 1pm to 4pm (from Monday until Friday, up until 22nd November 2024) – which correlates with the timings of the 2024 KCSE exams. This suggests that the blocking of

Telegram during the 2023 KCSE exams may have similarly taken place on weekdays from 07:00 to 10:00 local time (04:00 - 07:00 UTC), and then from 13:00 to 16:00 local time (10:00 - 13:00 UTC) between 1st November 2023 to 24th November 2023.

All the following charts are based on the analysis of OONI Probe Web Connectivity measurements pertaining to the testing of telegram.org and are limited to the Telegram IP address 149.154.167.99. The analysis was limited to Telegram's IPv4 address because the data shows a lack of IPv6 connectivity in the tested networks and, therefore, the measurements for the IPv6 endpoints are not relevant to the analysis.

On the Safaricom network (AS33771), OONI data shows TLS level blocking where connections timeout after the ClientHello message during the TLS handshake. This behaviour is consistent with what would be observed when Deep Packet Inspection (DPI) technology is being used.

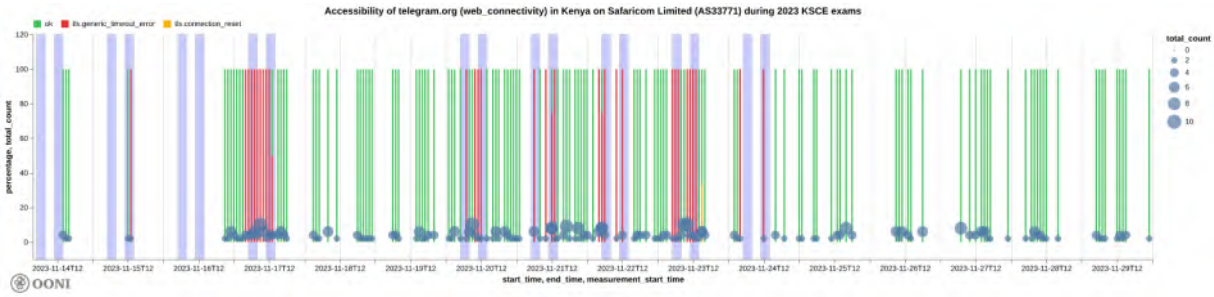


Chart: Analysis of OONI Probe Web Connectivity testing of telegram.org on Safaricom (AS33771) in Kenya during the 2023 KCSE exam period (source: OONI data).

A similar blocking technique also seems to be used on Airtel (AS36926), where anomalous measurements also present connection timeouts during the TLS handshake (illustrated below), though the measurement coverage is much more limited (in comparison to measurements collected on Safaricom).

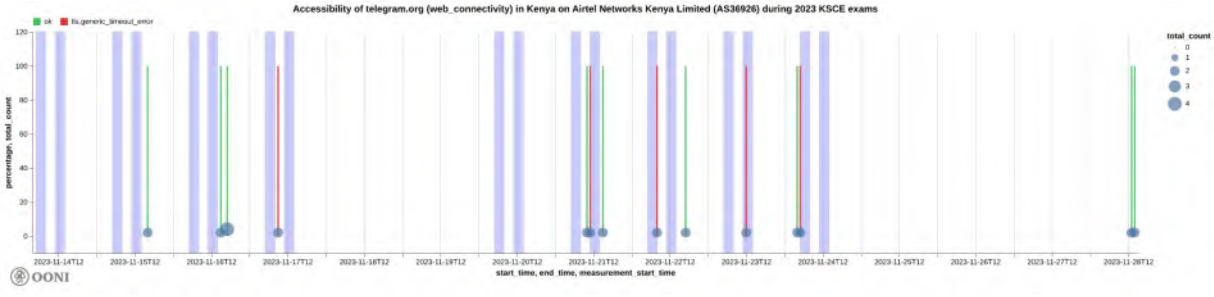


Chart: Analysis of OONI Probe Web Connectivity testing of telegram.org on Airtel (AS36926) in Kenya during the 2023 KCSE exam period (source: OONI data).

On the Jambonet network (AS12455), however, OONI data suggests a different blocking technique, as the blocking of telegram.org appears to be implemented at the DNS level (illustrated below).

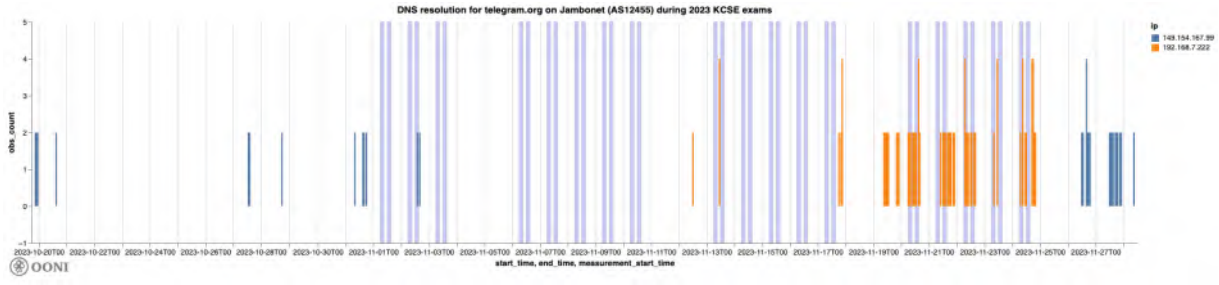


Chart: Analysis of OONI Probe Web Connectivity testing of telegram.org on Jambonet (AS12455) in Kenya during the 2023 KCSE exam period (source: OONI data).

When looking at the DNS resolutions performed by a probe on the Jambonet network (AS12455) using the ISP-provided resolver, OONI data shows that telegram.org resolves to 192.168.7.222, which is a bogon IP address. OONI data shows that this behavior persists even outside of the exam hours. For example, an OONI measurement shows the DNS-based blocking of telegram.org at 18:36 UTC (which is 21:36 local time) on 24th November 2023 on the Jambonet network (AS12455).

Overall, OONI Web Connectivity data shows that, in November 2023, access to the web resource "https://telegram.org" was blocked in Kenya through the following methods:

- **TLS interference.** On the Safaricom (AS33771) and Airtel (AS36926) networks, OONI data shows the timing out of the session after the ClientHello message during the TLS handshake (in most anomalous measurements pertaining to the testing of telegram.org).
- **DNS tampering.** On the Jambonet network (AS12455), OONI data shows that DNS resolution for the testing of telegram.org returned an IP address in local IP space (192.168.7.222), instead of the actual IP address for telegram.org.

Blocking of Telegram Web

OONI data collected from the OONI Probe Telegram experiment shows similar patterns and results. When looking at the overall failures for Telegram Web (web.telegram.org) based on the Telegram test results, OONI data shows that these failures started on 8th November 2023 and ended on 24th November 2023 (as illustrated below).

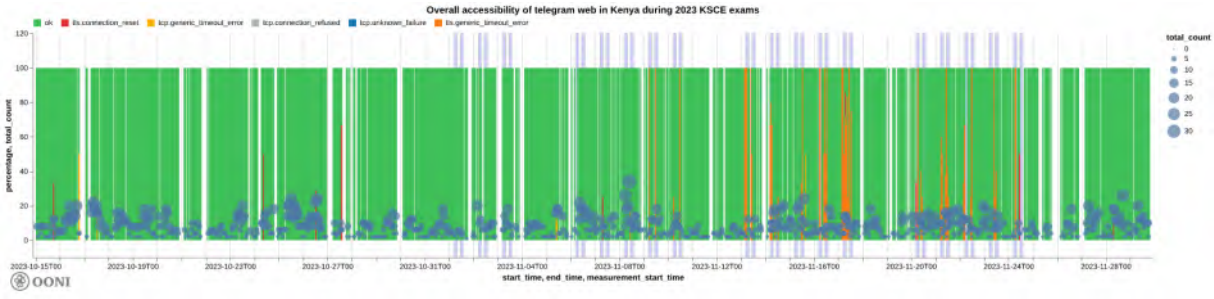


Chart: Analysis of OONI Probe Telegram measurements pertaining to the testing of Telegram Web (web.telegram.org) on multiple networks in Kenya between 15th October 2023 to 29th November 2023 (source: OONI data).

Similar to what was observed in the testing of the Telegram web resource (telegram.org), OONI data shows that Safaricom and Airtel blocked access to Telegram Web (web.telegram.org) by means of TLS interference. Specifically, OONI data shows TLS level blocks affecting the IP address 149.154.167.99 (which is the IP of the Telegram web application) on the networks in the following charts.

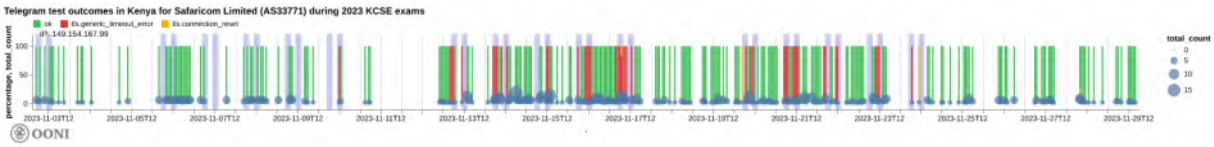


Chart: Analysis of OONI Probe Telegram measurements on Safaricom (AS33771) in Kenya during the 2023 KCSE exam period, demonstrating the TLS level blocking of Telegram Web (source: OONI data).

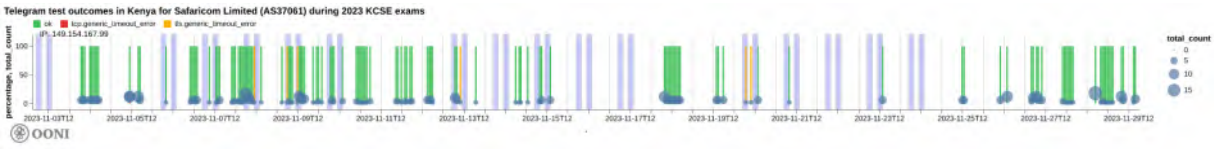


Chart: Analysis of OONI Probe Telegram measurements on Safaricom (AS37061) in Kenya during the 2023 KCSE exam period, demonstrating the TLS level blocking of Telegram Web (source: OONI data).

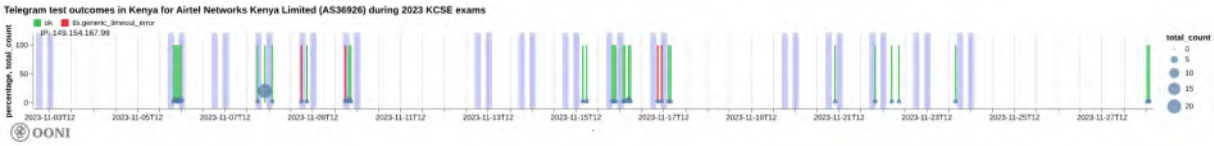


Chart: Analysis of OONI Probe Telegram measurements on Airtel (AS36926) in Kenya during the 2023 KCSE exam period, demonstrating the TLS level blocking of Telegram Web (source: OONI data).

Blocking of Telegram app endpoints

The OONI Probe Telegram experiment measures the reachability of the endpoints used by the Telegram application. This means that it's a more accurate representation of what the Telegram

application would really be attempting to connect to when in use, as opposed to just checking if the website or web application are accessible (as measured with the OONI Probe Web Connectivity experiment discussed previously).

When looking at the rate of failures for accessing the Telegram endpoints across all tested networks in Kenya between 15th October 2023 to 29th November 2023, OONI data (illustrated below) shows that the first consistent failures emerged around 8th November 2023 (which correlates with the timing of when the first anomalies appeared in the testing of telegram.org), with most failures occurring in the week leading up to 24th November 2023 (the last day of the 2023 KCSE exams).

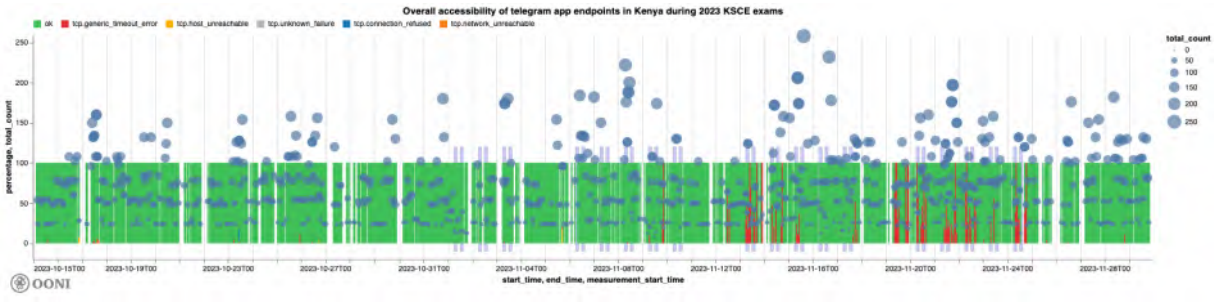


Chart: Analysis of OONI Probe Telegram measurements collected from multiple networks in Kenya between 15th October 2023 to 29th November 2023, demonstrating the overall failure rate of accessing Telegram app endpoints (source: OONI data).

Even though the above chart is based on aggregate measurements collected from the OONI Probe Telegram experiment and pertaining to the testing of Telegram endpoints, the patterns in this chart are similar to those observed in charts discussed previously, pertaining to the testing of telegram.org with the OONI Probe Web Connectivity experiment. Specifically, there are two main similarities: (1) Presence of anomalies/failures between 8th to 24th November 2023 (with the first anomalies emerging on 8th November 2023), which correlates with the dates of the 2023 KCSE exams, (2) Presence of successful measurements, indicating the *intermittent* nature of the block, and that the block was *not* implemented on all tested networks.

Of all tested networks, OONI data shows that only Jambonet (AS12455) seems to have implemented IP level blocking of Telegram endpoints, as can be observed through the following chart.

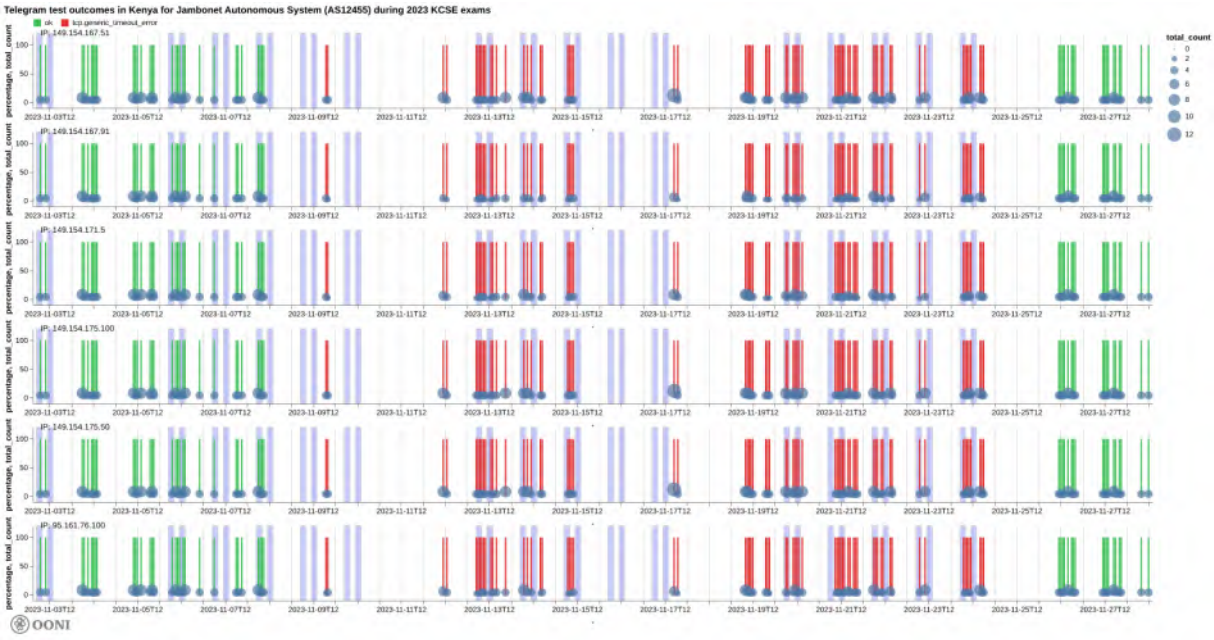


Chart: Analysis of OONI Probe Telegram measurements showing the IP level blocking of Telegram endpoints on the Jambonet network (AS12455) in Kenya in November 2023 (source: OONI data).

As can be observed in the above chart, all of the tested Telegram endpoints consistently presented timeout errors between 8th November 2023 to 24th November 2023, providing a strong signal of IP level blocking on this network (Jambonet). It's worth noting that OONI data shows that the blocking of Telegram also occurred outside of the time period of the 2023 KCSE national exams, such as during the weekend and outside of exam hours. OONI data does not show any other network beyond AS12455 implementing TCP level blocks affecting the Telegram endpoints.

2024 KCSE exams: Blocking of Telegram in Kenya

Access to Telegram was blocked again in Kenya the following year during the 2024 KCSE exams. The block was reportedly requested by the Communications Authority of Kenya (CA) to prevent cheating during the national exams.

An order by the Communications Authority of Kenya (dated 31st October 2024) specifies that while other social media platforms operating in Kenya took steps to address misuse, Telegram remained non-responsive and continued to host "offending forums and channels" in breach of Kenyan laws and data protection principles, and in interference with the integrity of the national examinations. In response, the Communications Authority of Kenya directed all mobile network operators to suspend Telegram services between 7am to 10am, and between 1pm to 4pm from Monday until Friday up until 22nd November 2024 – all of which correlated with the dates and timings of the 2024 KCSE exams.

Telegram was tested in Kenya with both the OONI Probe Web Connectivity experiment (designed to measure the blocking of websites) and with the dedicated OONI Probe Telegram experiment (designed to measure the blocking of the Telegram app and web version). OONI measurements collected from both experiments present signs of Telegram blocking on some tested networks in Kenya in November 2024.

The hypothesis that Telegram was down globally – as opposed to being blocked locally in Kenya by ISPs – is ruled out because global OONI measurement coverage pertaining to the testing of Telegram shows that the Telegram app was mostly accessible on tested networks in most countries globally between 1st October 2024 to 31st December 2024 (which includes the November 2024 KCSE exam period), as illustrated below.

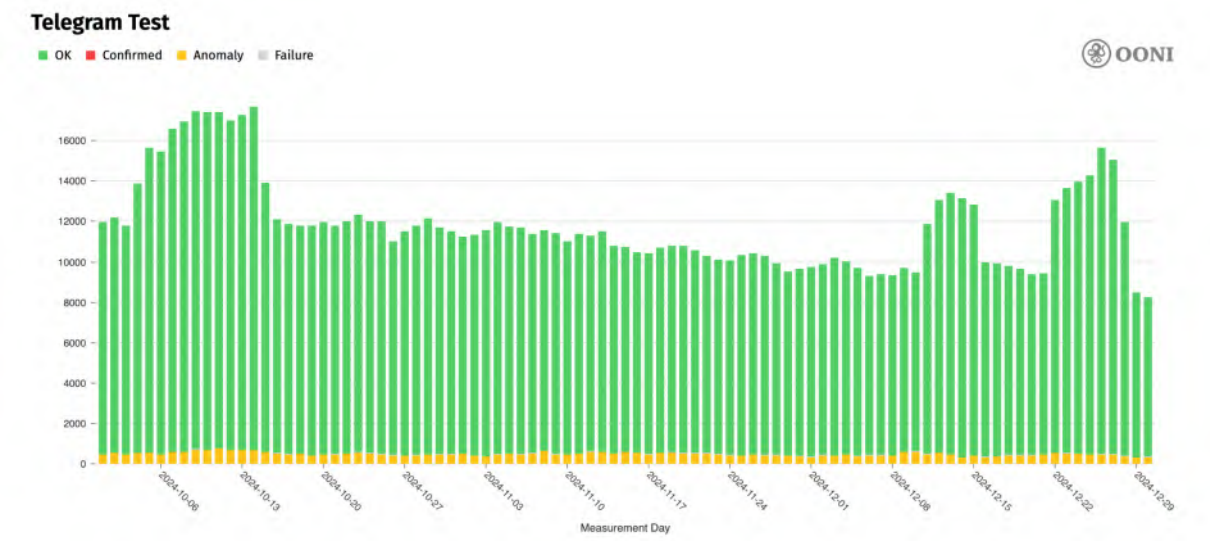


Chart: Global OONI Probe testing of Telegram between 1st October 2024 to 31st December 2024 (source: OONI data).

The above chart shows global OONI measurement coverage pertaining to the testing of Telegram app endpoints and Telegram Web (web.telegram.org). If Telegram were down globally, the above chart would have presented a large volume of measurements annotated as "anomalous" because attempted TCP connections to the Telegram app endpoints would have failed globally. Instead, the above chart shows that most measurements were "OK", meaning that it was possible to successfully establish TCP connections to Telegram app endpoints from thousands of networks in most countries around the world. Telegram therefore seemed to work globally during the 2024 KCSE exams, suggesting that any restrictions were imposed locally.

Blocking of Telegram website

The following chart aggregates OONI measurement coverage from the OONI Probe Web Connectivity testing of Telegram's website (telegram.org) on multiple networks in Kenya between 15th October 2024 to 15th December 2024.

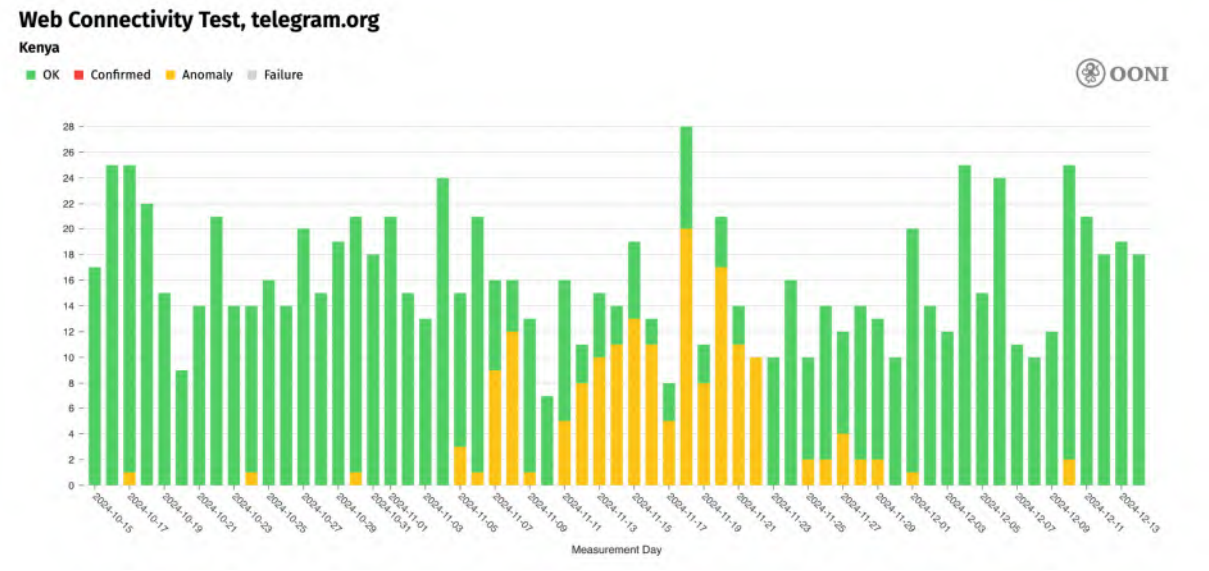


Chart: OONI Probe Web Connectivity testing of telegram.org on multiple networks in Kenya between 15th October 2024 to 15th December 2024 (source: OONI data).

As is evident from the above chart, OONI measurements from the Web Connectivity testing of telegram.org presented a substantial volume of anomalies between 7th November 2024 to 22nd November 2024 (which correlates with the last day of the 2024 KCSE exams), suggesting that access to telegram.org was mostly blocked on tested networks during this period. The presence of anomalies before 7th November 2024 and after 22nd November 2024 suggest that access to telegram.org may have been blocked on a few networks beyond this date range.

A similar pattern is observed when looking at OONI measurements collected from the OONI Probe Telegram experiment on multiple networks in Kenya during the same period (15th October 2024 to 15th December 2024), as illustrated below.

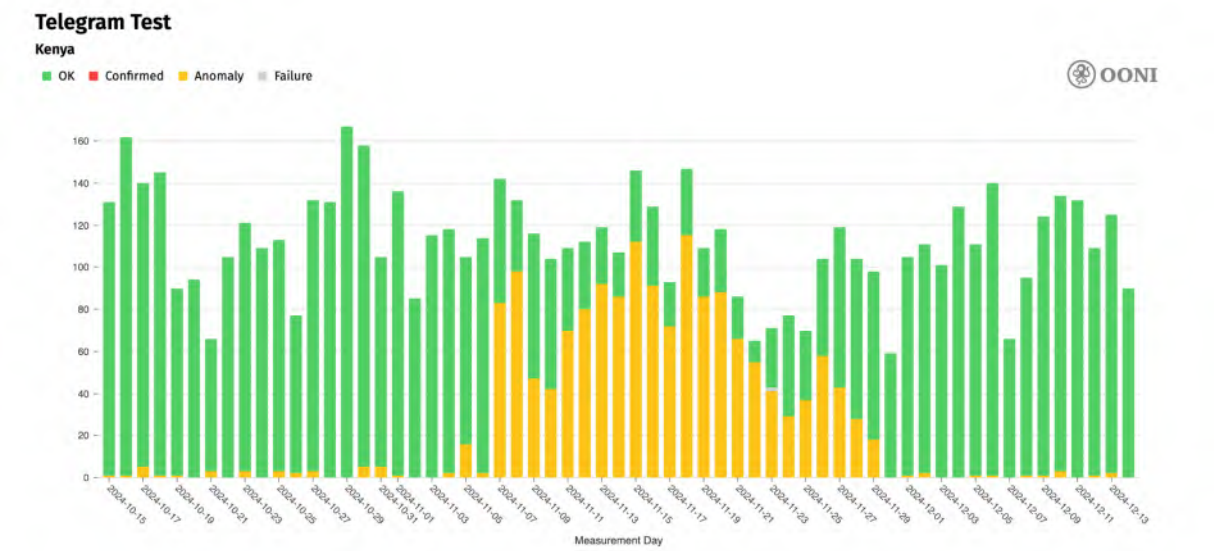


Chart: OONI Probe testing of Telegram on multiple networks in Kenya between 15th October 2024 to 15th December 2024 (source: OONI data).

In both cases demonstrated in the above two charts, there is a substantial volume of anomalous measurements during the same period, suggesting that access to Telegram was blocked on tested networks in Kenya. OONI analyzed these anomalous measurements to determine what caused them, and if they were symptomatic of censorship.

The following chart illustrates the results of OONI's analysis of the Web Connectivity testing of telegram.org in Kenya, demonstrating that most anomalous measurements presented TCP/IP timeout errors (annotated in red in the chart below).

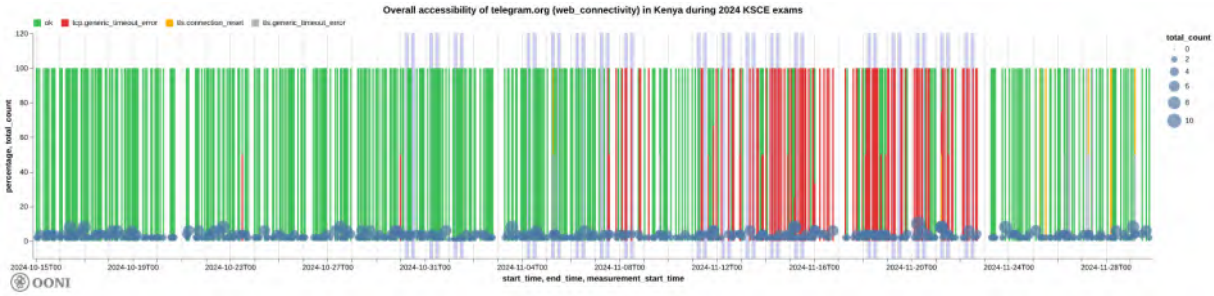


Chart: Aggregated results from the OONI Probe Web Connectivity testing of telegram.org on multiple networks in Kenya between 15th October 2024 to 29th November 2024 (source: OONI data).

OONI further limited their analysis to the networks which received the largest measurement coverage and volume of anomalies: two Safaricom networks (AS33771, AS37061).

On Safaricom (AS33771), OONI data shows that the blocking of telegram.org appears to have begun on 11th November 2024 and lasted up until 22nd November 2024.

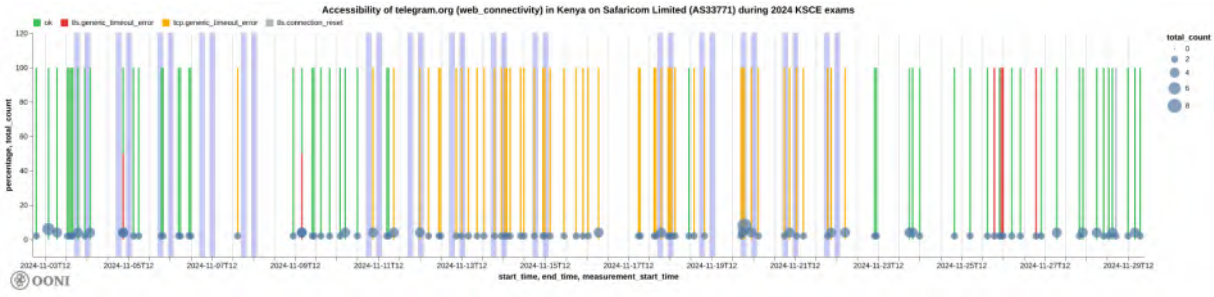


Chart: Analysis of OONI Probe Web Connectivity testing of telegram.org on Safaricom (AS33771) in Kenya during the 2024 KCSE exam period (source: OONI data).

Most anomalous measurements presented TCP/IP timeout errors, suggesting that access to telegram.org was blocked at an IP level on Safaricom (AS33771) during the 2024 KCSE exams. It's worth noting that the block seemed to also persist outside of the exam hours and throughout the weekend, even though ISPs were only instructed to block access to Telegram on weekdays during the exam hours.

On another Safaricom network (AS37061), OONI data shows a similar pattern with most anomalies presenting TCP/IP timeout errors, but the block seems to have started earlier (on 7th November 2024) and to have been paused during the weekend of 9th November 2024, but *not* during the weekend of 16th November 2024.

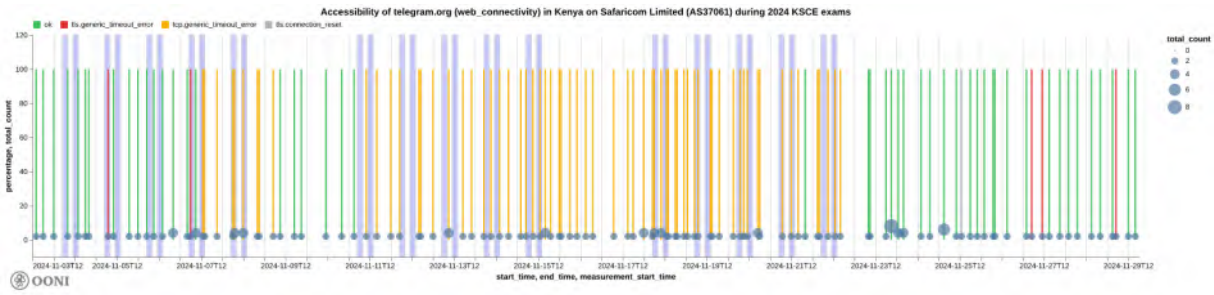


Chart: Analysis of OONI Probe Web Connectivity testing of telegram.org on Safaricom (AS37061) in Kenya during the 2024 KCSE exam period (source: OONI data).

Other tested networks are excluded from the analysis either because they did not present significant signs of telegram.org blocking, or because the measurement coverage was too limited to determine if telegram.org blocking occurred during the 2024 KCSE exam period.

Blocking of Telegram app endpoints

The OONI Probe Telegram experiment measures the reachability of the endpoints used by the Telegram application. This means that it's a more accurate representation of what the Telegram application would really be attempting to connect to when in use, as opposed to just checking if the website is accessible (as measured with the OONI Probe Web Connectivity experiment discussed previously).

When looking at the results for the Telegram app endpoints in aggregate, it is evident that access to Telegram was interfered with during the 2024 KCSE exam period. Specifically, the following chart presents aggregate results from the OONI Probe testing of Telegram app endpoints on multiple networks in Kenya, illustrating that the testing of Telegram app endpoints started presenting failures on 7th November 2024, and that this spike in failures continued until 22nd November 2024 (which correlates with the last day of the 2024 KCSE exams).

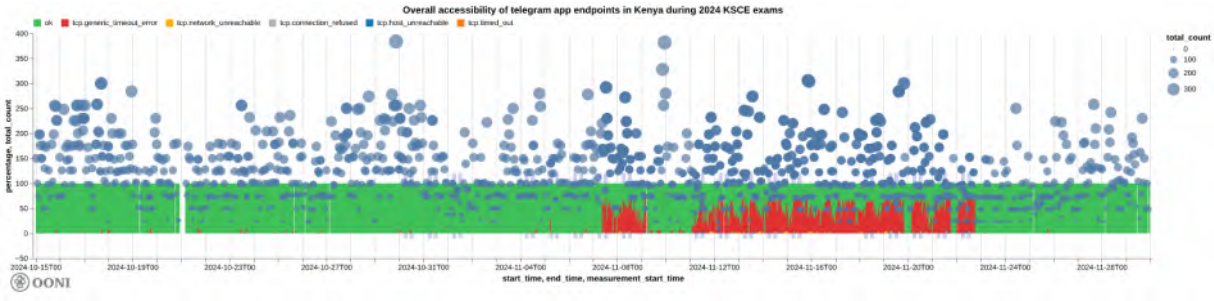


Chart: Analysis of OONI Probe Telegram measurements collected from multiple networks in Kenya between 15th October 2024 to 29th November 2024, demonstrating the overall failure rate of accessing Telegram app endpoints (source: OONI data).

The aggregate findings presented in the above chart suggest that Telegram app endpoints were mainly blocked between 7th to 22nd November 2024, which correlates both with the timing of the 2024 KCSE exams, and with the dates during which access to telegram.org was blocked (discussed previously). Out of all tested networks, OONI further limited their analysis to the networks which received the largest measurement coverage and strongest signals of Telegram app endpoint blocking throughout November 2024: Jambonet (AS12455) and Safaricom (AS33771 and AS37061).

On Jambonet (AS12455), OONI data shows consistent failures to establish TCP connections to all measured Telegram endpoints, which coincide with the timing of the 2024 KCSE national exams. It's worth noting though that access to these endpoints was restored outside of the exam hours.

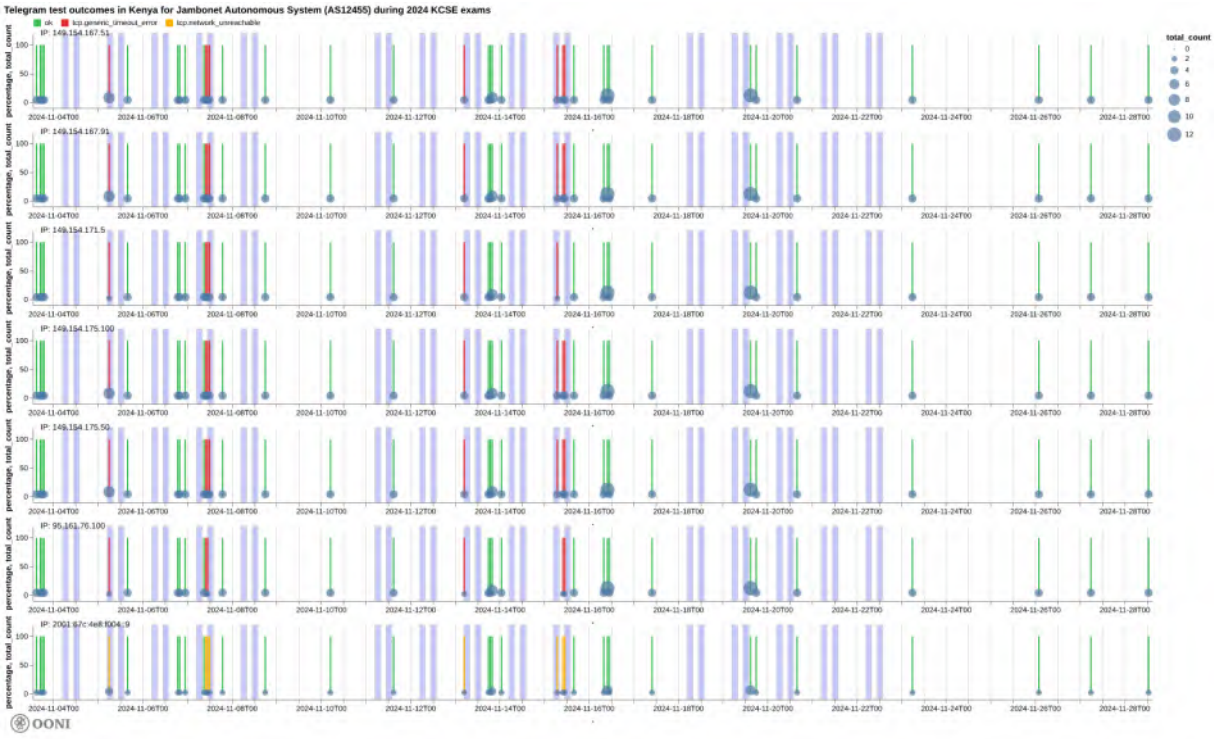


Chart: Analysis of OONI Probe Telegram measurements showing the IP level blocking of Telegram endpoints on the Jambonet network (AS12455) in Kenya in November 2024 (source: OONI data).

On Safaricom (AS33771), on the other hand, OONI data shows the blocking of all but 2 Telegram endpoints (149.154.175.100 and 149.154.175.50). The blocking of Telegram app endpoints on this network appears to be present even outside of the hours of the national exams (for example, during the weekend).

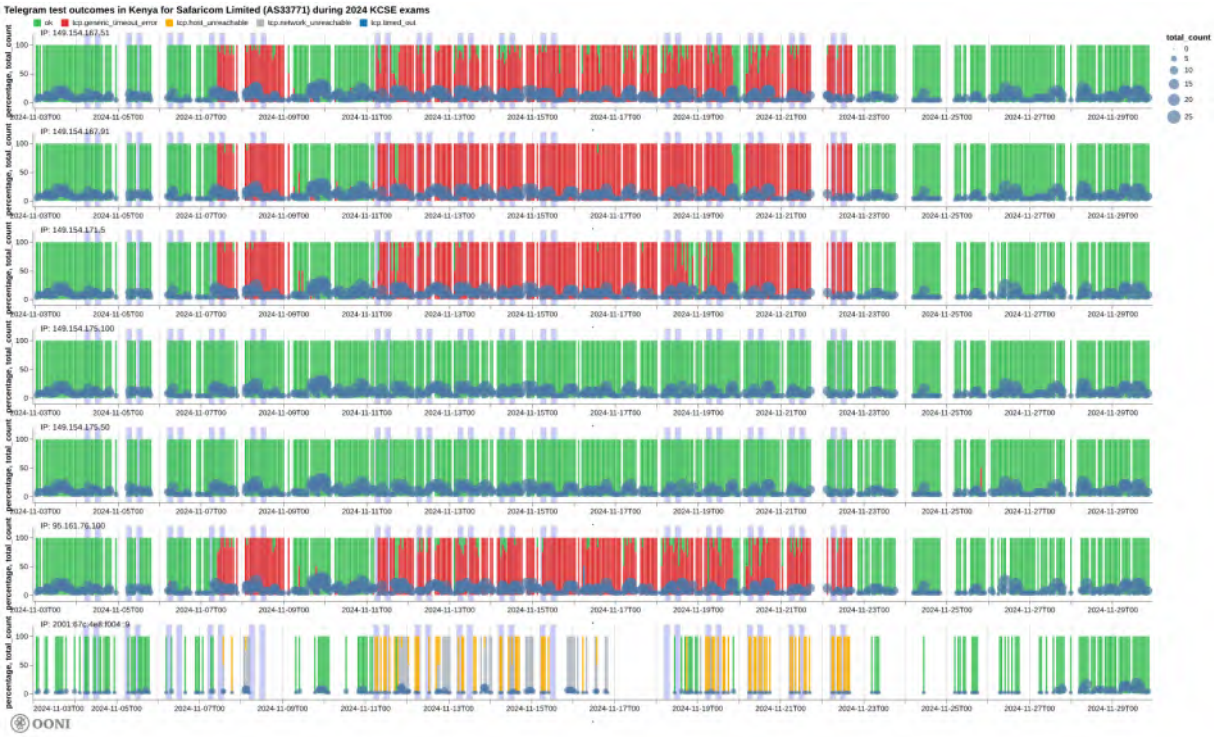


Chart: Analysis of OONI Probe Telegram measurements showing the IP level blocking of Telegram endpoints on the Safaricom network (AS33771) in Kenya in November 2024 (source: OONI data).

The same pattern is also observed on the other Safaricom network (AS37061), illustrated in the chart below. The fact that two Telegram app endpoints were not blocked on Safaricom networks may suggest that users might still have been able to use the Telegram app, even when the block was ongoing.

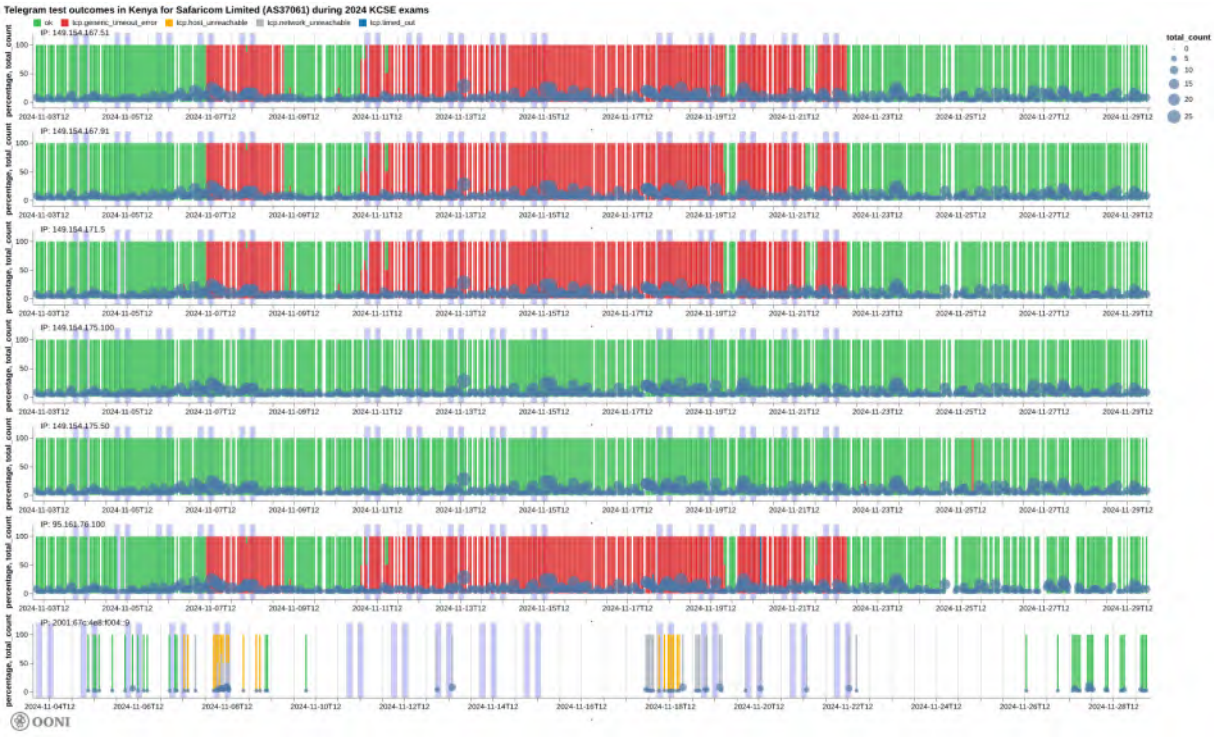


Chart: Analysis of OONI Probe Telegram measurements showing the IP level blocking of Telegram endpoints on the Safaricom network (AS37061) in Kenya in November 2024 (source: OONI data).

Blocking of Telegram Web

Beyond the testing of Telegram app endpoints, the OONI Probe Telegram experiment also measures the accessibility of Telegram Web (web.telegram.org). In both cases, OONI measurements show consistent patterns in terms of the timing of IP level blocks.

Specifically, when looking at aggregate OONI measurements from the testing of Telegram Web (web.telegram.org) on all tested networks in Kenya, it is evident that there is a spike in failures between 7th November 2024 to 22nd November 2024. These failures (annotated in red in the chart below) are TCP/IP timeout errors, suggesting IP level blocking of Telegram Web.

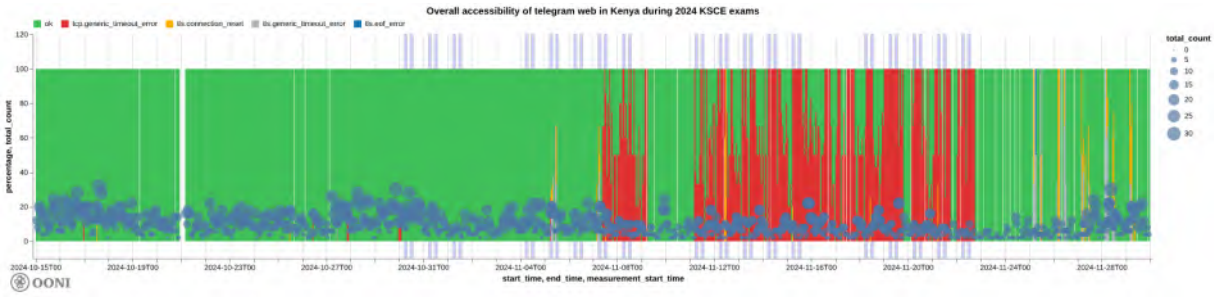


Chart: Analysis of OONI Probe Telegram measurements pertaining to the testing of Telegram Web (web.telegram.org) on multiple networks in Kenya between 15th October 2024 to 29th November 2024 (source: OONI data).

While the blocking of Telegram Web appears to have persisted until the last day of the 2024 KCSE exams (22nd November 2024), it's worth noting that web.telegram.org was found accessible on tested networks over the weekend (9th and 10th November 2024), suggesting that the block was limited to the exam days. And while the IP level block appears to have been lifted after the end of the exam period, OONI data shows that some measurements thereafter presented signs of TLS level interference.

On Safaricom networks (AS33771 and AS37061), the blocking pattern for Telegram Web is consistent with what was observed for Telegram app endpoints, where the block is implemented at the IP level. The following two charts demonstrate that the majority of anomalous measurements pertaining to the testing of web.telegram.org on Safaricom networks throughout November 2024 presented TCP/IP timeout errors, providing a strong signal of IP level blocks.

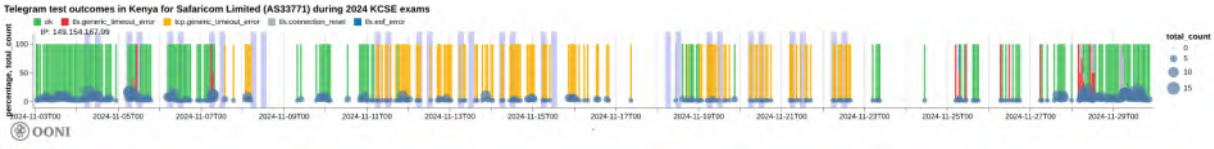


Chart: Analysis of OONI Probe Telegram measurements on Safaricom (AS33771) in Kenya during the 2024 KCSE exam period, demonstrating IP level blocking of Telegram Web (source: OONI data).

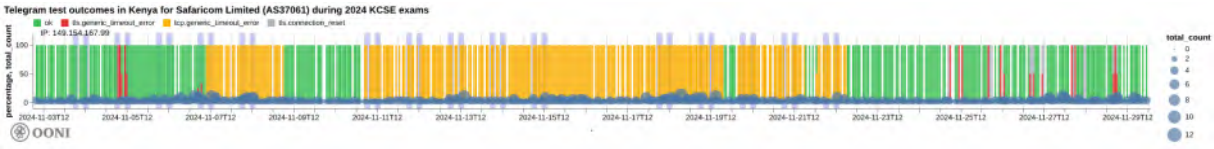


Chart: Analysis of OONI Probe Telegram measurements on Safaricom (AS37061) in Kenya during the 2024 KCSE exam period, demonstrating IP level blocking of Telegram Web (source: OONI data).

Similarly, OONI data suggests IP level blocking of Telegram Web on Jambonet (AS12455), as anomalous measurements present TCP/IP timeout errors.

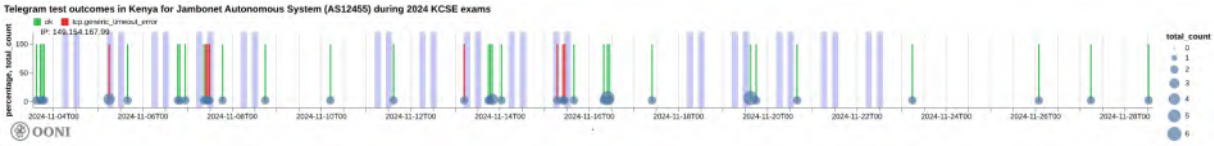


Chart: Analysis of OONI Probe Telegram measurements on Jambonet (AS12455) in Kenya during the 2024 KCSE exam period, demonstrating IP level blocking of Telegram Web (source: OONI data).

On Jamil (AS36866), however, OONI data suggests that the blocking of web.telegram.org was implemented at the TLS level because the connection was reset after the ClientHello message during the TLS handshake. However, it's worth noting though that very few measurements are available that overlap with the 2024 KCSE exam hours, limiting the findings.

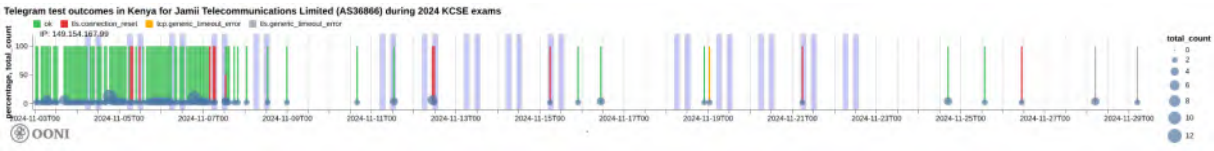


Chart: Analysis of OONI Probe Telegram measurements on Jamil Telecommunications (AS36866) in Kenya during the 2024 KCSE exam period, presenting signs of TLS level blocking of Telegram Web (source: OONI data).

OONI data collected from the TCP reachability testing of Telegram app endpoints on the Jamil network (AS36866) does not present any strong signs of endpoint blocking, which might suggest the use of technology to block the Telegram app through other means.

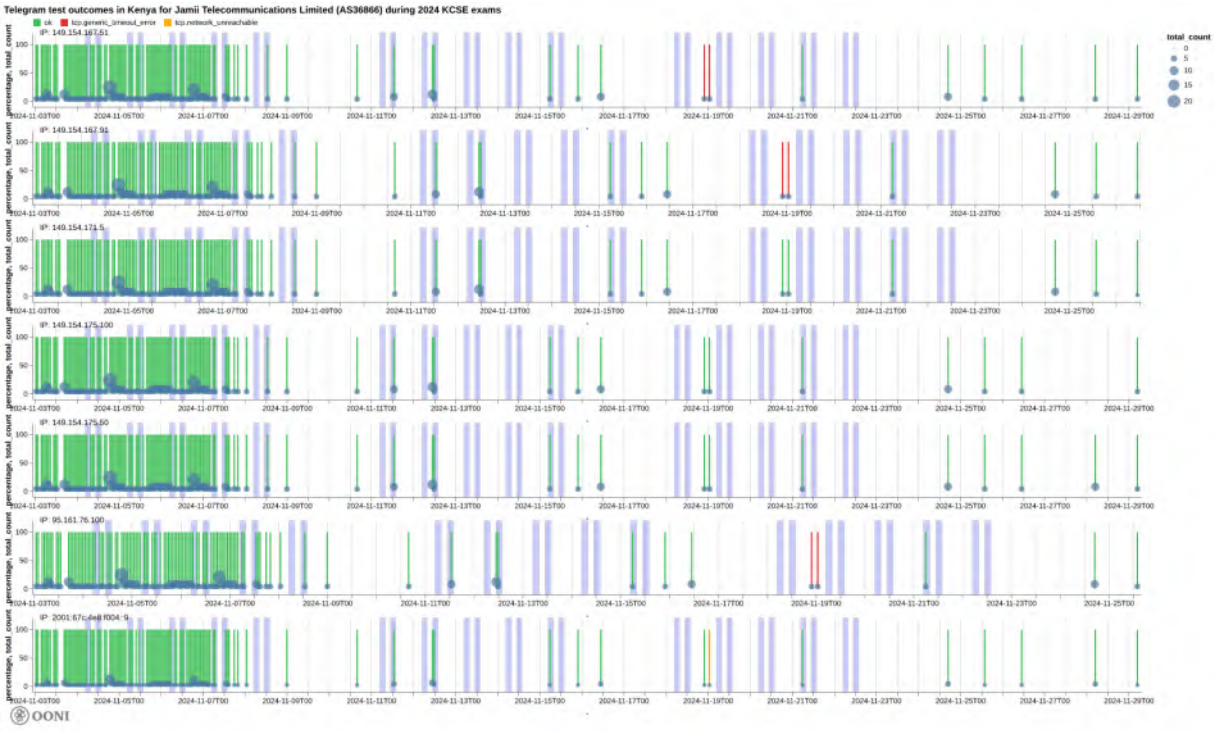


Chart: Analysis of OONI Probe Telegram measurements based on tested Telegram app endpoints on Jamil Telecommunications (AS36866) in Kenya during the 2024 KCSE exam period (source: OONI data).

Conclusion

Kenya's record of maintaining access to Internet services declined during the November 2023 and November 2024 KCSE national exams, when access to Telegram was blocked on several networks in the country.

While the blocking of Telegram in November 2023 does not appear to have been publicly acknowledged or verified by the Communications Authority (CA) of Kenya, the blocking of Telegram was reportedly requested by the authority to prevent cheating during the 2024 KCSE national exams. A leaked order by the Communications Authority of Kenya directs all mobile network operators to block access to Telegram between 7am to 10am, and between 1pm to 4pm on weekdays up until 22nd November 2024 (the last day of the 2024 KCSE exams).

During the 2023 KCSE exams, OONI data shows that access to Telegram was **intermittently blocked** on Safaricom (AS33771 and AS37061) and Airtel (AS36926), and **persistently blocked** on Jambonet (AS12455). Safaricom and Airtel blocked access to Telegram's website (telegram.org) and web interface (web.telegram.org) by means of TLS interference, while Jambonet blocked access to telegram.org by means of DNS tampering (returning a bogon IP address as part of DNS resolution). Out of all tested networks, OONI data only shows the blocking of Telegram app endpoints on Jambonet. Similarly to the blocking of telegram.org, OONI data shows that Jambonet continued to block access to Telegram endpoints outside of the time period of the 2023 KCSE national exams (such as during the weekend and outside of exam hours). The blocking of Telegram was lifted by 25th November 2023, which correlates with the end of the 2023 KCSE exams.

During the 2024 KCSE exams, OONI data shows that access to Telegram was blocked on Safaricom (AS33771 and AS37061), Jambonet (AS12455), and on Jamil Telecommunications (AS36866). The strongest signal of Telegram blocking is visible on Safaricom networks, which received the largest measurement coverage throughout November 2024. The blocking techniques are also quite different in comparison to those observed in November 2023, as OONI data shows that access to Telegram was predominantly blocked by means of **IP blocking** in November 2024. More specifically, OONI data shows IP blocking of telegram.org on Safaricom networks (AS33771 and AS37061), while access to Telegram Web (web.telegram.org) was restricted by means of IP blocking on Safaricom (AS33771 and AS37061) and Jambonet (AS12455). On Jamil Telecommunications (AS36866), however, OONI data suggests that the blocking of web.telegram.org was implemented at the TLS level.

Between 7th to 22nd November 2024, OONI data shows that access to Telegram app endpoints was blocked on the Jambonet (AS12455) and Safaricom (AS33771 and AS37061) networks. On Jambonet (AS12455), OONI data shows that *all* tested Telegram endpoints were blocked, and

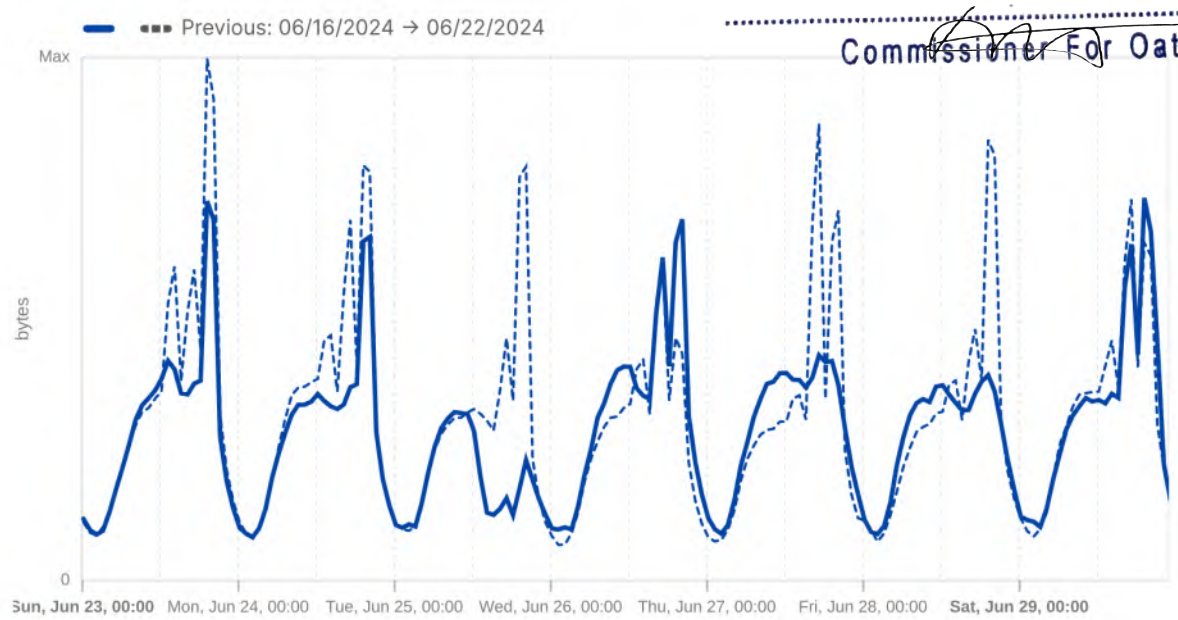
that the block was limited to exam hours. On Safaricom networks (AS33771 and AS37061), OONI data shows the blocking of most Telegram endpoints, except for two (149.154.175.100 and 149.154.175.50), and that the block persisted outside of the hours of the national exams. While the blocking of Telegram app endpoints was lifted by 23rd November 2024 (at the end of the 2024 KCSE exams, as instructed by the Communications Authority of Kenya), OONI data suggests that access to Telegram Web (web.telegram.org) remained blocked on Safaricom networks (AS33771 and AS37061) until 29th November 2024.

Overall, despite the blocking order, OONI data suggests that the blocking of Telegram was not implemented on all networks in Kenya, nor was it implemented consistently. Different ISPs blocked access to different Telegram services, using different censorship techniques. Even though the timings of the block were specified in the blocking order, in practice, these timings were not always closely followed by ISPs. In some instances, the blocking of Telegram was limited to exam hours, while in others, the block remained in place outside of exam hours and on weekends. Telegram Web remained blocked on Safaricom beyond the end of the 2024 KCSE exams. This highlights the challenges in implementing targeted blocks without overreach.

This is the Exhibit Marked "....."
Referred to in the Annexed Affidavit Declaration
of... Eric Mukoya .....
Sworn / declared before me
this... 13 ...day of... May ...20.. 24 .....
at... Nairobi .....
.....
Commissioner For Oaths

Network traffic time series for Kenya

Network traffic (NetFlows) over time

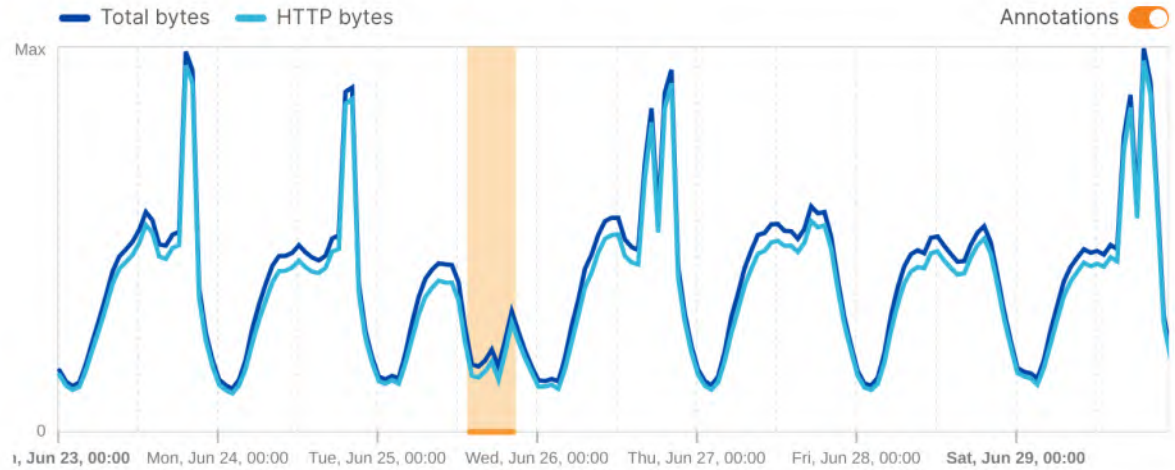


Cloudflare Radar

Jun 23, 2024, 00:00 UTC → Jun 29, 2024, 23:45 UTC

Traffic trends in Kenya

Bytes transferred over the selected time period

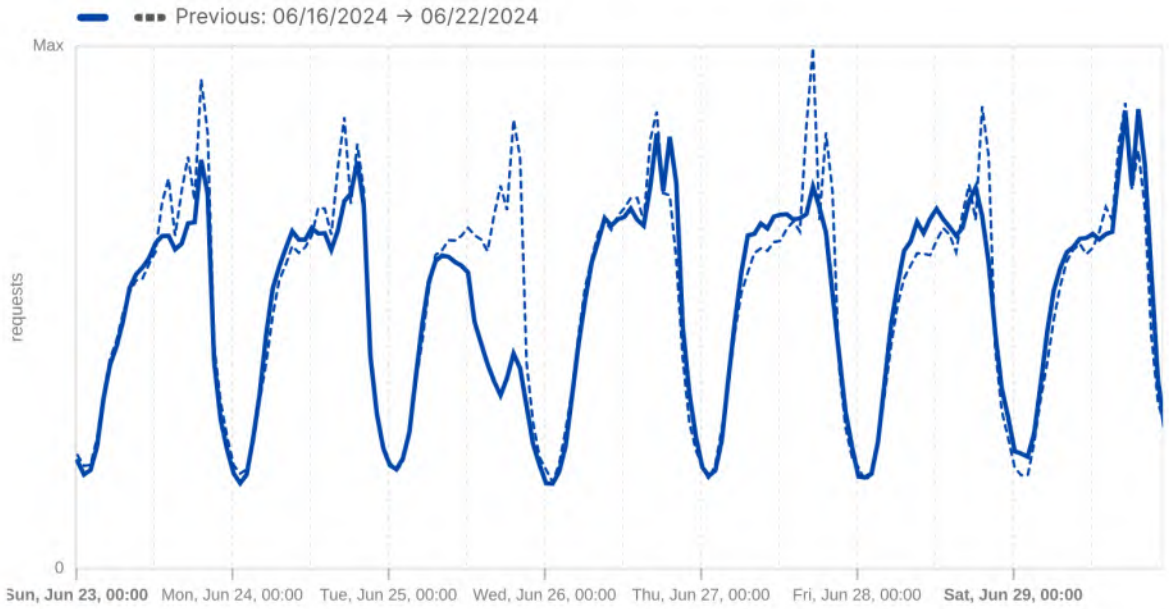


Cloudflare Radar

Jun 23, 2024, 00:00 UTC → Jun 29, 2024, 23:45 UTC

HTTP requests time series for Kenya

HTTP requests over time

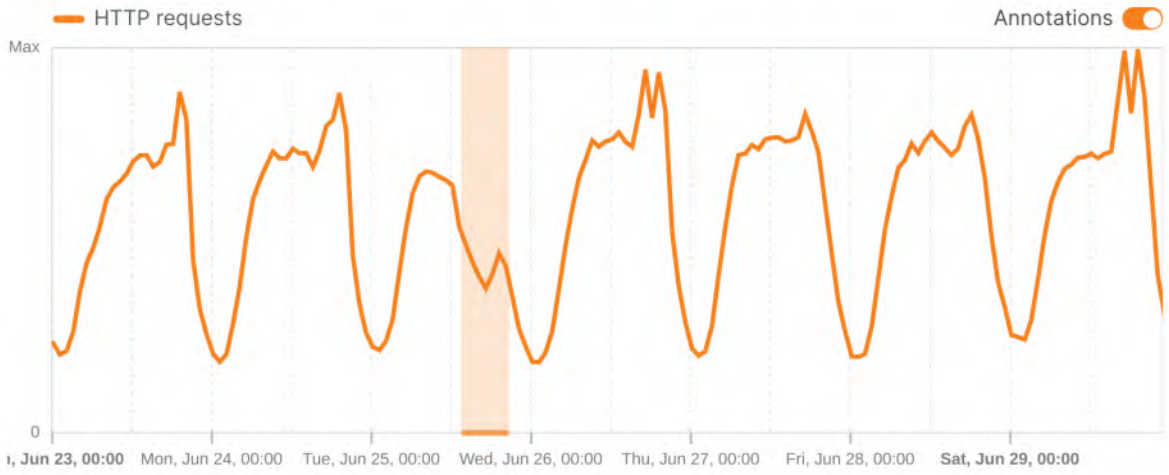


Cloudflare Radar

Jun 23, 2024, 00:00 UTC → Jun 29, 2024, 23:45 UTC

HTTP traffic in Kenya

HTTP requests over the selected time period

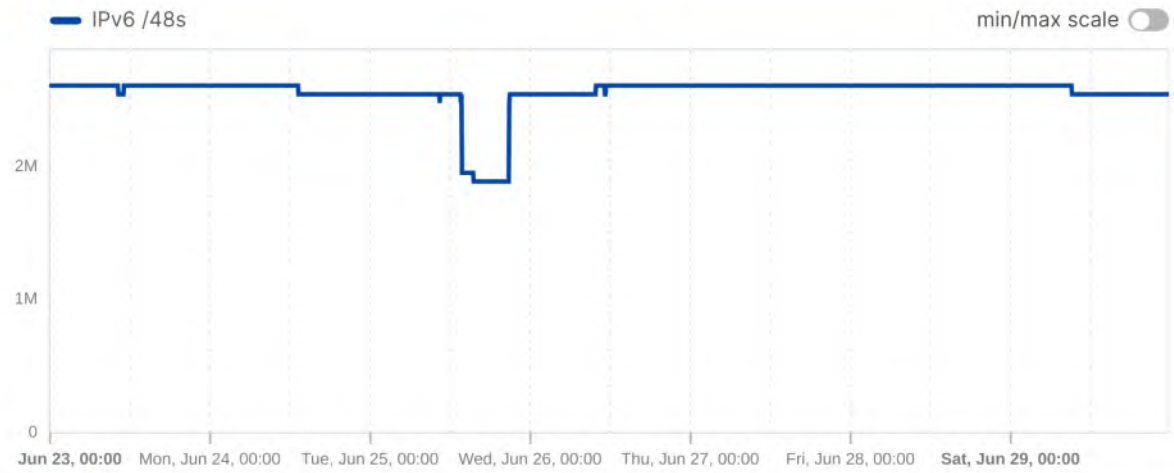


Cloudflare Radar

Jun 23, 2024, 00:00 UTC → Jun 29, 2024, 23:45 UTC

Announced IP Address Space in Kenya

Announced IP address space over the selected time range

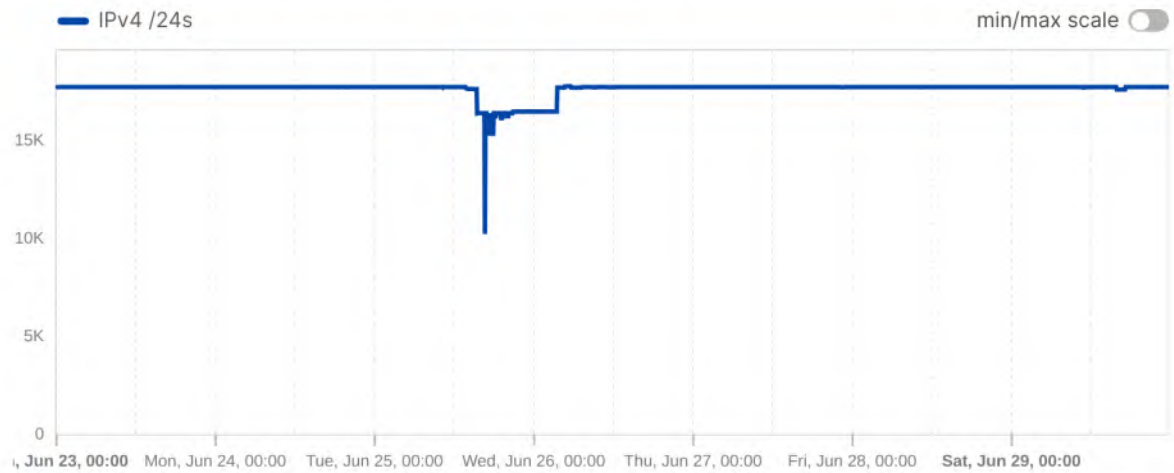


Cloudflare Radar

Jun 23, 2024, 00:00 UTC → Jun 29, 2024, 23:45 UTC

Announced IP Address Space in Kenya

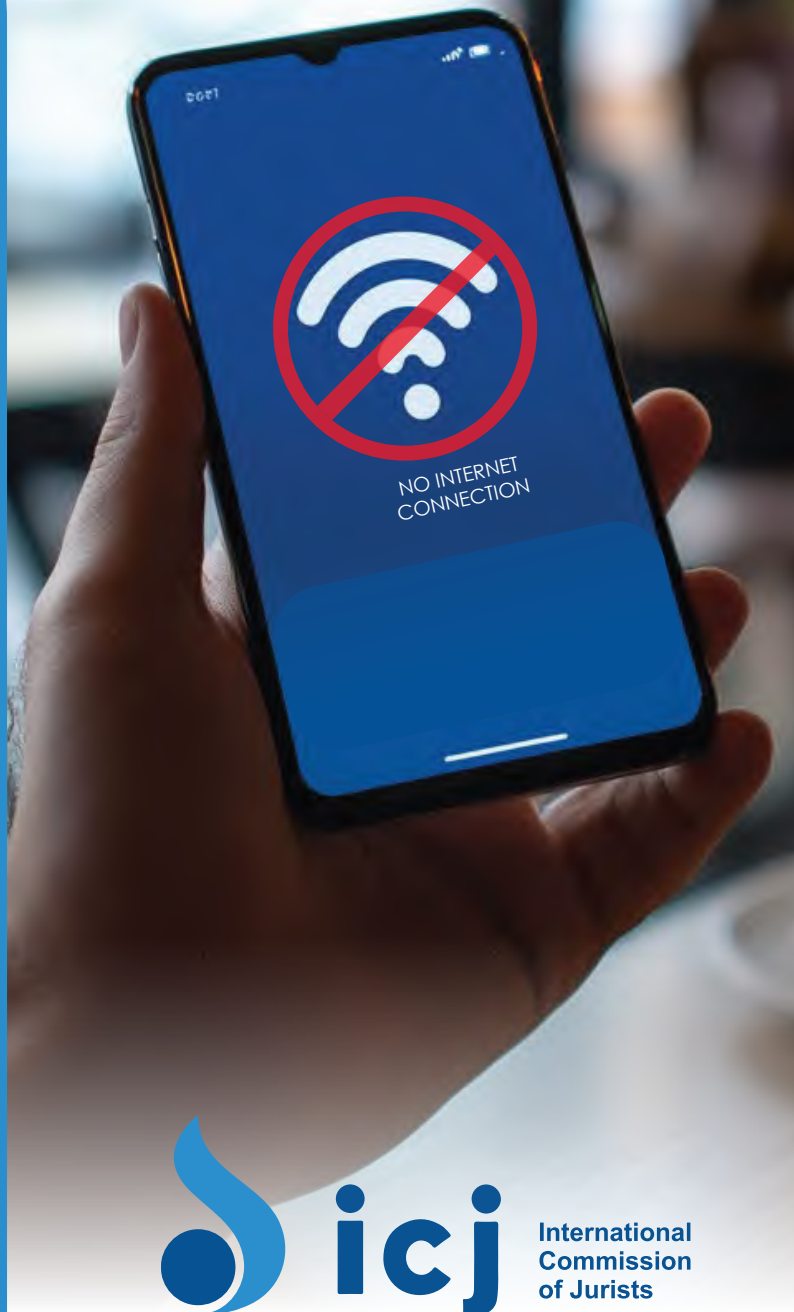
Announced IP address space over the selected time range



Cloudflare Radar

Jun 23, 2024, 00:00 UTC → Jun 29, 2024, 23:45 UTC

ANALYSIS OF INTERNET SHUTDOWNS AND GOVERNANCE FRAMEWORKS IN KENYA



icj International Commission of Jurists
KENYAN SECTION | Since 1959

Published by
The Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ICJ Kenya House, Off Silanga Road, Karen
P.O Box 59743 - 00200, Nairobi, Kenya
Tel: +254-20-2084836/8|+254 720 491549
Email: info@icj-kenya.org
Website: www.icj-kenya.org

Design and Layout:
Ndolo Anderson
Lead Graphics Designer & illustrator - ICJ Kenya

Acknowledgement

This publication, *Strengthening Legal Protections for Freedom of Expression through Digital Rights: A Critical Analysis of Internet Shutdowns and Governance Frameworks in Kenya,* is the result of collective dedication and collaboration driven by the passion to safeguard digital civic space in Kenya.

We extend our deepest gratitude to the Digital Rights portfolio at ICJ Kenya, ably managed by **Demas Kiprono,** whose stewardship and unwavering commitment throughout the project ensured its successful delivery. Special thanks to **Jaika Charles,** the Project Lead and Editor, whose visionary leadership from the inception of the research through topic formulation, coordination, and meticulous editorial guidance was instrumental in shaping the final output. Their tireless efforts and collaborative spirit made this research a true success.

Our heartfelt appreciation goes to **Ephraim Kenyanito** and his team for their exceptional research, critical analysis, and intellectual rigor that form the backbone of this publication.

We also thank **Open Society Foundations (OSF)** for their generous support in funding this project. The valuable contributions from our esteemed digital rights partners, **Article 19** and the **Bloggers Association of Kenya (BAKE),** enriched the research with practical insights and grounded perspectives on internet governance and freedom of expression in Kenya.

This publication stands as a testament to what is possible through collaboration, expertise, and a shared commitment to promoting and protecting digital rights for all.

Signed,

Eric Mukoya
Executive Director
ICJ Kenya.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Kenya's rapid digital transformation, fueled by initiatives like the Digital Superhighway Programme, has positioned the Internet as a vital tool for economic growth, social inclusion, and political participation. Yet, this potential is increasingly undermined by recurrent Internet shutdowns, legal ambiguities, and a lack of accountability in governance frameworks. This report focusses on Kenya's and Africa's digital landscape for over a decade. "This study is framed" through the lens of preserving digital civic space. In this online arena, citizens exercise their rights to expression, information, and assembly. This report critically analyses Kenya's legal frameworks governing Internet freedom, explicitly focusing on shutdowns during politically sensitive periods like the 2024 #RejectFinanceBill protests. It proposes actionable reforms to align with international human rights standards.

The analysis reveals a troubling pattern: Kenya's constitutional guarantees under Articles 33, 34, and 35—freedom of expression, media freedom, and access to information—are eroded by vague provisions in laws like the Computer Misuse and Cybercrimes Act (2018) and the Kenya Information and Communications Act (KICA). These statutes enable government-ordered shutdowns, often justified by nebulous "national security" claims, with minimal transparency or judicial oversight. The Communications Authority of Kenya (CAK), tasked with regulating telecommunications, lacks independence from executive influence. At the same time, telecom providers like Safaricom and Airtel[1] allegedly follow shutdown directives, exacerbating socio-economic harms, evidenced by a $6.3 million daily GDP loss during the 2024 protests. Proposed legislation, such as the 2024 Cybercrimes Amendment Bill, risks further entrenching these threats by broadening state powers over digital content.

In context, the Bill grants authorities broader authority to block websites and online platforms deemed to disseminate "harmful content," a term that remains vaguely defined and open to abuse. This builds on existing loopholes in the 2018 Act, such as Section 22, which criminalises the publication of "false information" without clear definitions, allowing for subjective enforcement.

Compared to existing legal loopholes, the 2024 Bill introduces even broader discretionary powers without addressing the lack of safeguards for proportionality, necessity, and transparency. For instance, it does not require judicial approval for website blocking or data interception, nor does it establish precise mechanisms for redress for individuals whose rights are violated. This represents a significant regression in Kenya's commitment to upholding constitutional and international human rights standards, such as those outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Case studies, including the 2017 Kenyan election disruptions and Uganda's 2021 blackout, underscore the regional fragility of digital rights, while comparative lessons from India's judicial oversight and South Africa's constitutional protections highlight Kenya's regulatory deficits. Key gaps include the absence of specific shutdown laws, limited oversight mechanisms, and disproportionate impacts on vulnerable groups like rural women and small businesses.

These findings are grounded in a mixed methodology—legal analysis and case studies. To safeguard Kenya's digital civic space, the researchers recommend: (1) amending vague legal provisions (e.g., Section 22, 23 and 27 of the Cybercrimes Act) to align with ICCPR standards; (2) enacting legislation mandating judicial approval for shutdowns; (3) enhancing CAK's autonomy from executive overreach; (4) requiring telecoms to publish transparency reports on government requests; and (5) establishing compensation mechanisms for shutdown-affected users in line with the UNHRC's emphasis on access to remedies for human rights violations.

These reforms aim to enhance transparency, accountability, and legal protections, aligning with ICJ Kenya's mission to strengthen Internet freedom and Kenya's obligations under international human rights frameworks. Kenya stands at a crossroads: without urgent action, its digital promise risks becoming a tool of repression rather than empowerment. By adopting these measures, Kenya can align itself with global best practices and ensure its digital space remains a platform for democratic participation, innovation, and human rights.

[1] 'Kenya Borrows Leaf From Peers on Internet Restriction' (The East African, 27 June 2024) <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-borrows-leaf-from-peers-on-internet-restriction-4671858> accessed 22 February 2025

INTRODUCTION

Background

The history of Internet shutdowns in Kenya can be traced back to the 2017 general elections, when the government directed telecommunications providers to block access to social media platforms and messaging services, citing concerns over the spread of hate speech and incitement to violence. Despite clear guidance under the Constitution of Kenya 2010 and various court interpretations; the government has continued to impose restrictions on Internet access during politically sensitive periods, such as the 2022 general elections, raising concerns about the misuse of laws like Section 12 of the National Cohesion and Integration Act and Section 56 of the Cybercrimes Act to justify such actions.

Internet freedom and digital rights are critical components of modern democratic societies, enabling individuals to access information, express opinions, and participate in civic activities. In Kenya, the importance of these rights is underscored by the country's rapid digital transformation and the increasing reliance on Internet connectivity for economic, social, and political activities. Through Articles 33, 34, and 35, the Kenyan Constitution guarantees freedom of expression, media freedom, and access to information, aligning with international frameworks such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

Initiatives like the Digital Superhighway Programme, a World Bank-backed project aimed at expanding Internet access nationwide, have significantly shaped Kenya's digital landscape. These efforts have facilitated better connectivity and digital inclusion, contributing to economic growth and social development. However, the benefits of digitalisation are contingent upon the protection of Internet freedom and digital rights. Without these protections, the potential of the Internet as a tool for empowerment and development is severely undermined.

Despite constitutional and international protections, Kenya has experienced recurrent Internet shutdowns and other forms of censorship, particularly during politically sensitive periods such as protests and elections. These actions pose significant challenges to the free flow of information and the exercise of digital rights, raising concerns about the country's commitment to upholding these fundamental freedoms.

Problem Statement

The primary challenges to Internet freedom in Kenya stem from legal ambiguities, government interference, and private sector complicity. The Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019) under Sections 22 and 23 contain provisions that enable arbitrary arrests and unchecked surveillance, undermining the protections guaranteed by the Constitution. In addition, there is the provision on prevention of "hate speech" and "incitement" under Section 12 of the National Cohesion and Integrity Act. These laws allow for broad and vague interpretations that can be used to justify Internet shutdowns and other restrictive measures. The 2018 arrest and prosecution of Blogger, Cyprian Nyakundi, represents many of the failed and misused attempts by the government to limit the digital rights of citizens, which has a resultant effect of discouraging citizens from engaging in political discourse on digital platforms.

Government interference is evident through actions such as Internet shutdowns during protests and elections. The Communications Authority of Kenya has been implicated in issuing directives for shutdowns, often citing national security concerns. These shutdowns have significant socio-economic impacts, disrupting communication, business operations, and access to information. For instance, during the June 2024 #RejectFinanceBill2024 protests, the government ordered an Internet shutdown that lasted several days, causing daily GDP losses of $6.3 million and disproportionately affecting rural women and small businesses.

The UN General Assembly Resolution 78/213 calls for respect for human rights in the operation, use, and regulation of all digital technologies and provides redress and remedies for all abuses caused by, contributed to, or that may be directly linked to[2].

[2] UNGA Res 78/213 (22 December 2023) UN Doc A/RES/78/213

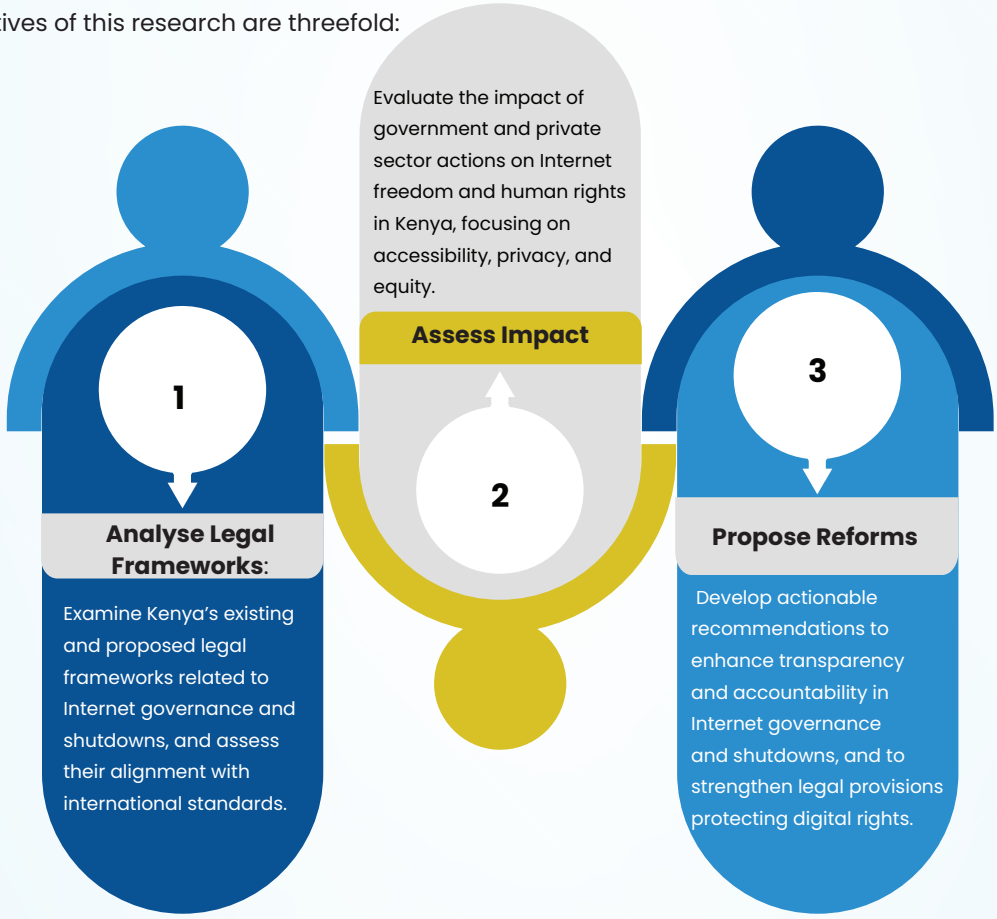
Private sector complicity further exacerbates these challenges[3]. Telecom providers like Safaricom and Airtel[4] have allegedly complied with government directives for Internet shutdowns, raising concerns about transparency and accountability. These actions highlight the need for stronger regulatory frameworks to ensure that companies uphold human rights standards and resist government overreach.

Specifically, Kenya's obligations under the UN Guiding Principles on Business and Human Rights under Pillar 2 require corporate businesses to undertake ongoing human rights due diligence to identify, prevent and mitigate human rights abuses. Fundamentally, companies should enable remediation mechanisms for the negative impacts they have caused or contributed to.[5]

In the same vein, ARTICLE 19 recommends that operators could achieve more for human rights by being more transparent about issues that affect human rights.[6] In Kenya, transparency could entail disclosure to consumers on information with which they can distinguish between typical Internet glitches and government-sanctioned disruptions.[7] Additionally, there is a critical need for explicit legal provisions that mandate corporate resistance to overreaching government orders, ensuring that companies prioritise human rights over compliance with unconstitutional actions.

Research Objectives

The objectives of this research are threefold:



[3] Freedom House, 'Kenya: Freedom on the Net 2024 Country Report' (Freedom House 2024)<https://freedomhouse.org/country/kenya/freedom-net/2024> accessed 22 February 2025

[4] 'Kenya Borrows Leaf From Peers on Internet Restriction' (The East African, 27 June 2024) <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-borrows-leaf-from-peers-on-internet-restriction-4671858> accessed 22 February 2025

[5] John Ruggie, 'Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises' (21 March 2011) UN Doc A/HRC/17/31, annex ('Guiding Principles on Business and Human Rights')

[6] ARTICLE 19, 'Getting connected: Freedom of expression, telcos and ISPs' (June 2017) <https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf> accessed 7 April 2025

[7] For instance, Ugandan President responded to media questions about the shutdown order inFebruary 2016. BBC News, 'Uganda election: Facebook and WhatsApp blocked' (18 February 2016) <http://www.bbc.com/news/world-africa-35601220> accessed 18 March 2025

Scope of the Research

This research focuses on the following key areas:

- **Legal Frameworks:** A comprehensive analysis of existing laws, such as the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and proposed legislative frameworks. The analysis will include a comparative study of best practices from other jurisdictions, such as India and South Africa, to identify gaps and areas for improvement.

- **Transparency and Accountability:** Examining the mechanisms to ensure transparency and accountability in government directives and private sector compliance. This includes assessing the role of the Communications Authority and telecom providers in implementing Internet shutdowns and other restrictive measures.

- **Human Rights Impact:** This evaluation of the socio-economic and human rights implications of Internet shutdowns focuses on vulnerable populations such as rural women and small businesses. It includes analysing the impact on accessibility, privacy, and equity.

Legal and Regulatory Framework.

1. Constitution of Kenya 2010.

The Constitution of Kenya, 2010, offers a strong legal foundation for Internet freedom, safeguarding key rights such as freedom of expression, access to information, privacy, and media independence rights that are increasingly important in the digital era. Article 33 guarantees freedom of expression, including the right to seek, receive, and impart information[8]. This protection extends to online platforms, enabling individuals to express their views, engage in discussions, and share information without undue restrictions. However, this freedom is not absolute; the Constitution permits limitations [9]based on considerations like hate speech, incitement to violence, and defamation.

Equally important, Article 35[10] enshrines the right to access information, obliging the government to facilitate public access to official information. This provision promotes transparency and accountability, ensuring citizens can request and access information affecting their interests. However, challenges persist, such as the government's reluctance to disclose sensitive information and instances where online content is restricted. This creates a gap between the constitutional promise of transparency and the practical limitations on access to information, especially in the digital space.

It follows that theories surrounding digital authoritarianism suggest that governments may employ Internet shutdowns as tools to control information and suppress dissent under the guise of maintaining national security and public order.[11] This undoubtedly contravenes established international human rights norms, despite the insistence of offending governments to uphold their "sovereign authority" to counter threats to public order.[12] A pertinent example would be the Internet shutdown witnessed in the recently dubbed #RejectFinanceBill2024 protest, where government restriction was seen as a suggestion to control the flow of information,[13] which was key to the protest essentially gaining traction over social media.

---

8 Constitution of Kenya 2010.

9 Constitution of Kenya 2010.

10 Constitution of Kenya 2010.

11 K V Bhatia and others. 'Protests, Internet shutdowns, and disinformation in a transitioning state.' Media, Culture & Society, 45 (2023): 1101 – 1118. <https://doi.org/10.1177/01634437231155568/> accessed 18 March 2025

12 Steven Feldstein, 'Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?' (Carnegie Endowment for International Peace, March 2022) <https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en/> accessed 18 March 2025

13 APC, 'Digital protests, access and freedoms in Kenya' (18 July 2024) <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 18 March 2025

Privacy is another critical right under the Constitution, as outlined in Article 31[14]. This right protects individuals from unwarranted surveillance and interference with their private affairs. This provision is critical on the Internet, given the rise of digital surveillance, data collection, and online tracking.

Further reinforcing Internet freedom, Article 32[15] guarantees freedom of conscience, religion, belief, and opinion, ensuring that individuals can freely express their beliefs and opinions online. The Internet has become a primary political, social, and religious discourse space. However, the government has occasionally imposed restrictions on online speech, often under the guise of national security or the fight against radicalisation, hate speech, and misinformation[16]. These restrictions sometimes undermine the broader constitutional goal of promoting free expression, mainly when used selectively to stifle dissent.

Article 34[17] guarantees freedom of the media, which is integral to ensuring a free and open Internet. In its digital form, the media plays a central role in providing information, educating the public, and facilitating debate on essential issues. Yet, there have been increasing cases of censorship, media shutdowns, and content moderation by both the government and private platforms[18]. While some of these actions are justified by concerns over hate speech or national security, they can be used to suppress dissenting voices, raising questions about the balance between regulation and freedom. The independence of digital media is essential for maintaining a pluralistic and democratic society[19].

Article 38 supports political participation, including the right to engage in political activities and expression online. The Internet has become a crucial tool for political mobilization, enabling citizens to engage in political discourse, campaign, and advocate for change. However, during election periods, attempts have been made to regulate digital campaigning, restrict political content, and combat misinformation. These measures often conflict with the right to free political expression, leading to debates over regulatory limits and digital rights protection during such critical periods.

Finally, Article 21 requires the state to respect, protect, promote, and fulfill human rights. This obligation mandates that the government ensure policies and laws enacted do not undermine fundamental rights. The most critical fundamental rights in the context of Internet shutdowns pertain to the denial of the citizen's right to access information and freedom of expression, as has been established by many court precedents. Regarding contextualisation, Section 29, KICA was among the few established laws that were key in prosecuting bloggers. However, it was challenged in the case of ***Geoffrey Andare v Attorney General & 2 others***, which led to the section being declared unconstitutional.[20] This speaks to the government's role in ensuring its policies and laws do not undermine fundamental rights and the courts' role in interpreting such rights.

In the larger African context, the African Court, while dealing with the application brought against the State of Guinea,[21] noted that the right to information aims to enable citizens to participate usefully in the democratic process and decisions concerning their future. It held that the right to information is an extension of freedom of the press and freedom of expression and that any unjustified measure that suspends or restricts free access to information constitutes a violation of the right to information. As such, the government's actions in interrupting access to the Internet without justification constituted a violation of the right to information.

---

14 Constitution of Kenya 2010.

15 Constitution of Kenya 2010.

16 CIPIT, 'Technology-Facilitated Rights and Digital Authoritarianism: Examining the Recent Internet Shutdown in Kenya' *(Centre for Intellectual Property and Information Technology Law,* 9 August 2024) <https://cipit.org/technology-facilitated-rights-and-digital-authoritarianism-examining-the-recent-internet-shutdown-in-kenya/> accessed 15 February 2025.

17 Constitution of Kenya 2010.

18 Pulselive Kenya, '6 Media Houses Warned over Coverage of Azimio Mass Action Protest' (29 July 2024) <https://www.pulselive.co.ke/articles/news/local/citizen-tv-ntv-k24-kbc-tv47-and-ebru-tv-warned-over-coverage-of-azimio-protest-20240729085143951O1> accessed 15 February 2025

19 J ack M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society', Popular Culture and Law (Routledge 2017).

20 *Geoffrey Andare v Attorney General & 2 others* [2016] eKLR (Kenya)

21 *Association des Blogueurs de Guinee (ABLOGUI) and Others v State of Guinea* [2023] ECOWASCJ 1 (ECOWAS)

These constitutional provisions form a comprehensive framework for protecting Internet freedom in Kenya. While they provide a strong legal basis for protecting digital rights, challenges remain in their practical implementation, especially as digital technology evolves. Notably, the absence of explicit constitutional provisions or specific laws governing Internet shutdowns in Kenya creates a significant gap in the legal framework, leaving room for arbitrary actions that may undermine digital rights.

Continued judicial oversight, legal reforms, and advocacy for digital rights will be necessary to ensure that Kenya upholds its constitutional promise of a free and open Internet. Furthermore, the Courts' crucial role in interpreting digital rights in past cases, such as addressing Internet access as a fundamental right, sets a precedent as a judicial trend aimed at guiding future legal reforms. Balancing security concerns, regulation, and individual freedoms is key to ensuring that the Internet remains a space for democratic participation, expression, and access to information.

2. Computer Misuse & Cybercrimes Act, 2018

The Computer Misuse and Cybercrimes Act[22] is a critical piece of Kenya legislation addressing cybercrime and online conduct issues. While the Act aims to regulate online activities to prevent harm, its provisions have sparked concerns over Internet freedom, particularly with respect to free expression, privacy, and access to information. Below is an analysis of specific sections of the Act that relate to Internet freedom:

Section 22 criminalises the publication of false information, particularly when it is likely to cause fear, harm, or violence. This provision has significant implications for Internet freedom, as it grants authorities the power to target individuals who share content deemed false or misleading. While this provision addresses issues such as misinformation and fake news, it raises concerns about the potential for government overreach, where legitimate opinions or political commentary could be prosecuted as "false information." The subjective nature of what constitutes false information can stifle free speech and curb the diversity of voices in online spaces, especially if applied in a manner that targets political dissent or controversial opinions.

Section 23 criminalises publication of false information calculated to cause panic, chaos or violence, or likely to discredit the reputation of a person. While this section intends to protect public order, national security and rights and reputations of others, it invents its own limitations to freedom of expression that are inconsistent with Article 33 (2), such as propaganda for war, incitement to violence and advocacy for hatred. Regarding protecting the reputations of others, the law sneaks back criminal defamation, which had been declared unconstitutional by the High Court in 2017.

Section 27 seeks to protect individuals from cyber harassment. However, it contains broad terms such as criminalising content that causes "apprehension" or fear of violence to them or damage or loss to that person's property; or "detrimentally affects that person"; or "grossly offensive nature". These may offend the principle that limitations for freedom of expression must be clear and concise.. The Act's[23] provisions could be used to prosecute individuals for online speech that is critical, controversial, or confrontational, even if it does not constitute harassment. The fear of being charged under this section may discourage people from engaging in critical discourse or expressing dissenting opinions, thus potentially infringing on freedom of expression.

In the Kenyan context, the online campaign dubbed, "Tumtumie Salamu" was a representation of such instances, where the publication of public servants contacts across social media platforms was met with threats of prosecution and launch of complaints from the Office of the Data Protection over violation of the right to privacy as a protection accorded under the Act.

While the government runs along with maintaining public order and national security, a line has to be drawn between a State's sovereign authority and accountability measures. Since its enactment, persons who have been arrested for the dissemination of false information have been charged under both sections 22 and 23 of the CMCA.

---

22 Computer Misuse and Cybercrimes Act 2018 (Kenya)

23 Computer Misuse and Cybercrimes Act 2018 (Kenya)

The Act has been weaponised as a tool to combat dissent. Bloggers and activists such as Edgar Obare[24] and Mutemi wa Kiama[25] are some of those who have been arraigned in court over violation of this law after threats and intimidation from unknown third parties. Activists have also been threatened with arrest and other consequences for speaking out on issues touching on police brutality. Others have even had their laptops and other equipment confiscated.[26]

Section 24 criminalises unauthorised access to information, which includes hacking or accessing someone else's computer systems without permission. While this provision is essential for protecting individuals' and organisations' data privacy and security, it has raised concerns regarding protecting journalists, whistleblowers, and activists. In some cases, the law could be misused to target individuals or groups attempting to expose corruption or wrongdoing[27], as unauthorised access to certain information might be perceived as a criminal act. This provision could be seen as limiting access to information, particularly when uncovering abuses of power or holding authorities accountable, potentially infringing upon the public's right to access important information.

Section 26 criminalises identity theft and impersonation, particularly using someone else's personal information for fraud. While protecting individuals from identity theft is crucial for online safety, this section could have implications for digital rights if misapplied. For instance, activists or whistleblowers who attempt to expose government corruption or abuse may be at risk of being accused of impersonating officials or unauthorised access. Furthermore, the law could be used to suppress digital activism or independent journalism if authorities target individuals who engage in online campaigns using pseudonyms or anonymous profiles, undermining the right to freedom of expression and participation.

Section 27 defines and criminalises cyberterrorism, which involves the use of technology to promote terrorism or extremist acts. While the Act aims to protect national security by preventing cyberattacks that threaten the country's infrastructure, there is concern that this section may be used to justify broad surveillance or censorship of online content. Under the guise of national security, this section could be misused to restrict political speech, suppress activism, or censor online discussions critical of government policies. The potential for the law to be applied to curtail legitimate political engagement, protests, or free speech is a significant challenge to Internet freedom.

Section 34 allows for the interception of communications under specific conditions, particularly to investigate crimes. While the goal of preventing cybercrimes is essential, the provisions of this section have raised significant concerns regarding privacy and surveillance. The ability of authorities to monitor online communications can lead to the infringement of individuals' right to privacy, particularly if such powers are exercised indiscriminately or without proper judicial oversight[28]. The risk of over-surveillance is heightened in the digital age, where governments could monitor political dissidents, journalists, or activists, thereby chilling free expression and curtailing the right to privacy.

Section 37 grants authorities the power to arrest individuals suspected of committing offenses under the Act without a warrant, particularly in cases involving cybercrimes. While this provision is designed to enhance law enforcement's ability to quickly respond to cyber threats, it raises concerns about the potential for arbitrary arrests and the abuse of power.

---

24 Directorate of Criminal Investigations (@dci_kenya), 'Statement on arrest of Edgar Obare under Section 23 of Computer Misuse and Cybercrimes Act 2018' (X, 4 March 2021) <https://twitter.com/dci_kenya/status/1367512899044925442/> accessed 18 March 2025

25 ARTICLE 19, 'Kenya: Release and cease attacks on Edwin Mutemi wa Kiama' (8 April 2021) <https://www.article19.org/resources/kenya-cease-attacks-on-and-release-edwin-mutemi-wa-kiama/> accessed 18 March 2025

26 Human Rights Watch, 'Kenya: Police Threaten Activists Reporting Abuse' (4 June 2018) <https://www.hrw.org/news/2018/06/04/kenya-police-threaten-activists-reporting-abuse> accessed 22 February 2025

27 Abdulmalik Sugow and others, 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression' (2021) 1(1) JIPIT <https://www.researchgate.net/publication/352475154_Appraising_the_Impact_of_Kenya's_Cyber-Harassment_Law_on_the_Freedom_of_Expression> accessed 17 February 2025

28 Mugambi Laibuta, 'State surveillance: Kenyans have a right to privacy – does the government respect it?' (*The Conversation*, 29 November 2024) <https://www.polity.org.za/article/state-surveillance-kenyans-have-a-right-to-privacy-does-the-government-respect-it-2024-11-29> accessed 17 February 2025

The broad application of this section could be used to target individuals who engage in online activities critical reporting, or political opposition[29]. If not carefully controlled, such provisions could lead to a chilling effect on free expression, as individuals may fear legal repercussions for their online activities.

Section 50 outlines the liability of Internet intermediaries, such as Internet service providers (ISPs) and social media platforms, for content hosted or transmitted through their services.

This section can affect Internet freedom, particularly when platforms are pressured to follow government requests to censor or remove content critical of the government. The potential for Internet intermediaries to act as gatekeepers, by either removing content or blocking access to websites, raises concerns about the erosion of free speech online[30]. In some instances, these platforms may be compelled to restrict online content to avoid facing legal consequences, undermining the principle of free and open access to information.

Section 56 of the Act gives the government powers to regulate and control digital content, particularly concerning national security, public order, and morality. This section raises concerns about Internet shutdowns and content filtering, particularly during political unrest, protests, or elections. The broad scope of regulation could be used to justify the shutdown of social media platforms or entire Internet services, which would infringe on citizens' rights to access information, communicate freely, and participate in democratic processes. While content regulation is necessary to address harmful or illegal online activity, it should not be used to suppress free expression or limit the flow of information.

Data Protection Act, 2019

The Data Protection Act, 2019[31] and its regulations in Kenya contain provisions that raise significant concerns about the balance between privacy, Internet freedom, and public interest. Several controversial sections can potentially undermine individuals' privacy rights, particularly regarding indirect data collection, exemptions from consent, and the scope of data processing for law enforcement, national security, and public interest.

Section 41 of the Act outlines broad exemptions, allowing personal data to be processed without consent for national security, law enforcement, and public interest purposes. Though necessary for certain state functions, these exemptions are controversial because they could be used to justify mass surveillance and unwarranted data collection under vague justifications. The national security exemption, for instance, opens the door to invasive data collection, potentially infringing on individuals' rights to privacy and freedom of expression, especially if the criteria for "national security" are not clearly defined[32].

Section 41(2) further exempts data processing for investigating or prosecuting crimes, enabling law enforcement agencies to collect personal data without consent. While essential for crime prevention, this provision raises concerns about overreach and the potential for surveillance, mainly when such activities are conducted without oversight. Similarly, Section 41(3) allows personal data to be processed in the public interest, including activities like public health research or safety measures. However, the broad interpretation of public interest may be exploited for data collection purposes unrelated to public welfare, infringing individual privacy.

Regulation 14, which deals with the indirect collection of personal data for law enforcement or public interest, is another area of contention. This regulation permits data to be gathered without the subject's direct consent, including through third-party data collection or surveillance.

---

29 Abdulmalik Sugow and others, 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression' (2021) 1(1) JIPIT <https://www.researchgate.net/publication/352475154_Appraising_the_Impact_of_Kenya's_Cyber-Harassment_Law_on_the_Freedom_of_Expression> accessed 17 February 2025

30 Council of Europe (Freedom of Expression), 'The Role of Internet Intermediaries as Gatekeepers to Freedom of Expression – Conference in Vienna' (2017) <https://www.coe.int/en/web/portal/-/the-role-of-internet-intermediaries-as-gatekeepers-to-freedom-of-expression-conference-in-vienna> accessed 17 February 2025

31 Data Protection Act 2019 (Kenya)

32 Mercy Muendo, 'Kenya Plans to Place Public Security above Data Privacy. That's a Bad Idea' (The Conversation, 11 February 2019) <http://theconversation.com/kenya-plans-to-place-public-security-above-data-privacy-thats-a-bad-idea-111099> accessed 17 February 2025

While necessary for criminal investigations, the regulation could be misused to conduct broad, intrusive monitoring of individuals, undermining the principle of informed consent and leaving people unaware that their data is being processed.

Moreover, the guise of national security may be used to justify Internet shutdowns. Authorities might argue that indirect data collection alone is insufficient to address imminent threats such as organised crime, thus necessitating a complete shutdown of Internet services to prevent the spread of harmful content or coordination of illegal activities. Without clear legal safeguards and judicial oversight, the broad language of Regulation 14 risks being exploited to legitimise excessive measures that undermine digital rights under the pretext of national security.

Kenya Information & Communication Act, 1998

The Kenya Information and Communications Act (KICA) regulates communications, including the Internet, broadcasting, and telecommunication services in Kenya. While designed to promote efficient communication and broadcasting services, specific provisions of KICA[33] raise concerns regarding Internet freedom and privacy.

Section 84 on retention of communication data mandates that telecommunications service providers retain user communication data, including Internet browsing history, for up to two years to assist in law enforcement investigations. While aimed at combating crime, the lack of clear guidelines for data protection and the potential for unauthorised access to this retained data heighten concerns over privacy violations. The risk of mass surveillance is significant, and the provision lacks oversight mechanisms to ensure that the data is not misused.

Section 88 grants the Communications Authority of Kenya (CAK) the authority to monitor, regulate, and censor content transmitted over electronic communications. The broad powers provided to the CAK raise concerns about potential censorship, particularly when content critical of the government or national interests is deemed harmful. The discretion to regulate content without adequate checks and balances could suppress free expression, especially in politically sensitive contexts. The lack of oversight increases the potential for abuse and curtails the diversity of online content.

These provisions within KICA threaten Internet freedom by allowing mass surveillance and broad content control without sufficient safeguards, potentially undermining online privacy rights and freedom of expression.

Prevention of Terrorism Act, 2012

The Prevention of Terrorism Act (POTA)[34] aims to curb terrorism activities in Kenya. While crucial for national security, several sections have raised concerns about Internet freedom and privacy, particularly regarding surveillance and data collection.

Section 26 allows law enforcement agencies to intercept communications, including Internet communications, when investigating or preventing terrorism. The broad authority granted for communication interception raises concerns over the surveillance of individuals not connected to terrorism. The lack of defined limits on the scope of surveillance may lead to widespread monitoring of online activities without adequate safeguards or oversight.

Section 29 allows authorities to collect personal data from service providers to aid terrorism-related investigations. This provision provides access to vast amounts of personal data, including communication logs and Internet usage data, which can infringe on privacy. The ability to collect data without sufficient checks and balances poses a significant risk of mass surveillance, particularly for individuals not involved in criminal activities.

33 Kenya Information and Communications Act 1998 (Kenya)

34 Prevention of Terrorism Act 2012 (Kenya)

National Cohesion & Integration Act, 2008

The National Cohesion and Integration Act (NCIA)[35] promotes national unity and prevents ethnic and political violence in Kenya. However, specific provisions raise concerns about online freedom of expression and the potential for censorship.

Section 13 criminalises the use of hate speech and the incitement of violence through communication platforms, including social media. While necessary for national unity and peace, the definitions of "hate speech" and "incitement" are broad and open to subjective interpretation.

The ambiguity in these definitions could restrict legitimate political discourse or controversial opinions, potentially stifling free speech online.

An equally good example as the basis for the Internet Shutdown in 2017, as claimed by the government, was to curb the spread of hate speech, misinformation and incitement to violence. The resulting factor, however, was a limitation on digital rights, such as access to information and freedom of expression, in implementing an Internet shutdown without demonstrating that less restrictive measures were insufficient. The reliance on this section for the prosecution of bloggers has had a chilling effect, discouraging Kenyans from engaging in online discussion, particularly on sensitive topics such as politics and governance issues.

Section 13 empowers the government to monitor and control content promoting political or ethnic violence. The vague wording of "political or ethnic violence" raises concerns that it could be used to suppress free expression on politically sensitive issues. The broad discretion granted to authorities to regulate content may cause the censorship of opinions critical of government policies or controversial ethnic matters, limiting the diversity of political discourse online.

Section 62 criminalises the publication or distribution of materials that are threatening, abusive, or insulting and likely to incite ethnic hatred. While this provision aims to prevent the spread of harmful content, the lack of clear definitions for these terms leaves room for subjective interpretation and potential misuse by authorities. This section can target critics, activists, and journalists who publish controversial content online, particularly political commentary. Moreover, it does not provide sufficient protection for legitimate public debate, leading to a chilling effect on online discussions due to the fear of prosecution.

Closely related is Section 62(2), which criminalises intent to incite ethnic hatred, even if the material published did not lead to such incitement. This provision is particularly problematic because it allows authorities to prosecute individuals based on perceived intent rather than clear evidence of harm. Such an approach opens the door for arbitrary enforcement and could be used to silence online activists, bloggers, and independent media expressing dissenting views. The risk of individuals being prosecuted for sharing political or controversial opinions is high, as authorities could claim that such content was intended to incite hatred.

Another concerning provision is Section 63, which prohibits the possession, publication, or dissemination of materials that promote ethnic hatred, including digital content shared on social media. The broad and undefined scope of what constitutes "hate-related materials" raises concerns that political or dissenting opinions could easily be criminalised. Additionally, this provision makes online users and platforms liable for simply sharing or even unknowingly possessing controversial content. Given the lack of judicial oversight, enforcement could disproportionately target political opposition, human rights defenders, or minority groups, further restricting free speech online.

The National Cohesion and Integration Commission (NCIC) powers under Section 66 add another layer of concern. The NCIC is granted authority to investigate, prosecute, and recommend legal action against individuals accused of promoting ethnic hatred or incitement. However, the Commission has been criticised for political bias, raising concerns that these powers could be used selectively to target government critics while ignoring speech that supports those in power.

35 National Cohesion and Integration Act 2008 (Kenya)

Furthermore, its ability to monitor online content without clear procedural safeguards increases the risk of mass surveillance and censorship, undermining Internet freedom.

Section 67 further restricts online expression by prohibiting media houses from publishing or broadcasting content deemed "prejudicial to cohesion and integration." The vague nature of this provision makes it possible for authorities to restrict news reports, opinion pieces, or online discussions that critique the government.

Media houses, bloggers, and social media users could face penalties for publishing investigative reports on corruption, electoral fraud, or human rights violations if such content is deemed to undermine "cohesion." This provision could also justify blanket bans on social media platforms or suppress online discussions, particularly during elections or political unrest.

Proposed legislation and its impact on free speech.

Kenya has seen several proposed laws and regulations in recent times following the #RejectFinanceBill2024 protests; this legislation touches on freedom of expression, social media regulation, and Internet shutdowns. These proposals have arisen as a disguise to balance national security, public order, and individual rights, but they have sparked debates about their potential impact on democratic freedoms. Below are some notable examples based on recent developments:

i. Computer Misuse and Cybercrimes (Amendment) Bill, 2024

This bill seeks to amend the existing Computer Misuse and Cybercrimes Act of 2018, which governs cyber offenses in Kenya. The proposed amendments aim to expand the government's powers to address illegal online activities. It includes measures to allow authorities to close websites and applications that perform unlawful activities, such as spreading misinformation, inciting violence, or hosting harmful content. It also broadens the definitions of cyber offenses. Critics argue that the vague wording of "illegal activities" could lead to overreach, potentially stifling free speech and access to information[36]. The ability to block websites raises concerns about censorship and suppressing dissenting voices.

The bill reflects a growing push to regulate digital spaces amid concerns over misinformation and security, but it has been met with calls to ensure it doesn't undermine constitutional rights like freedom of expression enshrined in Article 33 of the Kenyan Constitution.

ii. Kenya Information and Communications (Amendment) Bill, 2019 ("Social Media Bill")

Proposed by Malava MP Moses Injendi, this Bill aimed to introduce strict regulations on social media use in Kenya by amending the Kenya Information and Communications Act (KICA). The law would require bloggers and social media group administrators to obtain licenses from the Communications Authority of Kenya (CA). The bill also mandated that social media platforms accessible in Kenya have a physical office in the country and maintain user data for submission to the CA upon request. Further, the bill imposed obligations on users to refrain from posting certain types of content, though penalties for non-compliance were unclear.

The Bill was widely criticised for infringing on privacy, freedom of expression, and association. Human rights advocates, including Amnesty International Kenya, argued it threatened the democratic strides made in digital expression[37]. The ICT Committee of Parliament deemed it unconstitutional, citing violations of rights to speech and privacy. Due to public outcry and opposition from stakeholders like the Kenya Union of Journalists and the Bloggers Association of Kenya, the bill did not progress beyond its first reading and was effectively shelved..

[36] kictanetadmin, 'Proposal to Block Websites and Applications Threatens Kenya's Digital Ecosystem' (KICTANet Think Tank, 2 October 2024) <https://www.kictanet.or.ke/proposal-to-block-websites-and-applications-threatens-kenyas-digital-ecosystem/> accessed 23 February 2025

[37] Brian Murimi, 'Proposed Changes to Kenya's Constitution: A Look at the 2024 Amendment Bill' (Sharp Daily, 2 October 2024) <https://the-sharpdaily.com/kenya-constitutional-amendment-bill-2024/> accessed 23 February 2025

Case Study of Internet Shutdowns and the Interconnection with Civil Space

The erosion of Internet freedom and freedom of expression in Kenya has been marked by numerous incidents involving state interference, online censorship, surveillance, and crackdowns on dissent. While the government has sometimes upheld digital access, various legal and extrajudicial measures have been used to suppress critics, silence activists, and control online discourse.

Examining specific case studies helps to illustrate how state agencies have wielded laws, technology, and security forces to intimidate and punish those exercising their rights. From Internet shutdowns and digital surveillance to arbitrary arrests and violent crackdowns on protesters, these instances highlight the fragile state of Internet freedom in Kenya and the ongoing struggle to protect digital rights in an increasingly repressive environment.

i. Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)[38]

In 2017, the Bloggers Association of Kenya (BAKE) challenged the Computer Misuse and Cybercrimes Act, 2018, arguing that specific provisions violated the freedom of expression and Internet freedom guaranteed under Articles 33 and 34 of the Kenyan Constitution. Specifically, BAKE contested sections criminalising false publication, cyber harassment, and the misuse of telecommunication devices, claiming that these provisions were vague, overbroad, and susceptible to abuse by state authorities. The High Court initially suspended the enforcement of these contentious provisions, but subsequent rulings allowed the government to enforce most of them. This case highlights the ongoing legal battles over digital rights in Kenya, where cybercrime laws are often used to target journalists, bloggers, and activists under the guise of regulating online content.

ii. The Arrest of Cyprian Nyakundi and Other Bloggers

Kenyan bloggers and social media commentators, particularly those publishing critical content, have frequently faced arrests and intimidation. A prominent example is Cyprian Nyakundi, a blogger known for exposing alleged corruption and misconduct among Kenya's political and business elites. Nyakundi was arrested multiple times under Section 23 of the Computer Misuse and Cybercrimes Act, which criminalises the publication of "false information." His case underscores how laws designed to combat cybercrime are often weaponised to suppress dissent and curb investigative journalism, threatening the fundamental right to freedom of expression and access to information.

iii. The 2024 Finance Bill Protests

In mid-2024, widespread protests erupted in response to a proposed finance bill that included controversial tax hikes. These protests, organised mainly by Generation Z activists through social media, faced heavy crackdowns by security forces. At least 23 protesters were killed, and hundreds were arrested[39]. The government's heavy-handed response, including reports of abductions and intimidation, raised serious concerns about the suppression of dissent and the erosion of Internet freedom[40]. The protests also highlighted the critical role of social media in facilitating decentralised activism and how authorities responded with excessive force to stifle political dissent.

---

38 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR (Kenya)

39 Nita Bhalla, 'Why has Kenya's finance bill triggered protests?' (*Context.news*, 26 June 2024) <https://www.context.news/money-power-people/why-has-kenyas-finance-bill-triggered-public-outrage> accessed 17 February 2025

40 Nicholas Mwangi, 'Surge in Abductions of Government Critics in Kenya Sparks Mass Public Outcry' (*Peoples Dispatch*, 14 January 2025) <https://peoplesdispatch.org/2025/01/14/surge-in-abductions-of-government-critics-in-kenya-sparks-mass-public-outcry/> accessed 17 February 2025

iv. Abduction of Kizza Besigye

In November 2024, Ugandan opposition leader and activist Kizza Besigye was abducted in Kenya and forcibly returned to Uganda[41]. Besigye was in Kenya to attend a book launch by Martha Karua, a known critic of the Kenyan government. His abduction highlights the increasing risks faced by government critics and the apparent collaboration between regional security agencies to suppress dissent. This incident is a stark reminder of the escalating challenges faced by activists and critics within the region.

v. Abduction of Maria Sarungi Tsehai

In January 2025, a prominent Tanzanian activist and media owner, Maria Sarungi, who fled to Kenya in 2020 owing to her intense criticism of the government, was kidnapped in Kenya with concerted efforts to transport her to Tanzania.[42]

This presents the critical danger presented to online activists who dare act as critics of the government, even with Sarungi's story showing the strong determination behind her kidnappers' wanting to gain access to her phone and have access to her social media accounts unsuccessfully. This equally presents a harsh reality of day-to-day risks faced by online activists and any individuals whose expressions do not fit a positive 'government agenda' and 'security.'

Comparative Analysis: Lessons from Other Jurisdictions

A Case Study of India

Anuradha Bhasin v. Union of India and Ghulam Nabi Azad v. Union of India is a landmark case where the Indian Supreme Court, accepted that Article 19(1)(a) protects the right to disseminate and receive information online. Therefore, the constitutional validity of every Internet shutdown would have to be tested (at least) against the three standards ordinarily applied to test restrictions on the freedom of speech.[43] It held that suspension of Internet services is a "drastic measure" that must be considered by the state only if it is "necessary" and "unavoidable," after assessing the "existence of an alternate less intrusive remedy."

Human Rights Watch and Internet Freedom Foundation identified 127 shutdowns in the three years between the Supreme Court's *Anuradha Bhasin* judgment in January 2020 and December 31, 2022.[44] Of 28 Indian states, 18 shut down the Internet at least once in these three years. Local authorities used Internet shutdowns in 54 cases to prevent or in response to protests, 37 to prevent cheating in school examinations or exams for government jobs, 18 in response to communal violence, and 18 for other law and order concerns. This number barely included Internet shutdowns in the Union Territory of Jammu and Kashmir, where the authorities continued to shut down the Internet more than any other place in the country.

The persistence of Internet shutdowns in India, particularly in an era of 'Digital India', where the government actively promotes Internet access as a key development tool, presents significant contradictions. These disruptions interfere with essential social protection programs, such as the National Food Security Act, which provides subsidised food grains through a targeted public distribution system. Additionally, shutdowns hamper rural banking services, delay utility bill payments, and obstruct access to official documentation—all of which disproportionately impact marginalised communities.

---

41 Amnesty International, 'Uganda: Opposition Politician Charged after Abduction: Kizza Besigye' (*Amnesty International*, 26 November 2024) <https://www.amnesty.org/en/documents/afr59/8779/2024/en/> accessed 17 February 2025

42 Danai Nesta Kupemba & Ian Wafula, 'Manhandled and choked - Tanzanian activist recounts abduction' (*BBC News Online* (London), 13 January 2025) <https://www.bbc.com/news/articles/cd7dxz48e0lo/> accessed 20 February 2025

43 Hardwaj, Shrutanjaya; Nayak, Nakul; Dandamudi, Raja Venkata Krishna; Singh, Sarvjeet; and Handa, Veda (2020) "Rising Internet Shutdowns in India: A Legal Analysis," *Indian Journal of Law and Technology*: Vol. 16: Iss. 1, Article 7.<https://repository.nls.ac.in/ijlt/vol16/iss1/7/> accessed 20 February 2025

44 Human Rights Watch, 'No Internet Means No Work, No Pay, No Food' (*Human Rights Watch*, 14 June 2023) <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic#:~:text=the%20court%20said:-,Arbitrary%20Internet%20Shutdowns,once%20in%20these%20three%20years./> accessed 20 February 2025

Governments often justify Internet shutdowns by citing concerns over mob violence fuelled by online misinformation. However, United Nations human rights experts in the 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations stated that even in times of civil unrest, "using communications 'kill switches' can never be justified under human rights law." The UN Human Rights Council further reinforced this stance in 2016, unequivocally condemning Internet shutdowns and urging states to "refrain from and cease such measures."

Moreover, the International Covenant on Civil and Political Rights (ICCPR)—to which India is a party—recognises Internet access as an enabler of fundamental human rights. In 2021, the UN Secretary-General emphasised the need for universal Internet access as a human right by 2030, further highlighting the incompatibility of blanket Internet shutdowns with international legal standards.

A Case Study of South Africa

In contrast to India, South Africa has a strong legal framework that protects Internet access as a fundamental right. The Constitution of South Africa, 1996, explicitly guarantees freedom of expression, including digital communication. Key legislations such as the Electronic Communications Act, 2005, and the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), 2002, regulate government intervention in telecommunications, ensuring that any restrictions align with constitutional safeguards. Notably, South Africa lacks specific laws permitting arbitrary Internet shutdowns.

The judiciary has consistently upheld the Internet's role in fostering democratic participation and economic growth, reinforcing that any restrictions must conform to constitutional mandates. However, while South Africa has not yet experienced large-scale Internet shutdowns, it is a growing and pernicious problem in Sub-Saharan Africa. Ordered by states to telecommunications companies, Internet shutdowns infringe on the right to freedom of expression, disrupt online services and create losses for telecoms companies. Incidents are on the rise, despite growing authoritative guidance that Internet shutdowns infringe on international human rights law.[45]

Identified Gaps and Improvement Areas for Kenya.

A comparative analysis of legal frameworks on Internet shutdowns in India and South Africa highlights critical regulatory gaps in Kenya's approach. India, despite its controversial history of frequent shutdowns, has a formalised legal framework under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, which grants government officials the authority to order shutdowns under specific conditions.[46] In contrast, South Africa leans towards stronger constitutional protections, recognising access to the Internet as an extension of fundamental rights such as freedom of expression and access to information.[47]

Kenya, however, lacks explicit legal provisions governing Internet shutdowns, resulting in legal ambiguity, weak oversight, and a heightened risk of human rights violations. The following are key gaps and areas for improvement:

i. Weak Constitutional Protection for Internet Access.

To prevent future Internet shutdowns, the Kenyan government must prioritise respecting and protecting constitutional and human rights, particularly freedom of expression, access to information, and peaceful assembly. These rights are fundamental and should not be compromised by Internet shutdowns.

---

45 Business and Human Rights Resource Centre, 'Internet shutdowns in Africa: Addressing the human rights responsibilities of telecoms companies' (*Business and Human Rights Resource Centre,* 10 May 2023) <https://www.business-humanrights.org/en/from-us/briefings/internet-shutdowns-in-africa-addressing-the-human-rights-responsibilities-of-telecoms-companies//>accessed 20 February 2025

46 Bailey, Rishab & Parsheera, Smriti. 'Data localisation in India: Questioning the means and ends,' (Working Papers 18/242, National Institute of Public Finance and Policy 2018) <https://ideas.repec.org/p/npf/wpaper/18-242.html/> accessed 22 February 2025

47 Arthur Gwagwa and others, 'Artificial Intelligence (AI) Deployments in Africa: Benefits, Challenges and Policy Dimensions' (2020) 26 The African Journal of Information and Communication 3 <http://dx.doi.org/10.23962/10539/30361> accessed 19 February 2025

It is also crucial for the government to commit to transparency and accountability, providing comprehensive explanations for any Internet shutdowns. Ensuring that such decisions are made transparently and with clear accountability allows the public to understand the reasons behind these significant actions.

ii. Lack of Clear Legal Provisions regulating Internet shutdowns

Kenya has no legal framework explicitly addressing Internet shutdowns, creating a regulatory vacuum. While the Kenya Information and Communications Act (KICA), 1998, grants the Communications Authority (CA) the power to regulate telecommunications, it does not explicitly address Internet shutdowns or outline due process for imposing restrictions (KICA, 1998).

In contrast, India's legal framework provides structured, though often criticised, guidelines for implementing shutdowns, requiring formal authorisation from high-level government officials and periodic review mechanisms.[48]

Kenya should consider developing explicit statutory provisions that define who has the authority to impose an Internet shutdown, what justifications are legally acceptable and how oversight mechanisms can be implemented to prevent arbitrary shutdowns.

iii. Limited public oversight and transparency

Building on the need to protect fundamental rights, it is essential to address the role of regulatory bodies in managing Internet shutdowns. To this end, the Communications Authority of Kenya (CA) must strengthen its regulatory oversight by clarifying its role during Internet shutdowns and ensuring robust regulatory procedures. Clear guidelines and procedures should be established to manage these situations effectively and fairly.

Simultaneously, telecommunication companies should take a proactive stance by resisting unwarranted government directives and refraining from sharing customer data in contravention of the Kenya Information and Communications Act 1998.[49]

Additionally, they should maintain transparency regarding government requests for data or directives to shut down services. This approach protects customer privacy and ensures companies act in the best interests of their users.

iv. Negative socio-economic impact

Governments often mistakenly believe that Internet shutdowns will quell unrest, stop the spread of misinformation, reduce harm from cybersecurity threats, or curb cheating in the case of exam-related shutdowns in Algeria. But shutdowns are highly disruptive to economic activity. They halt e-commerce, generate losses in time-sensitive transactions, increase unemployment, interrupt business-customer communications, and create financial and reputational risks for companies.[50]

Similar to the situation in India, Internet shutdowns in Kenya have disrupted businesses, interfered with financial transactions, and undermined access to essential services. During the shutdown witnessed on 26th June, with disruptions evidenced with mobile money services, credit and debit card transactions, and e-commerce platforms were all inaccessible, the Internet Society estimates that such outages could cost Kenya approximately $6.3 million in lost GDP per day.[51]

---

48 Bailey, Rishab & Parsheera, Smriti. 'Data localisation in India: Questioning the means and ends,' (Working Papers 18/242, National Institute of Public Finance and Policy 2018) <https://ideas.repec.org/p/npf/wpaper/18-242.html/> accessed 22 February 2025

49 Kenya Information and Communications Act 1998 (c 411A) s 31

50 Robert Mitchelle, 'The Real Impact of Internet Shutdowns'(*Internet Society*, 28 June 2023) <https://www.internetsociety.org/blog/2023/06/the-real-impact-of-internet-shutdowns/> accessed 21 February, 2025

51 Mwenda Kivuva, 'Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 demonstrations'(*KiC-TAnet*, 26 June 2024) <https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinance-bill2024-demonstrations/> accessed 21 February 2025

v. Transparency and Accountability

Several African countries, like Kenya, often justify Internet shutdowns on the grounds of national security and public order. In Kenya, national security is defined under Article 238 of the Constitution as "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability, prosperity, and other national interests."[52] The Constitution further provides that national security must conform to constitutional principles, follow the highest human rights standards, and respect the diversity of cultures.

Any Internet shutdown in Kenya justified under the pretext of national security must therefore meet constitutional standards, including the three-part test of legality, proportionality, and necessity when limiting human rights such as freedom of expression and access to information.[53]

For instance, Article 24(2) of the Constitution requires that any law limiting rights must be specific about the right being curtailed and the purpose of such limitation, ensuring that it does not undermine the core content of the affected right.

The case of *Okuta v Republic*[54] demonstrated the application of the proportionality test in evaluating whether pre-2010 laws remained justifiable under the new constitutional framework. The court found that the availability of alternative legal mechanisms, such as the National Cohesion and Integration Act and provisions on national security, could achieve the same objectives without resorting to outdated and potentially unconstitutional laws.

Despite these constitutional safeguards, Kenya's law enforcement agencies, including the National Security Council (chaired by the President), the Directorate of Criminal Investigations, and the National Intelligence Service, have faced criticism for their role in past Internet shutdowns.

This raises fundamental questions about the legal authority under which such orders were issued and whether they complied with constitutional and statutory requirements.

The Executive, through the Ministry of ICT, has established the ICT Authority as a state corporation under Legal Notice 183 of 2013, tasked with supervising the design, development, and implementation of critical ICT projects across the public sector. Additionally, the Communications Authority of Kenya (CA), established under the Kenya Information and Communications Act of 1998, serves as the statutory regulator of the ICT sector. It oversees the dissemination and management of information within the industry, including content shared on social media platforms.

Beyond government agencies, private corporations such as telecommunications companies and Internet service providers (ISPs) play a crucial role in enforcing shutdown orders. This raises significant concerns about the legality of such directives, whether due process was followed, and the extent of accountability among state and non-state actors. The involvement of private entities in executing shutdowns further complicates the issue of transparency, as decisions affecting public access to information are often made without sufficient public scrutiny or judicial oversight. Ultimately, transparency and accountability in Kenya's Internet governance framework become paramount.

Communications Authority of Kenya(CAK)

Sections 23 and 25 of the KICA, mandate the CA to protect the interests of all users of telecommunications services in Kenya with respect to tariffs, quality of service and availability of diverse products and services among others. This oversight is mainly achieved through grant of licenses and monitoring and enforcement of the various license conditions.

---

52 Constitution of Kenya 2010.

53 ibid

54 *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR (Petition No. 397 of 2016)

The #RejectFinanceBill2024 protests in Kenya were a significant political event marked by widespread public opposition to new tax measures proposed in the Finance Bill 2024. During the anti-tax protests against the Finance Bill 2024, concerns arose about a potential Internet shutdown.[55] The Communications Authority of Kenya (CA), through its director general, assured the public that there were no intentions to disrupt Internet services, aligning any such action with an infringement of the Constitution.[56] Despite this, disruptions occurred[57], raising questions about the true intentions behind the actions.

The recent Internet shutdowns can be attributed to several factors, despite official statements denying intentional plans. Firstly, and more importantly, government intervention appears to be a significant cause, as the disruptions suggest deliberate action to control the flow of information.[58] This starkly contrasts with official denials, which claimed no such plans were in place.

The Communications Authority is established as an independent body that should ideally not maintain functional or financial interests with the executive or commercial interests. This objective is achieved through independent appointment of the Board and economic autonomy as the Regulator is funded by licence fees that it collects from licensees or directly from the national budget.[59] However, Section 5C of KICA grants the Cabinet Secretary an avenue to issue policy guidelines to the Authority.

Having witnessed actual Internet shutdown in Kenya, the regulator must maintain its independence in making decisions about the Internet. This can be achieved through transparency in decision making, that is, explaining explicitly the legal basis, nature and extent of controls to the Internet and communication technologies.

Telecom Providers

Telecommunications companies empower people to exercise freedom of expression, but they can also enable politically motivated attempts to control online information flow. Kenya is a champion of the digital economy and has a strong reputation for putting technology to work for people's rights and interests. Telcos have a duty to reject government orders for a shutdown and respect human rights. They also have several tools to ensure this pushback is effective. Safaricom and Airtel are both parties to the United Nations Global Compact, which includes a commitment to respect and protect "internationally proclaimed human rights." Experts at the U.N. have explicitly affirmed that human rights apply online and have condemned Internet shutdowns.

A new report by U.N. special rapporteur David Kaye finds that shutdowns "involve measures to intentionally prevent or disrupt access to or dissemination of information online *in violation of human rights law*." Given these statements, we believe that telcos that are party to the Global Compact must refrain from intentionally disrupting networks.[60]

The role of communications companies in these protests is not only about Internet connectivity. Safaricom, Kenya's dominant telecommunications provider, has been blamed for sharing data with law enforcement facilities to facilitate the surveillance and abduction of people linked to the anti-finance bill movement. Safaricom has denied these claims, but the Office of the Data Protection Commissioner has yet to investigate

---

55 Kenyans.co.ke, 'Communications Authority of Kenya Assures Public There Will Be No Internet Shutdown,' <https://www.kenyans.co.ke/news/101971-govt-addresses-internet-shutdown-nairobi-during-finance-bill-protests> accessed 22 February 2025

56 ibid

57 Cloudflare Radar, 'Outage Center: Internet outages and traffic anomalies- 25th June 2024,' <https://radar.cloudflare.com/outage-center?dateStart=2024-06-25&dateEnd=2024-06-25> accessed 22 February 2025

58 Association for Progressive Communications, 'Digital protests, access and freedoms in Kenya,' <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 22 February 2025

59 Grace Mutung'u and others, 'Building trust between the state and citizens: A policy brief on Internet shutdowns and elections in Kenya 2017' (KiCTAnet 2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 22 February 2025

60 Tinuola Dada and Peter Micek, 'Election watch: If Kenya orders an Internet shutdown, will telcos help #KeepItOn?' (*AccessNow*, 26 July 2017) <https://www.accessnow.org/election-watch-kenya-orders-internet-shutdown-will-telcos-help-keepiton/%3eaccessed> 22 February 2025

the complaints.[61] As of 27 June 2024, some abducted protesters linked to the movement remained missing, raising concerns about telecom accountability and transparency in executing government directives.

To improve transparency, telecom operators should consider informing subscribers in advance of potential service disruptions and involving them, where possible, in discussions with other stakeholders to avert shutdowns. In the event of a government-ordered shutdown, mobile network operators (MNOs) should disclose the nature and extent of the disruption and engage in dialogue with affected users about its impact. AccessNow, a digital rights advocacy group, has proposed a ten-point plan to guide telecom operators in upholding human rights.

This includes mechanisms for handling customer grievances, policies ensuring timely investigations, and provisions for compensating those affected by service disruptions. While companies like Safaricom do compensate subscribers for general service outages, it remains unclear whether compensation applies in cases of government-mandated shutdowns. This question could be addressed through a consultative process involving all affected stakeholders.

Ultimately, resolving these challenges requires further study of dispute resolution mechanisms for regulatory actions and checks and balances on the regulator as an independent constitutional body. Additionally, greater transparency in the licensing process is needed to ensure that telecom operators are not compelled to take actions that could potentially violate human rights.[62]

Case Studies on Internet Shutdowns and Their Implications for Kenya

1. Kenya's 2017 General Election and Internet Disruptions

Concerns over digital restrictions and potential interference with online communications marked Kenya's 2017 general elections. Reports from digital rights organisations such as Access Now and Article 19 indicate that government agencies allegedly pressured telecom providers to restrict access to social media and messaging platforms, particularly during heightened political activity.

This phenomenon aligns with broader global trends where states resort to Internet shutdowns to control information flows, particularly during elections or civil unrest. The documented patterns of state-driven digital repression situate Kenya's case within a larger framework of governments leveraging Internet disruptions to influence political discourse and suppress dissent.[63] Furthermore, the use of Internet disruptions raises concerns about the violation of fundamental rights, including freedom of expression and access to information, as protected under Articles 33 and 35 of the Kenyan Constitution and international human rights instruments such as the African Charter on Human and Peoples' Rights (ACHPR).

2. Uganda's 2021 Election and Its Implications for Kenya

Although not a Kenyan case, Uganda's 2021 general elections offer critical insights into regional Internet governance challenges. The Ugandan government imposed a total Internet shutdown on January 13, 2021, just before the election, effectively cutting off communication for several days. Human Rights Watch (2021) and other advocacy groups condemned the move, noting its impact on transparency, election monitoring, and the free flow of information.[64]

---

61 Mwenda Kivuva, 'Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 demonstrations'(*KiC-TAnet,* 26 June 2024) <https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinance-bill2024-demonstrations/> accessed 21 February 2025

62 Grace Mutung'u and others, 'Building trust between the state and citizens: A policy brief on Internet shutdowns and elections in Kenya 2017' (KiCTAnet 2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 22 February 2025

63 Freedom House, 'Key Developments, June 1, 2017 - May 31, 2018', <https://freedomhouse.org/country/kenya/freedom-net/2018> accessed 22 February 2025

64 World Report 2022: Uganda (Human rights Watch) <https://www.hrw.org/world-report/2022/country-chapters/uganda> accessed 22 February 2025

The Ugandan shutdown raised serious concerns for Kenya due to shared telecommunications infrastructure and business interests. Kenyan telecom providers such as Safaricom and Airtel, which operate in Uganda, faced scrutiny over their role in enforcing the blackout. This case underscores the potential for similar actions in Kenya, especially given precedents in restricting online spaces during politically sensitive periods. Additionally, it highlights the broader East African regulatory landscape, where governments may draw inspiration from each other's digital governance approaches.

3. India's Internet Shutdowns

India, widely regarded as the global leader in Internet shutdowns, presents a legal framework that could influence Kenya's judicial and regulatory approach. The landmark case of ***Anuradha Bhasin v. Union of India (2020)***[65] set an important precedent. The court ruled that indefinite Internet shutdowns violate constitutional freedoms and must adhere to the principles of necessity and proportionality.

The judgment emphasised that any restriction on Internet access must be (a) based on clear legal grounds, (b) subject to judicial review, and (c) implemented as a last resort.

Given Kenya's Constitutional Article 24 on limitations of rights,[66] this ruling could serve as a reference for future legal challenges against government-imposed Internet disruptions in Kenya. It also aligns with the Kenyan High Court's 2021 decision in ***Bloggers Association of Kenya v. Attorney General***[67] where the court ruled to protect digital rights against state overreach.

Human Rights Impact.

From time to time, governments across the world's respect for human rights has been tested in several ways. Still, arguably, nothing has tested it more than the rise of civil activities that take place over the Internet.[68] As highlighted earlier, the Internet has become indispensable for communication, education, business, and even political participation. It has enabled individuals to freely and more easily do almost everything with a click of a button or a tap on a screen.

Expectedly, these powers and opportunities that the Internet has given to individuals are prone to abuse, and to prevent such abuse, laws have allowed governments to use disruptive measures such as Internet shutdowns.[69]

On the flipside, though, these measures are applied haphazardly without clear regulations and cause gross human rights violations as discussed hereunder.

Various justifications are given by governments whenever they intentionally disrupt the Internet (partial or total blackouts), including national security concerns, prevention of misinformation and curbing civil unrest, among others.[70] The broader adverse consequences of this are twofold: Firstly, the indeterminate nature of these justifications acts as a loophole for abuse of power; and secondly, these actions disproportionately affect socio-economic rights and fundamental freedoms, particularly among vulnerable populations. For example, in the age of e-commerce, small businesses such as those that rely on social media and digital platforms for marketing and transactions suffer significant losses during these shutdowns.[71]

---

65 Anuradha Bhasin v Union of India AIR 2020 SC 1308

66 Constitution of Kenya, 2010.

67 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR (Kenya)

68 Ewan Sutherland, 'The Internet and Human Rights: Access, Shutdowns, and Surveillance' (WG Hart Legal Workshop 2018, London, 11-12 June 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203883> accessed 22 February 2025

69 ibid

70 Office of the United Nations High Commissioner for Human Rights (OHCHR), 'Dramatic Real-Life Effects of Internet Shutdowns on People's Lives and Human Rights' (Press Release, 23 June 2022) <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human > accessed 22 February 2025

71 Ibid

Furthermore, rural women and children who depend on digital resources for education, healthcare, and economic empowerment get lockedout whenever Internet shutdowns occur.[72]

As the population using the Internet continues to grow, there is a need to protect their fundamental rights. Indeed, this has been recognised under international law with institutions such as the United Nations Human Rights Council (UNHRC) affirming that "the same rights that people have offline must also be protected online, in particular freedom of expression."[73] The **International Covenant on Civil and Political Rights (ICCPR, 1966)** further provides that:

"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[74]

This right is to be exercised without unwarranted interference unless it is for the sake of respect of the rights or reputations of others; protection of national security or public order (ordre public), or of public health or morals.[75] While these interferences are supposed to set limits when a right is exercised at the expense of the rights of others, Internet shutdowns end up being used as tools of control, which undermine human rights more than they protect them.[76] As such, they should be cautiously utilised and, in most cases, they should only be used as a last resort.

Furthermore, the effects of Internet outages go beyond the short-term interruptions. They worsen the digital divide by restricting opportunities for economic involvement and disproportionately harming members of vulnerable communities. For instance, when the Internet connection is cut off during elections, demonstrations, or emergencies, it hinders transparency and reduces civic participation, preventing people from making reasoned decisions. Such outrageous acts must be seen as a violation of Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the Universal Declaration of Human Rights (UDHR, 1948), among other laws.

Although this right is recognised under the umbrella of access to information and freedom of expression, it is also related to other rights, such as socio-economic rights. The focus lies on freedom of expression and access to information while demonstrating how any interference with these rights has a ripple effect towards other rights.

Rights under International Law

Since the Constitution of Kenya has accepted international laws to form part of Kenyan laws, accessing the Internet as a right is protected under various international instruments, as already observed.[77] This is guaranteed through fundamental rights and freedoms like free speech and access to information. To contextualise this, the UDHR, for example, under Article 19, guarantees the right to freedom of expression.[78] The same is reinforced under Article 19 (2) of the ICCPR, which reinforces this principle in Article 19(2), which protects the right to seek, receive, and impart information and ideas of all kinds, regardless of frontiers.[79]

---

72 Advocacy Assembly, 'The gendered impact of Internet shutdowns' (Advocacy Assembly, 2023) <https://advocacyassembly.org/en/news/245> accessed 23 February 2025

73 United Nations Human Rights Council (UNHRC), 'The promotion, protection and enjoyment of human rights on the Internet' (27 June 2016) UN Doc A/HRC/RES/32/13

74 International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, 999 UNTS 171, art 19(2)

75 Ibid

76 Jay T. Conrad, 'A New Right is the Wrong Tactic: Bring Legal Actions Against States for Internet Shutdowns Instead of Working Towards a Human Right to the Internet (Part 1)' (2023) 13 *Seattle Journal of Technology, Environmental & Innovation Law* 2

77 Constitution of Kenya 2010, Art 2 (6).

78 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) Art 19.

79 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19(2)

Moreover, the General Comment No. 34 (2011) by the Human Rights Committee has interpreted this provision explicitly by stating:[80]

"Paragraph 2 protects all forms of expression and the means of their dissemination. Such forms include spoken, written, and sign language, as well as non-verbal expressions such as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions. They include all forms of audio-visual as well as electronic and Internet-based modes of expression."[81]

Furthermore, it encourages States parties to take account that the extent to which developments in information and communication technologies, such as Internet and mobile-based electronic information dissemination systems, have substantially changed communication practices around the world.[82] Therefore, states should be cautious against arbitrary Internet restrictions limiting this freedom. Any limitations on Internet access must be necessary, proportionate, and in line with international human rights standards.

Continentally, the African Charter on Human and Peoples' Rights provides for the right to access information under Article 9.[83] It states that every individual has a right to receive information and freely express their opinions. Furthermore, the African Declaration on Internet Rights and Freedoms (2014) advocates for the promotion of Internet accessibility, digital inclusion, and the protection of online freedoms.[84] This declaration urges African states to refrain from arbitrary shutdowns and states that everyone should enjoy unrestricted access to the Internet.[85] Any shutting down or blocking of access to social networking platforms, and in fact, the Internet in general, constitutes a direct interference with this right. Free and open access to the Internet must therefore always be protected.

The African Commission on Human and Peoples' Rights has also reiterated the significance of the rights and freedoms guaranteed under Article 9 of the African Charter, which are to be enjoyed even in the digital space.[86] States must protect them, and state-imposed restrictions must meet the standards of legality, necessity, and proportionality. In the Commission's Resolution 362 (2016) on the Right to Freedom of Information and Expression on the Internet in Africa, there is explicit condemnation of the disruption of the Internet as a tool to suppress dissent and hinder access to information and freedom of expression.[87]

The same has a ripple effect that even affects other rights. For instance, children under the Competency-Based Curriculum may run into problems in their studies as they heavily rely on materials available online.[88] On top of that, many Micro, Small and Medium Enterprises (MSMEs) which constitute 98% of all business, create 30% of jobs annually and contribute 40% towards the country's GDP are have in the recent past heavily relied on the Internet for marketing and transactions and any shutdown of the Internet jeopardise their potential and their contribution to the economy[89]. Rightly then, the Commission emphasises the need for states to be hesitant when it comes to Internet shutdowns.

---

80 UN Human Rights Committee, 'General Comment No. 34: Article 19, Freedoms of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34, para 12.

81 ibid

82 Ibid

83 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev 5, Art 9.

84 African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (adopted 10 November 2019)

85 Ibid

86 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev 5, Art 9

87 African Commission on Human and Peoples' Rights, 'Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa' (4 November 2016) ACHPR/Res.362(LIX)2016

88 Kenya Institute of Curriculum Development, 'Competency-Based Curriculum Materials' <https://kicd.ac.ke/cbc-materials/> accessed 23 February 2025

89 Kenya National Bureau of Statistics, '2016 Micro, Small and Medium Enterprises (MSME) Survey Basic Report' (2016) <https://www.knbs.or.ke/2016-micro-small-and-medium-enterprises-msme-survey-basic-report/ > accessed 23 February 2025.

Rights under the Constitution and Kenyan Laws

Key and essential provisions of the Constitution of Kenya that can be interpreted to guarantee access to the Internet are under Article 33 and 35 on freedom of expression and right to access information, respectively. Article 33 provides that every person has the right to freedom of expression, which includes: freedom to seek, receive or impart information or ideas;[90] freedom of artistic creativity;[91] and academic freedom and freedom of scientific research.[92] This right however does not extend to: propaganda for war;[93] incitement to violence;[94] hate speech;[95] or advocacy of hatred that either constitutes ethnic incitement, vilification of others or incitement to cause harm; or is based on any ground of discrimination specified or contemplated in Article 27(4).[96]

Article 35 then guarantees the right of access to: information held by the State;[97] and information held by another person and required for the exercise or protection of any right or fundamental freedom.[98]

It is already established in law that a right or a fundamental freedom cannot be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. [99] The unjustified nature of limitations of these rights, as observed in this paper, is a gross violation of the Constitution and the rule of law and causes a disruption even in enjoying other rights and freedoms.

To demonstrate this disruption, the right to property, as enshrined in Article 40 of the Constitution, is one of the social and economic rights compromised by Internet shutdowns.[100] Where businesses that rely on the Internet are undermined. Other rights under this category, such as access to education, healthcare, and economic participation, are also affected negatively by Internet shutdown.[101] Finally, Article 46, which deals with consumer rights, requires that citizens get access to quality goods and services, which is violated in cases such as where mobile banking, e-commerce, and other digital services are disrupted due to an Internet shutdown.[102]

Digital rights are fundamental human rights, and as such, not absolute. As with most rights, they may be lawfully restricted where the restrictions are reasonable and justifiable in an open and democratic society.

Article 24 of the Constitution stipulates that limitations should align with the principles of legality, necessity and proportionality. Further, as confirmed in General Comment 34 and Principle 9 of the African Declaration,[103] the restrictions that states impose should not jeopardise these rights. In practice, this requires that any measures limiting digital rights, such as Internet shutdowns, surveillance, or content blocking, must be transparent, subject to judicial oversight, and accompanied by precise mechanisms for accountability and redress.

---

90 Constitution of Kenya 2010, Art 33 (1) (a).

91 Ibid, Art 33 (1) (b).

92 Ibid, Art 33 (1) (c).

93 Ibid, Art 33 (2) (a).

94 Ibid, Art 33 (2) (b).

95 Ibid, Art 33 (2) (c).

96 Ibid, Art 33 (2) (d).

97 Ibid, Art 35 (1) (a).

98 Ibid, Art 33 (1) (b).

99 Ibid, Art 24 (1); *In the Matter of the Principle of Gender Representation in the National Assembly and the Senate* [2012] KESC 5 (KLR).

100 Constitution of Kenya 2010, Art 40.

101 Ibid, Art 43.

102 Ibid, Art 46.

103 African Declaration no.6.

Although there is an expansive legal framework, enforcement of the same remains a challenge. The infrequency at which the government shuts down the Internet has excellent implications, including the erosion of investor confidence, deterrence of innovation, and stifling economic growth.

REFERENCES

Books

1. Balkin JM, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society* (Routledge 2017)

Journal Articles

2. Bhatia KV and others, 'Protests, Internet Shutdowns, and Disinformation in a Transitioning State' (2023) 45 *Media, Culture & Society* 1101
3. Conrad JT, 'A New Right is the Wrong Tactic: Bring Legal Actions Against States for Internet Shutdowns Instead of Working Towards a Human Right to the Internet (Part 1)' (2023) 13 *Seattle Journal of Technology, Environmental & Innovation Law* 2
4. Gwagwa A and others, 'Artificial Intelligence (AI) Deployments in Africa: Benefits, Challenges and Policy Dimensions' (2020) 26 *African Journal of Information and Communication* 3
5. Hardwaj S and others, 'Rising Internet Shutdowns in India: A Legal Analysis' (2020) 16 *Indian Journal of Law and Technology* 1
6. Sugow A and others, 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression' (2021) 1 *Journal of Intellectual Property and Information Technology Law* 1

Cases

7. *Anuradha Bhasin v Union of India* AIR 2020 SC 1308
8. *Association des Blogueurs de Guinee (ABLOGUI) v State of Guinea* [2023] ECOWASCJ 1
9. *Bloggers Association of Kenya (BAKE) v Attorney General* [2020] eKLR
10. *Geoffrey Andare v Attorney General* [2016] eKLR
11. *In the Matter of the Principle of Gender Representation in the National Assembly and the Senate* [2012] KESC 5 (KLR)
12. *Jacqueline Okuta v Attorney General* [2017] eKLR

Legislation

13. Computer Misuse and Cybercrimes Act 2018 (Kenya)
14. Constitution of Kenya 2010
15. Data Protection Act 2019 (Kenya)
16. Kenya Information and Communications Act 1998 (Kenya)
17. National Cohesion and Integration Act 2008 (Kenya)
18. Prevention of Terrorism Act 2012 (Kenya)

International Treaties and Conventions

19. African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev 5

20. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

21. Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III)

Official Documents

22. African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (10 November 2019)

23. African Commission on Human and Peoples' Rights, 'Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa' (4 November 2016) ACHPR/Res.362(LIX)2016

24. Ruggie J, 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises' (21 March 2011) UN Doc A/HRC/17/31

25. UNGA Res 78/213 (22 December 2023) UN Doc A/RES/78/213

26. UNHRC, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (27 June 2016) UN Doc A/HRC/RES/32/13

27. UN Human Rights Committee, 'General Comment No. 34: Article 19, Freedoms of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34

Reports

28. ARTICLE 19, 'Getting Connected: Freedom of Expression, Telcos and ISPs' (June 2017) <https://www.article19.org/wp-content/uploads/2017/06/Getting-Connected-2.pdf> accessed 7 April 2025

29. ARTICLE 19, 'Kenya: Release and Cease Attacks on Edwin Mutemi wa Kiama' (8 April 2021) <https://www.article19.org/resources/kenya-cease-attacks-on-and-release-edwin-mutemi-wa-kiama/> accessed 18 March 2025

30. Freedom House, 'Kenya: Freedom on the Net 2024 Country Report' (Freedom House 2024) <https://freedomhouse.org/country/kenya/freedom-net/2024> accessed 22 February 2025

31. Human Rights Watch, 'Kenya: Police Threaten Activists Reporting Abuse' (4 June 2018) <https://www.hrw.org/news/2018/06/04/kenya-police-threaten-activists-reporting-abuse> accessed 22 February 2025

32. Human Rights Watch, 'No Internet Means No Work, No Pay, No Food' (14 June 2023) <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic> accessed 20 February 2025

33. Kenya National Bureau of Statistics, '2016 Micro, Small and Medium Enterprises (MSME) Survey Basic Report' (2016) <https://www.knbs.or.ke/2016-micro-small-and-medium-enterprises-msme-survey-basic-report/> accessed 23 February 2025

34. Mutung'u G and others, 'Building Trust between the State and Citizens: A Policy Brief on Internet Shutdowns and Elections in Kenya 2017' (KiCTAnet 2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 22 February 2025

Conference Papers

35. Sutherland E, 'The Internet and Human Rights: Access, Shutdowns, and Surveillance' (WG Hart Legal Workshop, London, 11-12 June 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203883> accessed 22 February 2025

36. '6 Media Houses Warned over Coverage of Azimio Mass Action Protest' (Pulselive Kenya, 29 July 2024) <https://www.pulselive.co.ke/articles/news/local/citizen-tv-ntv-k24-kbc-tv47-and-ebru-tv-warned-over-coverage-of-azimio-protest-2024072908514395101> accessed 15 February 2025

37. 'Communications Authority of Kenya Assures Public There Will Be No Internet Shutdown' (Kenyans.co.ke) <https://www.kenyans.co.ke/news/101971-govt-addresses-internet-shutdown-nairobi-during-finance-bill-protests> accessed 22 February 2025

38. 'Competency-Based Curriculum Materials' (Kenya Institute of Curriculum Development) <https://kicd.ac.ke/cbc-materials/> accessed 23 February 2025

39. 'Digital Protests, Access and Freedoms in Kenya' (Association for Progressive Communications) <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 22 February 2025

40. 'Digital Protests, Access and Freedoms in Kenya' (APC, 18 July 2024) <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 18 March 2025

41. 'Dramatic Real-Life Effects of Internet Shutdowns on People's Lives and Human Rights' (OHCHR, 23 June 2022) <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human> accessed 22 February 2025

42. 'Election Watch: If Kenya Orders an Internet Shutdown, Will Telcos Help #KeepItOn?' (AccessNow, 26 July 2017) <https://www.accessnow.org/election-watch-kenya-orders-internet-shutdown-will-telcos-help-keepiton/> accessed 22 February 2025

43. 'Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?' (Carnegie Endowment for International Peace, March 2022) <https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en> accessed 18 March 2025

44. 'Internet Shutdowns in Africa: Addressing the Human Rights Responsibilities of Telecoms Companies' (Business and Human Rights Resource Centre, 10 May 2023) <https://www.business-humanrights.org/en/from-us/briefings/internet-shutdowns-in-africa-addressing-the-human-rights-responsibilities-of-telecoms-companies/> accessed 20 February 2025

45. 'Kenya Borrows Leaf From Peers on Internet Restriction' (The East African, 27 June 2024) <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-borrows-leaf-from-peers-on-internet-restriction-4671858> accessed 22 February 2025

46. 'Kenya Plans to Place Public Security above Data Privacy. That's a Bad Idea' (The Conversation, 11 February 2019) <http://theconversation.com/kenya-plans-to-place-public-security-above-data-privacy-thats-a-bad-idea-111099> accessed 17 February 2025

47. 'Key Developments, June 1, 2017 – May 31, 2018' (Freedom House) <https://freedomhouse.org/country/kenya/freedom-net/2018> accessed 22 February 2025

48. 'Manhandled and Choked – Tanzanian Activist Recounts Abduction' (BBC News, 13 January 2025) <https://www.bbc.com/news/articles/cd7dxz48e01o/> accessed 20 February 2025

49. 'Outage Center: Internet Outages and Traffic Anomalies – 25th June 2024' (Cloudflare Radar) <https://radar.cloudflare.com/outage-center?dateStart=2024-06-25&dateEnd=2024-06-25> accessed 22 February 2025

50. 'Proposal to Block Websites and Applications Threatens Kenya's Digital Ecosystem' (KiCTAnet, 2 October 2024) <https://www.kictanet.or.ke/proposal-to-block-websites-and-applications-threatens-kenyas-digital-ecosystem/> accessed 23 February 2025

51. 'Proposed Changes to Kenya's Constitution: A Look at the 2024 Amendment Bill' (Sharp Daily, 2 October 2024) <https://thesharpdaily.com/kenya-constitutional-amendment-bill-2024/> accessed 23 February 2025

52. 'State Surveillance: Kenyans Have a Right to Privacy – Does the Government Respect It?' (The Conversation, 29 November 2024) <https://www.polity.org.za/article/state-surveillance-kenyans-

have-a-right-to-privacy-does-the-government-respect-it-2024-11-29> accessed 13 February 2025

53. 'Surge in Abductions of Government Critics in Kenya Sparks Mass Public Outcry' (Peoples Dispatch, 14 January 2025) <https://peoplesdispatch.org/2025/01/14/surge-in-abductions-of-government-critics-in-kenya-sparks-mass-public-outcry/> accessed 17 February 2025

54. 'Technology-Facilitated Rights and Digital Authoritarianism: Examining the Recent Internet Shutdown in Kenya' (CIPIT, 9 August 2024) <https://cipit.org/technology-facilitated-rights-and-digital-authoritarianism-examining-the-recent-internet-shutdown-in-kenya/> accessed 15 February 2025

55. 'The Gendered Impact of Internet Shutdowns' (Advocacy Assembly, 2023) <https://advocacyassembly.org/en/news/245> accessed 23 February 2025

56. 'The Real Impact of Internet Shutdowns' (Internet Society, 28 June 2023) <https://www.internetsociety.org/blog/2023/06/the-real-impact-of-internet-shutdowns/> accessed 21 February 2025

57. 'Uganda Election: Facebook and WhatsApp Blocked' (BBC News, 18 February 2016) <http://www.bbc.com/news/world-africa-35601220> accessed 18 March 2025

58. 'Uganda: Opposition Politician Charged after Abduction: Kizza Besigye' (Amnesty International, 26 November 2024) <https://www.amnesty.org/en/documents/afr59/8779/2024/en/> accessed 17 February 2025

59. 'Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 Demonstrations' (KICTAnet, 26 June 2024) <https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinancebill2024-demonstrations/> accessed 21 February 2025

60. 'Why Has Kenya's Finance Bill Triggered Protests?' (Context.news, 26 June 2024) <https://www.context.news/money-power-people/why-has-kenyas-finance-bill-triggered-public-outrage> accessed 17 February 2025

61. Bailey R and Parsheera S, 'Data Localisation in India: Questioning the Means and Ends' (Working Paper 18/242, National Institute of Public Finance and Policy 2018) <https://ideas.repec.org/p/npf/wpaper/18/242.html> accessed 22 February 2025

62. Council of Europe, 'The Role of Internet Intermediaries as Gatekeepers to Freedom of Expression – Conference in Vienna' (2017) <https://www.coe.int/en/web/freedom-expression/home/-/asset_publisher/RAupmF2S6voG/content/the-role-of-internet-intermediaries-as-gatekeepers-to-freedom-of-expression-conference-in-vienna> accessed 17 February 2025

63. Directorate of Criminal Investigations, 'Statement on Arrest of Edgar Obare under Section 23 of Computer Misuse and Cybercrimes Act 2018' (X, 4 March 2021) <https://twitter.com/dci_kenya/status/1367512899044925442> accessed 18 March 2025

64. World Report 2022: Uganda (Human Rights Watch) <https://www.hrw.org/world-report/2022/country-chapters/uganda> accessed 22 February 2025

International Commission of Jurists
KENYAN SECTION | Since 1959

The Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ICJ Kenya House, Off Silanga Road, Karen
P.O. Box 59743 - 00200, Nairobi, Kenya
www.icj-kenya.org

ICJ Kenya

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

This is the Exhibit Marked "EM-5"
Referred to in the Annexed Affidavit Declaration
of Eric Mukoya
Sworn / declared before me
this 13 day of May 20 24
at Nairobi

Commissioner For Oaths

COMMUNICATIONS AUTHORITY OF KENYA
P. O. Box 14448 - 00800, NAIROBI
20 NOV 2023
RECEIVED
BY: Evelyn TIME: 16:05

20th November 2023

To:

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon Eliud Owalo, Cabinet Secretary for Information, Communications and the Digital Economy

Christopher Wambua, Acting Director General, Communications Authority of Kenya (CA)

RE: Blocking of Telegram in Kenya

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 300 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of communications application, Telegram, in Kenya. The blocking seemingly coincides with the ongoing Kenya Certificate Secondary Education (KCSE) examinations.

Data captured by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram starting from at least November 8, 2023 on Jambonet (Telkom) where it is persistently blocked until at least November, 15. Safaricom also appears to be blocking Telegram during the examination hours since at least November 10 until November 17. At the time of publication of this open letter, today, 20 November, Telegram is again blocked on Jambonet (Telkom). We will continue to monitor the situation and update your offices accordingly.

Several reports on X (formerly Twitter) indicated that the platform could only be accessed through the use of Virtual Private Networks (VPNs), which enable people to bypass the blocking.

Social Media platforms like Telegram have become an integral part of Kenyan society, playing a significant role in communication, information dissemination, business, and social change. Its impact is felt across various aspects of life, from connecting with friends and family to influencing political discourse and driving economic opportunities.

Measures to intentionally prevent or disrupt access to or the dissemination of information online are in violation of international human rights law. Blocking access to essential platforms that facilitate the exercise of rights and freedoms including freedom of expression and access to information is a violation of Articles 33 and 35 of the Constitution of Kenya as well as international human rights standards that provide for these rights.
We therefore demand clarification as to why Telegram is inaccessible in Kenya. In accordance with Article 35 of the Constitution of Kenya and the Access to Information Act 2016, we wish to request the following within 7 days:

1. Information on why Telegram has been blocked in Kenya;
2. Information on when the blockade will be lifted;
3. Information on which law/policy/regulation was relied upon to block Telegram in Kenya; and
4. Information on which Government agency, if any, directed that Telegram be blocked in Kenya.

We hope that you can respond to this letter and forward us this information as soon as possible. You can send your response to info@bake.or.ke.

Signed:

Africa Freedom of Information Centre (AFIC)
African Freedom of Expression Exchange (AFEX)
Access Now
Advocacy Initiative for Development (AID)
AfricTivistes
Africa Media and Information Technology Initiative (AfriMITI)
Africa Open Data and Internet Research Foundation (AODIRF)
Amnesty International Kenya
Article 19 Eastern Africa
Baraza Media Lab
Bloggers Association of Kenya (BAKE)
Bloggers of Zambia (BloggersZM)
Common Cause Zambia
Computech Institute
Human Rights Journalists Network Nigeria
Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ifreedom Uganda Network
International Press Centre (IPC)
International Press Institute
JCA-NET(Japan)
Katiba Institute
Kenya ICT Action Network (KICTANet)
Kenya Union of Journalists (KUJ)
Kijiji Yeetu
Life campaign to abolish the death sentence in Kurdistan
Media Foundation for West Africa (MFWA)
Miaan Group
Open Observatory of Network Interference (OONI)
Office of civil freedoms

Open Privacy Tech Foundation (OPTF)
Organization of Justice Campaign
Paradigm Initiative
Single Mothers Association of Kenya (SMAK)
Ubunteam
Webfala Digital Skills for all Initiative
Women of Uganda Network (WOUGNET)
Women ICT Advocacy Group (WIAG)
Wikimedia Community User Group Uganda
Zaina Foundation

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

20th November 2023

To:

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon Eliud Owalo, Cabinet Secretary for Information, Communications and the Digital Economy

Christopher Wambua, Acting Director General, Communications Authority of Kenya (CA)

RE: Blocking of Telegram in Kenya

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 300 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of communications application, Telegram, in Kenya. The blocking seemingly coincides with the ongoing Kenya Certificate Secondary Education (KCSE) examinations.

Data captured by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram starting from at least November 8, 2023 on Jambonet (Telkom) where it is persistently blocked until at least November, 15. Safaricom also appears to be blocking Telegram during the examination hours since at least November 10 until November 17. At the time of publication of this open letter, today, 20 November, Telegram is again blocked on Jambonet (Telkom). We will continue to monitor the situation and update your offices accordingly.

Several reports on X (formerly Twitter) indicated that the platform could only be accessed through the use of Virtual Private Networks (VPNs), which enable people to bypass the blocking.

Social Media platforms like Telegram have become an integral part of Kenyan society, playing a significant role in communication, information dissemination, business, and social change. Its impact is felt across various aspects of life, from connecting with friends and family to influencing political discourse and driving economic opportunities.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

20th November 2023

To:

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon Eliud Owalo, Cabinet Secretary for Information, Communications and the Digital Economy

Christopher Wambua, Acting Director General, Communications Authority of Kenya (CA)

RE: Blocking of Telegram in Kenya

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 300 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of communications application, Telegram, in Kenya. The blocking seemingly coincides with the ongoing Kenya Certificate Secondary Education (KCSE) examinations.

Data captured by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram starting from at least November 8, 2023 on Jambonet (Telkom) where it is persistently blocked until at least November, 15. Safaricom also appears to be blocking Telegram during the examination hours since at least November 10 until November 17. At the time of publication of this open letter, today, 20 November, Telegram is again blocked on Jambonet (Telkom). We will continue to monitor the situation and update your offices accordingly.

Several reports on X (formerly Twitter) indicated that the platform could only be accessed through the use of Virtual Private Networks (VPNs), which enable people to bypass the blocking.

Social Media platforms like Telegram have become an integral part of Kenyan society, playing a significant role in communication, information dissemination, business, and social change. Its impact is felt across various aspects of life, from connecting with friends and family to influencing political discourse and driving economic opportunities.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

20th November 2023

To:

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon Eliud Owalo, Cabinet Secretary for Information, Communications and the Digital Economy

Christopher Wambua, Acting Director General, Communications Authority of Kenya (CA)

RE: Blocking of Telegram in Kenya

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 300 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of communications application, Telegram, in Kenya. The blocking seemingly coincides with the ongoing Kenya Certificate Secondary Education (KCSE) examinations.

Data captured by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram starting from at least November 8, 2023 on Jambonet (Telkom) where it is persistently blocked until at least November, 15. Safaricom also appears to be blocking Telegram during the examination hours since at least November 10 until November 17. At the time of publication of this open letter, today, 20 November, Telegram is again blocked on Jambonet (Telkom). We will continue to monitor the situation and update your offices accordingly.

Several reports on X (formerly Twitter) indicated that the platform could only be accessed through the use of Virtual Private Networks (VPNs), which enable people to bypass the blocking.

Social Media platforms like Telegram have become an integral part of Kenyan society, playing a significant role in communication, information dissemination, business, and social change. Its impact is felt across various aspects of life, from connecting with friends and family to influencing political discourse and driving economic opportunities.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

20th November 2023

To:

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon Eliud Owalo, Cabinet Secretary for Information, Communications and the Digital Economy

Christopher Wambua, Acting Director General, Communications Authority of Kenya (CA)

RE: Blocking of Telegram in Kenya

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 300 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of communications application, Telegram, in Kenya. The blocking seemingly coincides with the ongoing Kenya Certificate Secondary Education (KCSE) examinations.

Data captured by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram starting from at least November 8, 2023 on Jambonet (Telkom) where it is persistently blocked until at least November, 15. Safaricom also appears to be blocking Telegram during the examination hours since at least November 10 until November 17. At the time of publication of this open letter, today, 20 November, Telegram is again blocked on Jambonet (Telkom). We will continue to monitor the situation and update your offices accordingly.

Several reports on X (formerly Twitter) indicated that the platform could only be accessed through the use of Virtual Private Networks (VPNs), which enable people to bypass the blocking.

Social Media platforms like Telegram have become an integral part of Kenyan society, playing a significant role in communication, information dissemination, business, and social change. Its impact is felt across various aspects of life, from connecting with friends and family to influencing political discourse and driving economic opportunities.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

11 November 2024

To:

David Mugonyi, Director General, Communications Authority of Kenya (CA)

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon. Margaret Nyambura Ndung'u, Cabinet Secretary for Information, Communications and the Digital Economy

Hon. Florence Kajuju, Chairperson, the Commission on Administrative Justice (Office of the Ombudsman)

RE: The Blocking of Telegram by the Kenyan Government

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 334 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of the digital communications application, Telegram, in Kenya reportedly ordered by the Communications Authority (CA) throughout the Kenya Certificate Secondary Education (KCSE) examination period in the country.

Data collected by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram, starting from at least 7 November 2024, on Safaricom during the examination hours. This is the second time in as many years that access to Telegram is being blocked in Kenya during national examinations. In 2023, reports indicated this measure was toin an effort to curb exam cheating; evidence has shown time and again that internet shutdowns are an ineffective and disproportionate measure against exam cheating and authorities in Kenya must stop this trend.

In June this year, authorities again shut down access to the internet to quell the "Reject Finance Bill" protests in the country despite a public commitment from the Communications Authority that they would not interfere with internet connectivity. Given the timing of this year's disruption during national exams, similarities to last year, and the news reporting of a blocking order issued by the CA, we are forced to assume — absent transparency or disclosures from the government — that the CA has ordered Telegram blocked.

It is concerning to see Kenya, a member of the Freedom Online Coalition — a network of 41 governments championing internet freedom globally — which used to be an example of countries advancing digital innovation and rights, turn away from human rights and falling into a dangerous pattern of shutting down internet access and digital platforms during important national events. The government of Kenya has recently committed to the *United Nations Global Digital Compact*, which in paragraph 29(d) states commit to "....refrain from internet shutdowns and measures that target internet access (SDG 16)".

Social media platforms like Telegram have become an integral part of Kenyan society, playing a significant role in communication, information dissemination, business, and social change. Its impact is felt across various aspects of life, from connecting with friends and family to influencing political discourse and driving economic opportunities.

Measures to intentionally prevent or disrupt access to or the dissemination of information online violate international human rights law. Blocking access to essential platforms that facilitate the exercise of rights and freedoms including freedom of expression and access to information is a violation of Articles 33 and 35 of the *Constitution of Kenya*, 2010 as well as international human rights standards that provide for these rights.

We therefore demand clarification as to why Telegram is inaccessible on the Safaricom network in Kenya. In accordance with Article 35 of the *Constitution of Kenya, 2010,* and the *Access to Information Act 2016*, we wish to request the following within seven days:

1. Information on which law/policy/regulation was relied upon to block Telegram in Kenya;
2. Information on when the blockade will be lifted; and
3. Information on which Government agency, if any, directed that Telegram be blocked in Kenya.

We anticipate a swift response to this letter with the requested information.

Signed:

1. Access Now
2. Africa Open Data and Internet Research Foundation (AODIRF)
3. Africa Rural Internet and STEM Initiative (AFRISTEMI)
4. African Freedom of Expression Exchange (AFEX)
5. AfricTivistes
6. Article 19 Eastern Africa
7. Baraza Media Lab
8. Bloggers Association of Kenya (BAKE)
9. Bloggers of Zambia - BloggersZM
10. Brave Media
11. Center for Media Studies and Peacebuilding (CEMESP-LIberia)
12. Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
13. Committee to Protect Journalists (CPJ)
14. Digital Rights and Freedoms Regional Hub
15. Eurasian Digital Foundation
16. FORUMVERT
17. Global Digital Inclusion Partnership (GDIP)
18. Human Rights Journalists Network Nigeria
19. JCA-NET(Japan)
20. Kenya Union of Journalists (KUJ)
21. KICTANet
22. Life campaign to abolish the death sentence in Kurdistan
23. Media Foundation for West Africa (MFWA)
24. Miaan Group
25. Nubian Rights Forum
26. Office of Civil Freedoms
27. Open Observatory of Network Interference (OONI)
28. Opening Central Africa coalition
29. Organization of the Justice Campaign
30. Paradigm Initiative (PIN)
31. PAWA254
32. Reclaiming Spaces Initiative - Uganda
33. RKS Global
34. Sassoufit Collective
35. Siasa Place
36. Southeast Asia Freedom of Expression Network (SAFEnet)
37. The Kenyan Section of The International Commission of Jurists (ICJ KENYA)

38. Ubunteam
39. West African Digital Rights Defenders Coalition
40. Women of Uganda Network (WOUGNET)
41. Wikimedia Community Usergroup Uganda
42. YODET

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471 / 020-3922...
Email: info@bake.or.ke
Website: www.bake.co.ke

11 November 2024

To:

David Mugonyi, Director General, Communications Authority of Kenya (CA)

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon. Margaret Nyambura Ndung'u, Cabinet Secretary for Information, Communications and the Digital Economy

Hon. Florence Kajuju, Chairperson, the Commission on Administrative Justice (Office of the Ombudsman)

RE: The Blocking of Telegram by the Kenyan Government

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 334 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of the digital communications application, Telegram, in Kenya reportedly ordered by the Communications Authority (CA) throughout the Kenya Certificate Secondary Education (KCSE) examination period in the country.

Data collected by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram, starting from at least 7 November 2024, on Safaricom during the examination hours. This is the second time in as many years that access to Telegram is being blocked in Kenya during national examinations. In 2023, reports indicated this measure was toin an effort to curb exam cheating; evidence has shown time and again that internet shutdowns are an ineffective and disproportionate measure against exam cheating and authorities in Kenya must stop this trend.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

11 November 2024

To:

David Mugonyi, Director General, Communications Authority of Kenya (CA)

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon. Margaret Nyambura Ndung'u, Cabinet Secretary for Information, Communications and the Digital Economy

Hon. Florence Kajuju, Chairperson, the Commission on Administrative Justice (Office of the Ombudsman)

RE: The Blocking of Telegram by the Kenyan Government

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 334 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of the digital communications application, Telegram, in Kenya reportedly ordered by the Communications Authority (CA) throughout the Kenya Certificate Secondary Education (KCSE) examination period in the country.

Data collected by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram, starting from at least 7 November 2024, on Safaricom during the examination hours. This is the second time in as many years that access to Telegram is being blocked in Kenya during national examinations. In 2023, reports indicated this measure was toin an effort to curb exam cheating; evidence has shown time and again that internet shutdowns are an ineffective and disproportionate measure against exam cheating and authorities in Kenya must stop this trend.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

11 November 2024

To:

David Mugonyi, Director General, Communications Authority of Kenya (CA)

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon. Margaret Nyambura Ndung'u, Cabinet Secretary for Information, Communications and the Digital Economy

Hon. Florence Kajuju, Chairperson, the Commission on Administrative Justice (Office of the Ombudsman)

RE: The Blocking of Telegram by the Kenyan Government

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 334 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of the digital communications application, Telegram, in Kenya reportedly ordered by the Communications Authority (CA) throughout the Kenya Certificate Secondary Education (KCSE) examination period in the country.

Data collected by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram, starting from at least 7 November 2024, on Safaricom during the examination hours. This is the second time in as many years that access to Telegram is being blocked in Kenya during national examinations. In 2023, reports indicated this measure was toin an effort to curb exam cheating; evidence has shown time and again that internet shutdowns are an ineffective and disproportionate measure against exam cheating and authorities in Kenya must stop this trend.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/0733-528229
Email: info@bake.or.ke
Website: www.bake.co.ke

11 November 2024

To:

David Mugonyi, Director General, Communications Authority of Kenya (CA)

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon. Margaret Nyambura Ndung'u, Cabinet Secretary for Information, Communications and the Digital Economy

Hon. Florence Kajuju, Chairperson, the Commission on Administrative Justice (Office of the Ombudsman)

RE: The Blocking of Telegram by the Kenyan Government

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 334 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of the digital communications application, Telegram, in Kenya reportedly ordered by the Communications Authority (CA) throughout the Kenya Certificate Secondary Education (KCSE) examination period in the country.

Data collected by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram, starting from at least 7 November 2024, on Safaricom during the examination hours. This is the second time in as many years that access to Telegram is being blocked in Kenya during national examinations. In 2023, reports indicated this measure was toin an effort to curb exam cheating; evidence has shown time and again that internet shutdowns are an ineffective and disproportionate measure against exam cheating and authorities in Kenya must stop this trend.

Bloggers Association of Kenya

4th Floor, Bishop Magua Centre, George Padmore Lane
Tel: 0704-090471/ 0733-522229
Email: info@bake.or.ke
Website: www.bake.co.ke

11 November 2024

To:

David Mugonyi, Director General, Communications Authority of Kenya (CA)

Peter Ndegwa, Chief Executive Officer, Safaricom PLC,

Ashish Malhotra, Managing Director, Airtel Kenya,

Mugo Kibati, Chief Executive Officer, Telkom Kenya,

cc:

Hon. Margaret Nyambura Ndung'u, Cabinet Secretary for Information, Communications and the Digital Economy

Hon. Florence Kajuju, Chairperson, the Commission on Administrative Justice (Office of the Ombudsman)

RE: The Blocking of Telegram by the Kenyan Government

We, the undersigned organisations and members of the #KeepItOn coalition — a global network of over 334 organisations from 105 countries working to end internet shutdowns — write to seek clarification on the ongoing disruption of the digital communications application, Telegram, in Kenya reportedly ordered by the Communications Authority (CA) throughout the Kenya Certificate Secondary Education (KCSE) examination period in the country.

Data collected by the Open Observatory of Network Interference (OONI) platform shows an ongoing disruption affecting Telegram, starting from at least 7 November 2024, on Safaricom during the examination hours. This is the second time in as many years that access to Telegram is being blocked in Kenya during national examinations. In 2023, reports indicated this measure was toin an effort to curb exam cheating; evidence has shown time and again that internet shutdowns are an ineffective and disproportionate measure against exam cheating and authorities in Kenya must stop this trend.

REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
HCCHRPET/ 276 /2025

INTERNATIONAL COMMISSION OF JURISTS
KENYA SECTION (ICJ KENYA) .....1ST PETITIONER
BLOGGERS ASSOCIATION OF KENYA (BAKE).....2ND PETITIONER
KENYA UNION OF JOURNALISTS (KUJ).....3RD PETITIONER
COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA (CIPESA).....4TH PETITIONER

AND

COMMUNICATION AUTHORITY OF KENYA (CA).....1ST RESPONDENT
ATTORNEY GENERAL.....2ND RESPONDENT
CABINET SECRETARY INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY.....3RD RESPONDENT
SAFARICOM LTD.....4TH RESPONDENT
AIRTEL KENYA LTD.....5TH RESPONDENT
PARADIGM INITIATIVE (PIN).....1ST INTERESTED PARTY
LAW SOCIETY OF KENYA.....2ND INTERESTED PARTY
KATIBA INSTITUTE.....3RD INTERESTED PARTY

EXPERT WITNESS STATEMENT - ARTURO BUZZOLAN FILASTÒ

I Arturo Buzzolan Filastò, of Via Ostiense 131L, 00154, Rome, Italy, CF 96568220584 state that:

1. I am the Founder, Executive Director, and Chief Technology Officer (CTO) of the Open Observatory of Network Interference (OONI) Foundation, an international initiative that develops free and open source software to measure internet censorship and network interference globally. I co-founded and serve as the Vice-President of the Hermes Center for Digital Human Rights.
2. Internet shutdowns and related forms of network interference have a direct and measurable impact on fundamental rights and freedoms, including freedom of expression, access to information, freedom of assembly, and participation in democratic processes.
3. The findings presented in the accompanying report are based on the analysis of network measurements collected via the OONI Probe app, which is run by users in over 170 countries to detect internet censorship

from local networks. To investigate the reported blocking of Telegram in Kenya, we analyzed data from two key experiments: Telegram and Web Connectivity. For more details about the methodology, please refer to our in depth report.

4. OONI's analysis found clear evidence of Telegram being blocked in Kenya during both the 2023 and 2024 KCSE national exams. Between 8th and 24th November 2023, access to Telegram was intermittently blocked on Safaricom and Airtel networks, and persistently blocked on Jambonet. The blocks were implemented through a combination of techniques (DNS, TLS, and IP-level blocking) and affected both the Telegram website and app. Similar blocking patterns were observed during the 2024 KCSE exams, with Telegram access restricted across Safaricom, Jambonet, and Jamil Telecommunications networks. Notably, in some cases, blocks extended beyond exam hours and continued after official instructions to lift them. These findings demonstrate a repeated pattern of targeted interference with Telegram services during national exam periods.

Dated at Rome on 13 May 2025

Arturo Buzzolan Filastò - Witness

Drawn and filed by:
Bond Advocates LLP
Top Plaza, 2nd Floor,
Kindaruma Road
P. O. Box 37551-00100
Nairobi
0112318576
bond@bondadvocates.com
ochieljd@bondadvocates.com