Ranking digital rights in East and Southern Africa:

The polices and practices of telecommunication companies.

Internews
Local voices. Global change.

Ranking Digital Rights

The Greater Internet Freedom (GIF) project is a three-year, global program that works to preserve an open, interoperable, reliable, and secure Internet and by extension, protects the individuals, civil society organizations, media outlets and vulnerable groups who rely on it to realize fundamental freedoms. Through its dual objective of enhancing digital security for civil society and media and increasing citizen engagement in Internet governance, GIF considers and supports a diverse range of elements that impact Internet freedom.

RDR: Ranking Digital Rights (RDR) is an independent research program at the policy think tank New America. RDR believes that transparency is the first step to accountability. RDR evaluates the policies and practices of the world's most powerful tech and telecom companies and studies their effects on people's fundamental human rights.

Lead researcher:

Kuda Hove Independent Researcher

Research Editors:

Lisa Goldman

Wakesho Kililo Greater Internet Freedom Project

Research Advisor:

Leandro Ucciferri, Global Partnerships Manager, Ranking Digital Right

Published April 2023

This report has been produced as part of the Greater Internet Freedom project work in East and Southern Africa

Table of Contents

Introduction

The past decade has seen an increase in the number of people accessing and using the internet across Africa.[1] In a research paper published in 2020, GSMA shows that owning a smartphone in Africa is one important enabler for becoming a regular mobile internet user.[2] This is corroborated by statistics from countries such as Zimbabwe, which show that over 80% of internet users in the country rely on mobile data to access the internet.[3][4] Mobile network operators thus play a key role in providing internet access across Africa.

In 2021 the United Nations Human Rights Council (UNHRC) adopted a resolution on "the promotion, protection and enjoyment of human rights on the Internet,"[5] which confirms the internet's role in enabling the enjoyment of fundamental rights such as the right to privacy, the right to free expression along with other information rights. Given the importance of the internet for human development it is imperative to monitor and evaluate the policies of telecommunications companies, which own and run internet infrastructure, to ensure they implement policies that promote the enjoyment of fundamental rights, instead of restricting them.

This research report uses the Ranking Digital Rights (RDR) Corporate Accountability Index methodology to analyse the policies of eight telecommunications companies operating across four African countries — Tanzania, Uganda, Zambia, and Zimbabwe. Specifically, to evaluate and record how each company's disclosed policies and practices affect people's rights to freedom of expression and privacy. For each of these four countries, we selected the two biggest telecommunications companies in terms of sub-

1 GSMA Mobile Internet Connectivity 2020: Sub-Saharan Africa Factsheet. GSMA. 2020. https://www.gsma.com/r/wp-content/uploads/2020/09/Mobile-Internet-Connectivity-SSA-Fact-Sheet.pdf

2 Delaporte, A. "The state of mobile internet connectivity in Sub-Saharan Africa: why addressing the barriers to mobile internet use matters now more than ever." *Mobile for Development*. January 4, 2020. https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-internet-connectivity-in-sub-saharan-africa/

3 Mobile data refers to internet traffic sent over 3G, HSDPA, and LTE networks

4 Postal and Telecommunications Regulatory Authority of Zimbabwe Abridged Postal and Telecommunications Sector Performance Report Third Quarter 2021. POTRAZ https://www.techzim.co.zw/wp-content/uploads/2021/12/Abridged-Sector-Performance-Report-Q3-2021-HMed.pdf

5 UNHRC, Draft resolution: The promotion, protection, and enjoyment of human rights on the Internet, 47th Sess, 2021, (A/HRC/47/L.22) http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/47/L.22&Lang=E

scribers. These companies are, Airtel and Vodacom in Tanzania; Airtel and MTN in Uganda; Airtel and MTN in Zambia; and Econet and Net One in Zimbabwe. In addition to evaluating the prepaid mobile services, this study also analyses the mobile money, or "digital wallets," services that each company provides.

Key findings

Our major findings are as follows:

- None of the eight companies commit definitively in their policies to the protection of information rights and the right to free expression. Only six of the eight companies publish their policy privacies.
- None of the companies shares mechanisms to evaluate how their policies affect the right to privacy and right to free expression.
- While all eight companies publish terms of use, they are not always comprehensive. In some cases, whether they applied to the corporate website or to company's services was unclear.
- Only one company published policies in a local language. The exclusive use of English means those who don't speak the language are prevented from understanding their rights per the company's policies.
- None of the companies shares sufficiently detailed privacy policies. Six of them share superficial privacy policies that lack, for example, information on data breach notifications, data retention periods or the contact information for the relevant data protection officer.
- None of the companies discloses a comprehensive advertising policy.
- None of the companies discloses how many information requests they receive from government agencies or law enforcement agencies within a specified period of time.

Recommendations on how to improve some of the shortfalls identified are at the end of each section. Relevant case studies are also included throughout the research as a way of highlighting the damage caused due to the absence of adequate policies to protect human rights.

Research Methodology

This is desk research guided by the 2020 Ranking Digital Rights Index methodology. Ranking Digital Rights (RDR) is an independent research programme under the auspices of New America, a think tank located in Washington, D.C. They evaluate the policies and practices of the world's most powerful tech and telecom companies and study their effects on fundamental human rights, publishing the only open data set on companies' commitments and policies affecting users' freedom of expression and privacy. Since 2015, RDR has published the annual Corporate Accountability Index, which ranks 26 companies around the world, using their own methodology to evaluate 58 indicators in three main categories: governance, freedom of expression and information, and privacy. In 2022, RDR split the release[6] of the Corporate Accountability Index into two publications: the Big Tech Scorecard[7], focused on the 14 most powerful digital platforms worldwide, and the Telco Giants Scorecard, focused on 12 global telecommunications operators.

For this project, RDR provided the author with technical assistance and guidance for the adaptation process of the research methodology, including the necessary materials to conduct the data collection and analysis. The author selected a subset of indicators from the 2020 RDR Index methodology[8] that best reflected the needs and issues to be addressed in the countries covered by the research. To that end, 40 indicators — from the three categories — were used to evaluate the level of transparency and disclosures of eight telecommunications companies, comprising 16 services in total.[9]

The **governance category** contains indicators that seek evidence to show the company follows robust governance processes to ensure it respects freedom of expression, information, and privacy.[10] In order to perform well in this category, a company's disclosure

6 Dheere, J. "The new shape of the RDR Corporate Accountability Index." Ranking Digital Rights, March 15, 2022. https://rankingdigitalrights.org/2022/02/23/new-corporate-accountability-index-big-tech-scorecard/

7 The 2022 Ranking Digital Rights Big Tech Scorecard. Ranking Digital Rights. https://rankingdigitalrights.org/index2022/

8 2020 Indicators. Ranking Digital Rights. https://rankingdigitalrights.org/2020-indicators/ June 15, 2022.

9 A list of the 40 indicators used in this report is available under Annex 1

10 2020 Ranking Digital Rights Corporate Accountability Index. Ranking Digital Rights. https://rankingdigitalrights.org/index2020/methodology

should at least follow, and ideally surpass, the UN Guiding Principles on Business and Human Rights and other industry-specific human rights standards focused on freedom of expression and privacy, such as those adopted by the Global Network Initiative.[11]

The **freedom of expression and information category** has indicators that analyse whether the company respects the right to freedom of expression and information, as articulated in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international human rights instruments.[12][13] Companies that perform well in this indicator demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also in how they determine, communicate, and enforce private rules and commercial practices that affect users' fundamental right to freedom of expression and information.[14]

Lastly, the indicators in the **privacy category** evaluate whether companies demonstrate concrete ways in which they respect the right to privacy of users, as articulated in the UDHR, the ICCPR, and other international human rights instruments. Companies that perform well on these indicators demonstrate a strong public commitment to transparency not only in terms of how they respond to government and private party demands for user data, but also how they determine, communicate, and enforce private rules and commercial practices that affect user privacy.[15]

The evaluation of the indicators was based exclusively on publicly available information that the companies disclosed on their respective websites. Each indicator has a list of elements, and companies receive credit (full, partial, or no credit) for each element they fulfil. The evaluation includes an assessment of disclosure for every element of each indicator, based on one of the following possible answers:

11 The GNI Principles. Global Network Initiative. https://globalnetworkinitiative.org/gni-principles/

12 OHCHR. Universal Declaration of Human Rights. https://www.ohchr.org/en/udhr/pages/introduction.aspx

13 OHCHR. International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

14 2020 Ranking Digital Rights Corporate Accountability Index. Ranking Digital Rights. https://rankingdigitalrights.org/index2020/methodology

15 Ibid

"Yes"/ full disclosure: Company disclosure meets the element requirement.

"Partial": Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of the element.

"No disclosure found": Researchers were unable to find information provided by the company on its website that answers the element question.

"No": Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of "no disclosure found," although both result in no credit.

"N/A": Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company's score.

Once the evaluation of the elements is complete, the final scores are calculated based on the following points:

Yes/full disclosure = 100

Partial = 50

No = 0

No disclosure found = 0

N/A = excluded from score and averages

These points are then used to create the data visualisations and rank the performance of the companies.

A comprehensive discussion on the history of the RDR Index methodology, along with the three categories and the different specific indicators contained therein is available on the RDR website.[16]

The findings for each indicator are discussed chronologically in this report, with the relevant recommendations that companies can follow to improve their ranking listed immediately below the discussion of each indicator.

16 Ibid

Knowing the Companies

This report covers four African countries: Tanzania, Uganda, Zambia, and Zimbabwe. In each country, we have selected the two biggest telecommunications companies based on their subscriber base. The evaluation focuses primarily on the respective company policies, which are available on each company's website. We consider other disclosed policies, where available, that are not on the website. The relevant product or service policies are the ones related to the use of each company's prepaid service and their respective mobile money service.

Vodacom Tanzania is the country's largest mobile network operator with a reported 14.8 million subscribers as of January 2020. In the same period, **Airtel Tanzania** had an estimated subscriber base of 11.6 million subscribers.[17] The mobile money services offered by Vodacom and Airtel in Tanzania are M-Pesa and Airtel, respectively.

In Uganda, **MTN Uganda** reported 15 million subscribers in August 2021, making it the country's most popular mobile network provider.[18] MTN Uganda's mobile money service is Momo Pay. **Airtel Uganda** is the country's second largest mobile network operator with an estimated 11.7 million subscribers in late 2020.[19] Its mobile money service is Airtel.

Airtel Zambia is the country's largest mobile network operator in terms of subscriber base, reporting a total of 19 million subscribers at the end of 2020.[20] Airtel Zambia operates the Airtel Money mobile payment service. The country's second largest mobile

17 O'Grady, V. "Airtel Tanzania grows subscriber numbers and expands 4G coverage." *Developing Telecoms*, September 2, 2019. https://developingtelecoms.com/telecom-technology/wireless-networks/9165-airtel-tanzania-grows-subscriber-numbers-and-expands-4g-coverage.html .

18 "MTN Uganda Hands over UGX 15 million to its 15 millionth subscriber as the Telecom Celebrates its 15 million Customer Base." MTN Uganda, August 3, 2021 https://www.mtn.co.ug/mtn-uganda-hands-over-ugx-15-million-to-its-15-millionth-subscriber-as-the-telecom-celebrates-its-15-million-customer-base/

19 Statista. "Share of mobile subscriptions Uganda 2015-2022, by operator." October 20, 2022. https://www.statista.com/statistics/671666/mobile-subscription-share-in-uganda-by-operator/

20 African Financials Digital Team. "Airtel Networks Zambia customer base stands at 6.771 million, up 16.02% Y-o-Y." *African Financials*. March 12, 2020. https://africanfinancials.com/airtel-networks-zambia-customer-base-stands-at-6-771-million-up-16-02-y-o-y/ .

network is **MTN Zambia**, which had reported eight million subscribers by mid-2019.[21] MTN's mobile money service is Momo Pay.

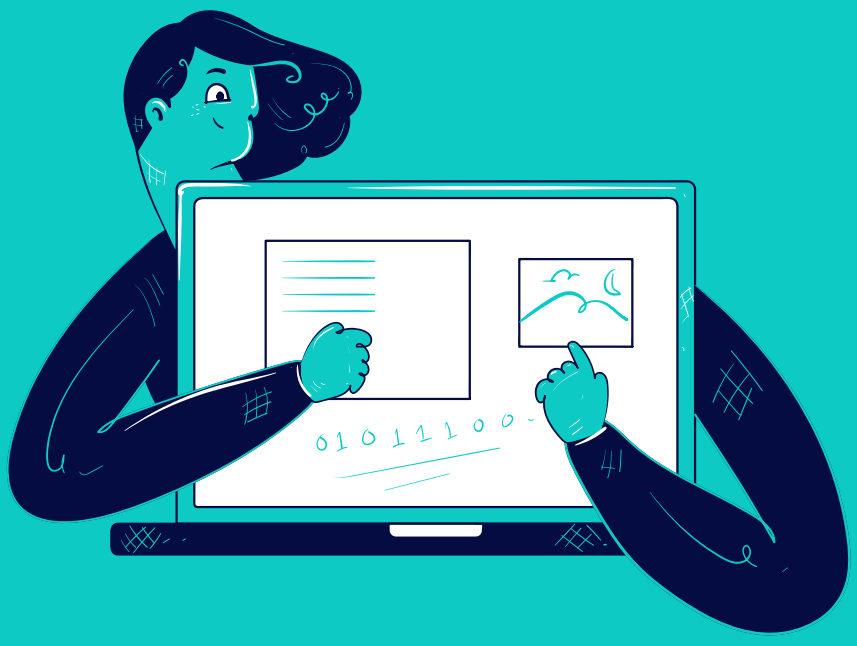
Figures from late 2020 indicate that Zimbabwe's largest mobile network operator is **Econet** with a subscriber base of nine million.[22] Econet's mobile money service is called Ecocash. The country's second largest network is **NetOne** with an estimated 4.2 million subscribers, and its mobile money service is called One Money.

Total Scores

21 "MTN Has Over 50% Market Share in 10 African Countries." *Connecting Africa*, September 2, 2019. https://www.connectingafrica.com/author.asp?doc_id=753808

22 Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) Abridged Postal and Telecommunications Sector Performance Report Third Quarter 2021 https://www.techzim.co.zw/wp-content/uploads/2021/12/Abridged-Sector-Performance-Report-Q3-2021-HMed.pdf

Delving deep into the research findings



Governance

There was no evidence that any of the local telecommunications companies involved in this research has published any policies indicating a commitment to freedom of expression and information. However, three of the companies have policies that clearly indicate their commitment to respecting the right to privacy.[23] This is evidenced by the disclosure of privacy policies for five of the eight services reviewed.[24] Econet Zimbabwe does not have a privacy policy for its prepaid mobile network plan[25]. NetOne Zimbabwe does not have any privacy policies for either of its services[26].

At the group level – meaning the parent companies of the local subsidiaries evaluated in this research – Bharti Airtel, MTN, and Vodafone groups have made commitments to respect human rights, which may include freedom of expression, information rights and the right to privacy. There was no information on the subsidiaries' websites that reflected the same commitments from the parent or global companies.

None of the companies seems to assess how national laws in their respective jurisdictions affect freedom of expression and privacy. Similarly, there is nothing indicating that any of the companies assesses whether their existing products and services carry

23 Airtel Uganda and Airtel Tanzania, MTN Uganda and MTN Zambia and Vodacom Tanzania.

24 Airtel Mobile and Airtel money in Airtel Tanzania and Uganda, MTN Mobile and Momo money in Uganda and Zambia and Vodacom Tanzania.

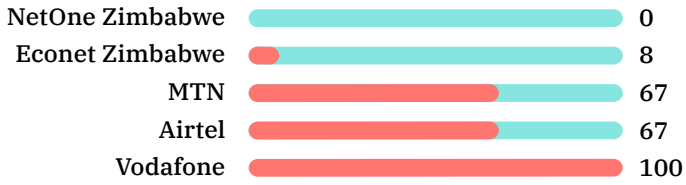
25 The privacy policy on Econet website says it only applies to their online activities and is valid for visitors to their website with regards to the information they shared and/ or collect in Econet wireless Zimbabwe, and the policy is not applicable to any information collected offline or via channels other than the Econet website.

26 The privacy policy on Net One's website is just for the website and applications related or connected to the website.

any freedom of expression and information risks or privacy associated risks. Additionally, no public disclosures were found that show any of the companies evaluates these risks in relation to its planned and new services and products. The companies also do not disclose any information showing that they conduct periodic assessments on a regular basis.

Governance scores

Policy Commitment

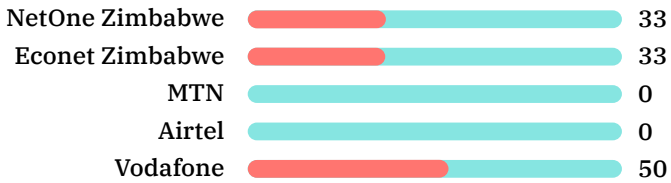


Impact assessment: Governments and regulations

Impact assessment: Processes for policy enforcement

Impact assessment: Targeted advertising

Stakeholder engagement and accountability



We found that none of the companies conducts regular evaluations to examine how their respective policy enforcement affects users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination.

Case study: Mandatory SIM card registration requirements

All four countries have mandatory SIM card registration laws.[27] As a result, mobile network users must provide some form of biometric national identity document when registering for a prepaid mobile service plan or mobile money service account. Acceptable forms of ID are usually a driving licence (if it shows the person's national unique identity number), a national identity card, or a valid passport.

At a global level, several privacy and freedom of expression advocates have published literature on the ways mandatory SIM card registration laws restrict the enjoyment of the right to privacy and create a chilling effect on free speech.[28] This is because mandatory SIM card registration laws allow states "...to know the identity of the owner of a SIM card, and thus who is most likely making a call or sending a message."[29] However, none of the telecommunications companies that are part of this research has publicly pushed back against the mandatory SIM card registration or suggested other, less intrusive, methods to confirm service users' identities.

If telecommunications companies assessed the effect of national laws on the right to privacy and freedom of expression, they would find that mandatory SIM card registration laws unjustifiably restricts the exercise of the right to privacy and the enjoyment of freedom of speech. By continuing to enforce SIM card registration requirements, telecommunications companies potentially expand each respective country's government's surveillance apparatus. The same is also true for other licensing requirements,

27 Tanzania: The Electronic and Postal Communications (SIM Card Registration) Regulations (the SCR Regulations), 2020.
Uganda: Regulatory directive issued by the Uganda Communications Commission in terms of Uganda's Communications Act, 2014
Zambia: Statutory Instrument on the Registration of Electronic Communication Apparatus No. 65 of 2011
Zimbabwe: Postal & Telecommunications (Subscriber Registration) Regulations, 2014 (SI 95 of 2014)

28 "101: SIM Card Registration." https://privacyinternational.org/explainer/2654/101-sim-card-registration

29 Ibid

which for example, require that telecommunications service providers install hardware and/or software that permits the real time interception of communications sent over their network infrastructure.[30]

We did not find any disclosures about assessments of the impact of targeted advertising on the right to freedom of expression, the right to privacy and other information rights. The lack of such assessments is a cause for concern. Telecommunications companies, by nature of their business, collect vast amounts of personal data, usage data, location data and other demographic data, which is valuable to advertisers seeking ways to optimize their targeted ad services.[31] Users deserve to know how their information is processed by the telecommunications companies and under what circumstances that information is shared with third parties such as advertisers. More importantly, in instances where telecommunications companies process user information for targeted advertising purposes, that should be done in a transparent and responsible manner.

None of the eight companies shares policies about engaging with stakeholders to discuss the company's impact on human rights online. However, some companies, such as Econet and NetOne, sometimes participate in civil society and government-led initiatives to discuss internet policy and digital rights-related issues.

None of the eight companies discloses grievance mechanisms specific to unjust acts related to the right to freedom of expression. The eight companies all have contact information on their websites, along with social media pages dedicated to interacting with and receiving general feedback from their users. In addition to these channels of communication, Airtel Uganda and Vodacom Tanzania provide the contact information for its data protection officer who can receive complaints related to data protection and privacy issues.[32] Airtel Tanzania states that complaints that are not resolved within 60 days from the time they were submitted will be referred to the Tanzania Communications Regulatory Authority.[33]

30 For example, as required by Zimbabwe's Interception of Communications Act, read together with the country's Postal and Telecommunications Act

31 *How are U.S. telcos playing the targeted advertising game?* https://rankingdigitalrights.org/2020/10/29/how-us-telcos-play-targeted-advertising-game/

32 Vodacom Privacy Policy https://vodacom.co.tz/privacy

33 https://www.airtel.co.tz/contact-us

Recommendations

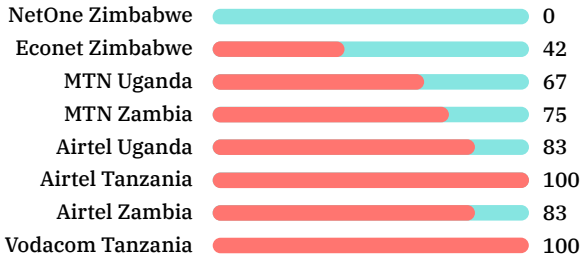
We recommend that companies:

- Make commitments to respect the freedom of expression and information rights.
- Establish robust human rights impact assessments to identify how government regulations and policies affect freedom of expression and right to information and privacy, and to mitigate any risks posed by those impacts in the jurisdictions in which they operate.
- Put in place measures to regularly assess how their existing and planned products and services affect fundamental rights.
- Assess how their policies affect freedom of expression, information rights and the right to privacy.

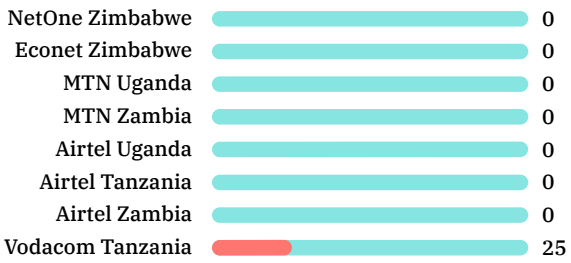
Freedom of Expression and Information

Freedom of Expression and Information indicator scores

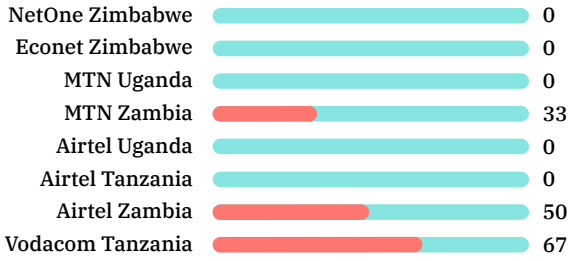
Access to terms of service



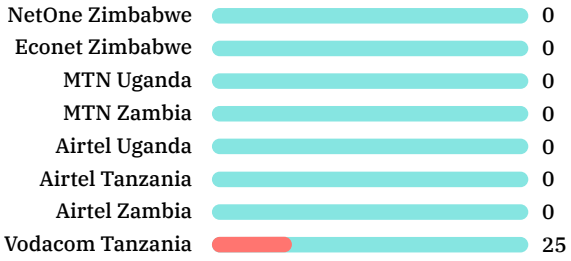
Changes to advertising content policies



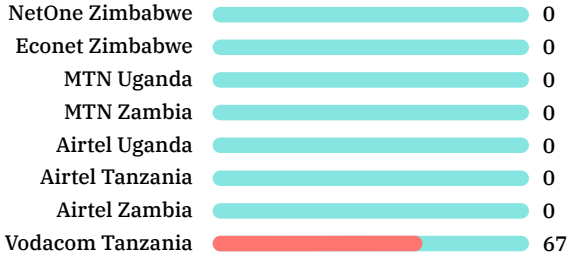
Access to advertising content policies



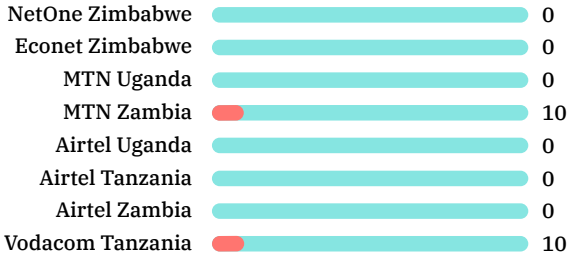
Changes to advertising targeting policies

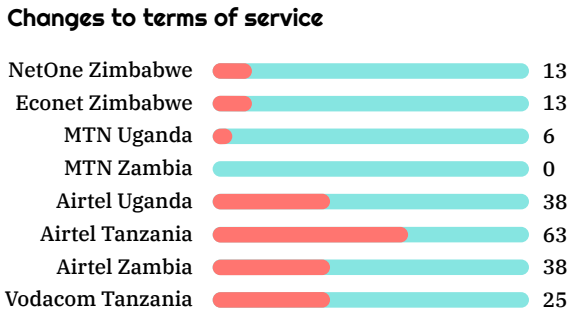


Access to advertising targeting policies



Changes to algorithmic system use policies





Access to terms of service

Econet does not share any terms of use for its prepaid mobile service. All the other companies publish terms of use, most of which can be viewed on the homepages of their websites. Vodacom Tanzania and Airtel Tanzania publish a Swahili version, but the other companies make their terms of service available in English only.

Vodacom Tanzania, the two MTN companies and the three Airtel companies all publish terms of service that communicate clearly how they apply to pre-paid services. But Econet's terms of reference are not clear on whether they apply to the company's website or their prepaid service. NetOne does not have any terms of service on their website and is the only company that does not share any terms of use for its mobile money service. Vodacom Tanzania and Airtel Tanzania are the only companies that publish terms of use for their mobile money services in English and Swahili; the other companies publish them in English only.

Access to advertising content policies

Some of the companies that publish user conditions and privacy policies mention advertisements but do not offer any comprehensive information about their advertising policy. None of the companies have a standalone advertising policy. Instead, each company's terms of us and some of the privacy policies, where available, contain a few lines on advertising.[34] None of the sections on advertising include clear disclosures on how changes to advertising would be communicated to users and advertisers (indicator F2(b)) or the enforcement of advertising policies (indicator F3(b)).

34 Vodacom Tanzania and MTN Uganda, for example

None of the companies publish advertising targeting policies, which relate to indicator F1(c). This means that there are also no disclosures under indicators F2(c) and F3(c).

Case study: Targeted advertising in Zimbabwe

Just before Zimbabwe's last general election, on July 31, 2018, registered voters who use the Econet network received targeted SMS from the ruling party, ZANU-PF. Each SMS included the recipient's name and constituency and asked them to vote for the ZANU-PF parliamentary candidate in that constituency as well as the presidential candidate. The Econet subscribers who received this targeted SMS were individuals who had previously registered to vote during the biometric voter registration, which had run over the months leading up to the elections.

Neither of Zimbabwe's two other mobile networks sent out such messages. One recipient of these targeted messages filed an application in the High Court of Zimbabwe in July 2018, arguing, among other things, that the electoral commission's sharing of his contact details with the ruling party was an infringement of his right to privacy. The court, however, has reserved judgement indefinitely; as of September 2022 it had not yet handed down a decision.[35] If Econet had had a targeted advertising policy in place, it would have been useful in determining the legality of the company's actions. A deviation from such an advertising policy would have provided grounds for affected users to initiate complaints against the company and seek relief for their grievances.

Access to algorithmic system use policies

None of the companies has disclosed any policies relating to the development or use of their algorithmic system. This means there are also no disclosures under indicator F2(d).

35 "Zanu-PF, Econet dragged to court over SMS." *Bulawayo24 News*. https://bulawayo24.com/index-id-news-sc-national-byo-140387.html

Recommendations

We recommend that:

- The terms of service be accessible in local languages as well as English; more importantly, that the terms of service be specific to the products and services the company offers.
- Companies should publish transparent, comprehensible advertising policies, that explain how user information is used in advertising, and when it is shared with advertising brokers.
- Users should have the choice to opt in on targeted advertising, instead of it being a default setting on the companies' services. Moreover, companies should inform users of the categories of targeted advertising they allow on their services.

Changes to terms of service

Each of the five telecommunications companies takes a default approach to changes in their terms of use, electing to post them on the company website.[36] Airtel Uganda and MTN Uganda state that in addition to updating the policy on the website, they may also notify users of changes by means of newspaper adverts or SMS. Apart from Airtel Tanzania, none of the companies provides a timeframe within which notice of changes would be given.

But none of the companies commit to maintaining and disclosing any change logs, making it the user's responsibility to read the updated terms of use and identify the changes made therein. This is an unreasonable expectation: the average person does not read

36 Airtel Uganda, Airtel Zambia, MTN Uganda, MTN Zambia, and Vodacom Tanzania share changes to their terms of service policies via their respective websites. Econet does not disclose any terms of use for its prepaid mobile service. NetOne does not disclose any terms of use for its prepaid mobile service or mobile money service.

the terms of use so closely as to notice slight changes or tweaks. Most of the terms of use state that if a subscriber continues to use the service after the company posts changes to their policies, including increases to fees, the company deems the subscriber to have accepted the updated terms.

This is problematic because it denies the user any opportunity to exercise informed consent. More critically, this approach gives the telecommunications service provider room to sneak in unfavourable terms of use without the user's knowledge and consent. The user is thus denied the right to make an informed decision about how they engage with the service provider. We recommend that companies share change logs of their terms of use or at least make previous versions of their terms of use publicly available.

Case study: Vodacom's results inflated by fraudulent subscriptions

One example of some of the potential abuses service users experience when there is no transparency over subscriptions and changes to terms of use comes from Vodacom South Africa.

An industry investigation revealed airtime theft on a mass scale from Vodacom's pre-paid customers, with fraudsters using a gateway developed by the mobile operator to bill service users without their knowledge.[37] Fraudulent wireless application service providers (WASP) used a gateway developed by Vodacom to subscribe users to several services without their permission.[38]

Vodacom reportedly did not act to stop this fraudulent billing; instead, it downplayed the harm caused to users.[39] It later emerged that Vodacom might have been slow to act because the "fraudulent subscriptions involved many of Vodacom's own content and entertainment services, which bolstered the revenue and subscriptions of its content services."[40] PlayInc, Vodacom's mobile gaming service, features prominently on the list

37 Muller, R. "Vodacom prepaid customers hit by airtime theft." *MyBroadband*. July 27, 2020. https://mybroadband.co.za/news/cellular/361389-vodacom-prepaid-customers-hit-by-airtime-theft.html

38 My Broadband. "Vodacom's results inflated by fraudulent subscriptions." August 23, 2022. https://mybroadband.co.za/news/cellular/457587-vodacoms-results-inflated-by-fraudulent-subscriptions.html

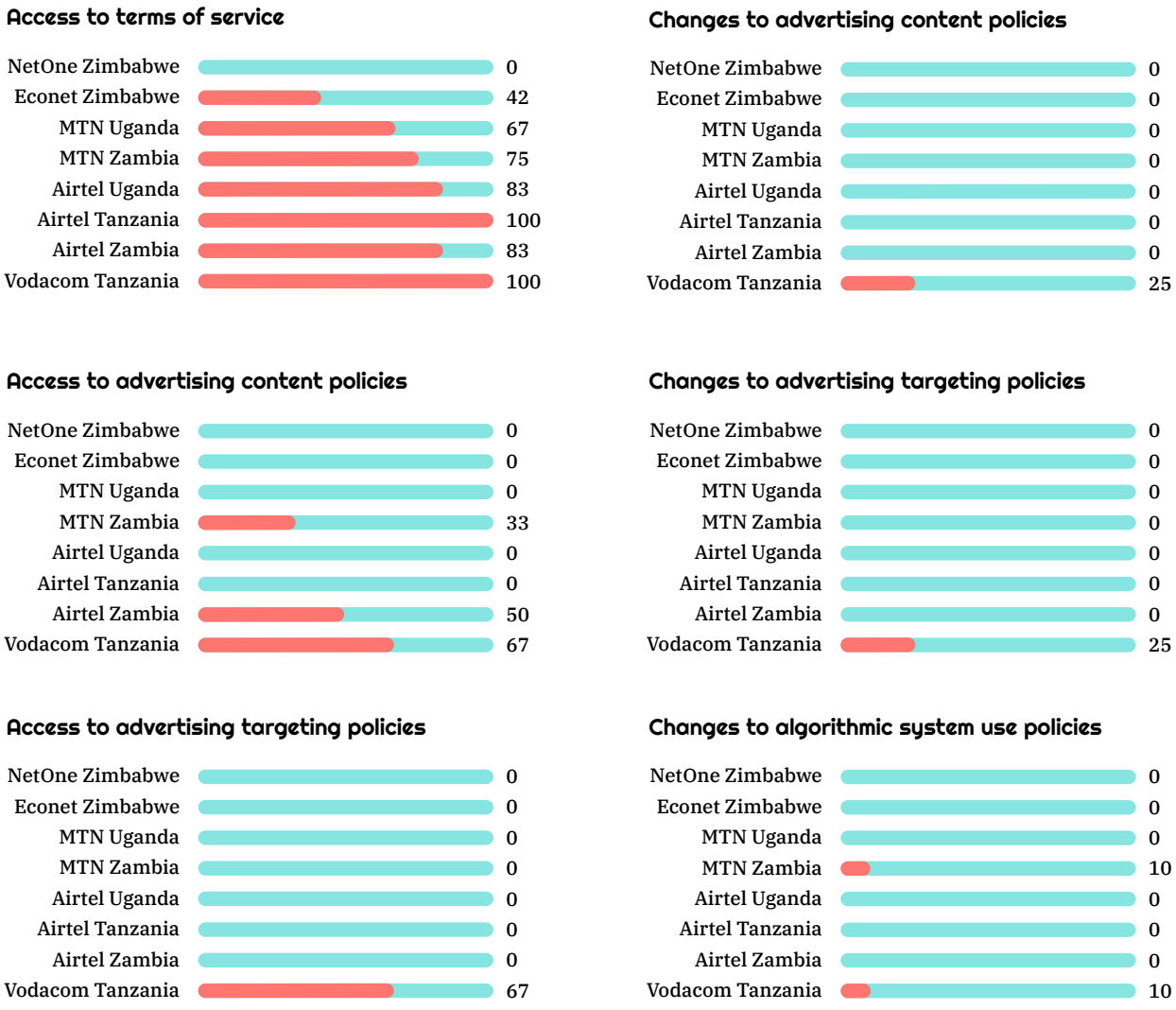
39 Ibid.

40 Ibid.

of services to which users were fraudulently subscribed. PlayInc reportedly signed up 800,000 users shortly after its launch.[41]

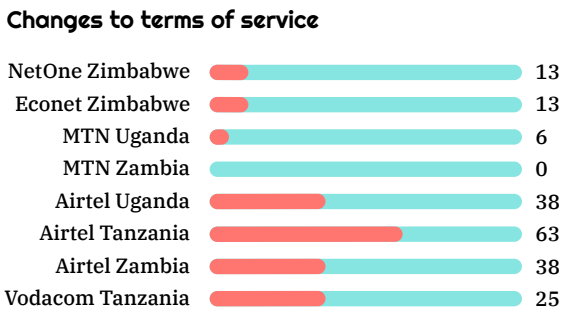
Vodacom eventually introduced controls to secure its direct-charge-to-bill (DCB) system in a way that prevents airtime theft and fraudulent subscriptions. Additionally, Vodacom raised awareness about the existence of a USSD-based self-service control system that enables users to block their SIMs for all WASP and other content services.[42]

Freedom of Expression and Information indicator scores



41 Ibid.

42 Muller, R. "Vodacom prepaid customers hit by airtime theft." *MyBroadband*. July 27, 2020. https://mybroadband.co.za/news/cellular/361389-vodacom-prepaid-customers-hit-by-airtime-theft.html



Data about content restrictions to enforce terms of service and data about advertising content

None of the companies publishes any transparency reports that would be useful in disclosing content moderation-related information. Indicators F4(a) and F4(b) seek to understand if any of the telecommunications companies covered in this study have used content moderation as a tool to enforce the companies' terms of service or advertising policies, but there are no publicly available disclosures on this. In the same vein, transparency reports would also contain the information required for indicator F4(c). Transparency reports will be discussed in further detail below under the discussion of indicators P10(a) and P11(a).

Network management (telecommunications companies)

None of the companies has revealed policies which disclose that they do not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network. But while we found no policies, the two Zimbabwean companies, Econet and NetOne, have entered into agreements with some local banks to zero rate those banks' mobile banking apps. Econet has entered into agreements with five Zimbabwean banks — the National Merchant Bank (NMB), the Commercial Bank of Zimbabwe (CBZ), Stanbic Bank, Nedbank, and First Capital Bank.[43] The National Merchant Bank announced that it is in negotiations with

43 Muhamba, V. "CBZ Bank joins the zero-rate revolution." *Techzim*. May 17, 2021. https://www.techzim.co.zw/2021/05/cbz-bank-joins-the-zero-rate-revolution/

NetOne to zero rate its mobile banking app and website on that network as well.[44] There is no publicly available information on the number of customers each bank has but they are among Zimbabwe's leading banks in terms of customer deposits.
Freedom of information advocates have pushed back against the use of zero rating or the prioritisation of certain types of network traffic for one app or service over other similar apps or services because it creates an unfair advantage and affects information rights. In Zimbabwe, organisations such as MISA Zimbabwe have highlighted some of the issues caused by the introduction of zero-rated services.[45] In general, however, consumers are not aware of the arguments for and against net neutrality.

Network shutdown (telecommunications companies)

None of the telecommunications companies covered in this report has disclosed the circumstances under which they might shut down or restrict access to the network or to specific protocols, services, or applications on the network. However, the governments of Tanzania, Uganda, Zambia, and Zimbabwe have all ordered telecommunications service providers operating within their respective borders to restrict access to the internet either partially or completely.

Zimbabwe's government ordered a total internet shutdown in January 2019 in response to nationwide riots against the increase in food and fuel prices in the country.[46] The internet shutdown lasted five days, during which Econet sent out SMS notifications to its users, informing them that the government had ordered the company to restrict internet access. In that SMS, Econet argued that it had no choice but to obey the government's instructions. In October 2020, the Tanzanian telecommunications regulator ordered the disruption of internet access a day before the country held its presidential elections.[47] The rolling internet disruptions stretched for over a week; Vodacom Tanza-

44 Muhamba, V. "The dominos are falling fast; NMBConnect is now zero-rated." *Techzim*. June 15, 2021. https://www.techzim.co.zw/2021/06/the-dominos-are-falling-fast-nmbconnect-is-now-zero-rated/

45 "Govt should prioritise internet affordability as a human right." *MISA Zimbabwe*. May 11, 2020. https://zimbabwe.misa.org/2020/05/11/govt-should-prioritise-internet-affordability-as-a-human-right/

46 Al Jazeera. "Zimbabwe imposes internet shutdown amid crackdown on protests." *News | Al Jazeera*. January 18, 2019. https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests

47 Sakpa, D. "Tanzania restricts social media during election." *DW*. October 29, 2020. https://www.dw.com/en/tanzania-restricts-social-media-during-election/a-55433057

nia and Airtel Tanzania complied with the order.[48]

On January 13, 2021, a day before Uganda's general election, the Uganda Communications Commission ordered the shutdown of the internet.[49] MTN Uganda and Airtel Uganda complied with the order. On August 12, 2021, during Zambia's election, the government ordered a partial internet shutdown, which targeted access to WhatsApp and social media services.[50] MTN Zambia and Airtel Zambia complied.

In all these four incidents, the internet shutdowns were in response to politically related events such as protests against government or elections. The telecommunications service providers covered in this report were instrumental in carrying out government orders. In each of these events, the governments acted with impunity and left it to the telecommunications companies to deal with members of the public who questioned the implementation of internet shutdowns. A publicly disclosed commitment, which sets out the circumstances under which these companies would restrict access to the internet, may be a good starting point in pushing against unjustified government instructions to arbitrarily restrict access to the internet.

Identity policy

Mobile network operators in all four countries require national identification to register a prepaid and mobile money service on their network.

48 Ssessanga, I. "Tanzania: Internet slowdown comes at a high cost." *DW*. November 5, 2020. https://www.dw.com/en/tanzania-internet-slowdown-comes-at-a-high-cost/a-55512732

49 "Uganda 2021 general elections: The internet shutdown and its ripple effects" *Association for Progressive Communications*. https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects

50 Anthonio, F. "Shutdown in Zambia on election day: How it affected people's lives and wellbeing." *Access Now*. September 21, 2021. https://www.accessnow.org/shutdown-in-zambia-on-election-day-how-it-affected-peoples-lives-and-wellbeing/

Recommendations

We recommend that companies:

- Maintain change logs that clearly document changes made to terms of service and other key policy documents.
- Publish policies on the circumstances under which they will disrupt access to the internet and other online platforms, such as social media and instant messaging apps and services.

Privacy

Access to privacy policies

All eight companies covered in this paper disclose some type of privacy policy. NetOne's privacy policy is the least useful as it consists of just two paragraphs and refers to the cookies used on the NetOne website, with no reference to the other services offered by the company.[51] Most of the privacy policies are accessible from the companies' respective website homepages. Only Vodacom Tanzania and Airtel Tanzania publish a Swahili version of the privacy policy; the other companies make them available only in English.

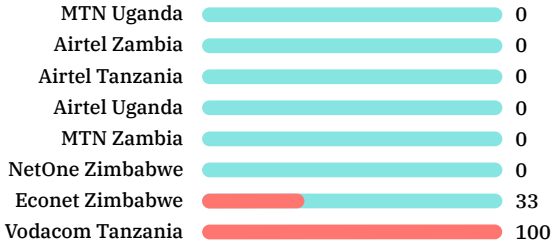
Vodacom Tanzania and Econet have separate privacy policies for their mobile money services. On the other hand, MTN Uganda, MTN Zambia, Airtel Tanzania, Airtel Uganda and Airtel Zambia disclose privacy policies that apply to their respective pre-paid services and mobile money services. NetOne and Econet do not have any disclosed privacy policies for their prepaid mobile service.

None of the companies has disclosed algorithmic system development policies. This means that we found no disclosures for indicators P1(b) and P2(b).

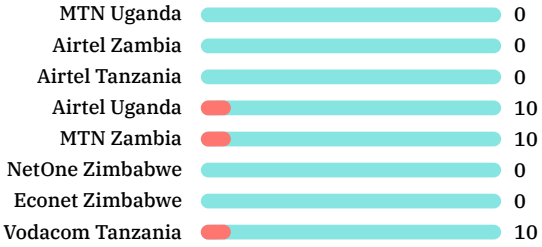
51 NetOne privacy policy available at https://www.netone.co.zw/#/privacy-policy

Privacy Indicator scores

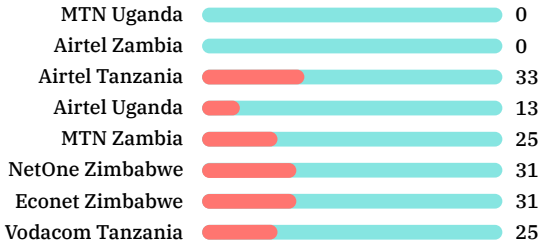
Access to privacy policies



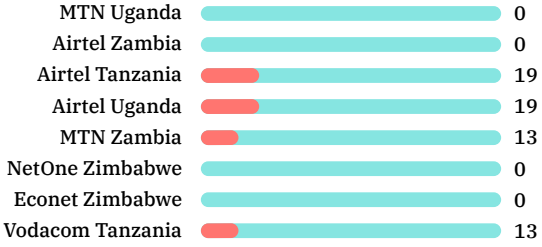
Retention of user information



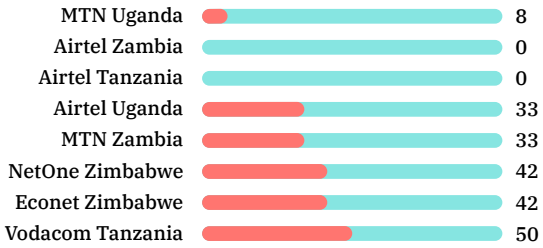
Changes to privacy policies



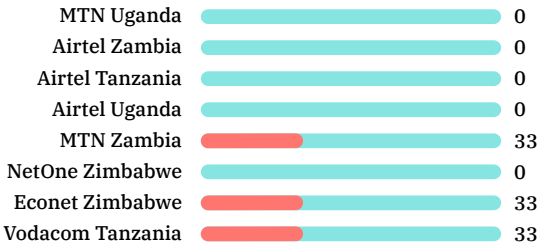
Users' control over their own user information



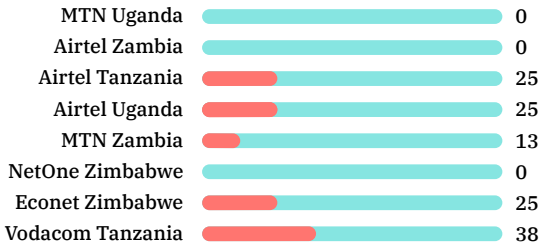
Collection of user information



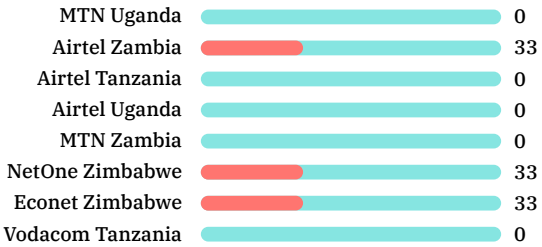
Users' access to their own user information



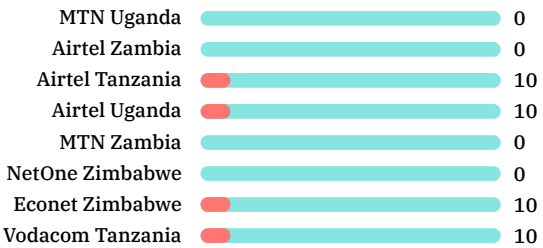
Sharing of user information



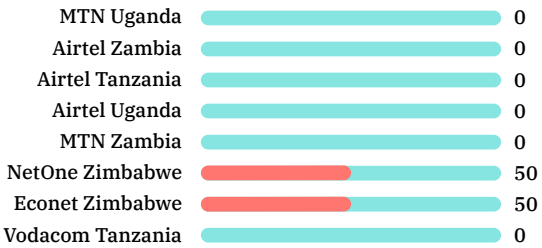
Account security (digital platforms)



Purpose for collecting, inferring, and sharing user information



Inform and educate users about potential risks



Changes to privacy policies

Only MTN Zambia discloses its commitment to inform its service users through email and/or a prominent notice of changes to their privacy policy, prior to the change becoming effective.[52] The other six companies with privacy policies state that changes made to their respective privacy policies are shared on the company's website. Econet also gives a broad commitment that the company might try to notify users of changes through "different channels before the changes come into effect."[53] None of the companies provides a timeframe for notification of changes

None of the companies commits to the use of maintaining and disclosing any change logs. This places the burden on the users to notice that there is an updated privacy policy and identify the changes made therein. None of the companies discloses a public change log relating to updates of their privacy policies.

The first data protection principle is that the processing of information should be lawful, necessary, and transparent. There is no transparency when a company silently changes its privacy policies without notifying the user of the specific changes and how those changes affect the users' right to privacy. We recommend that users be informed of each change to the privacy policy. This will enable users to give their informed consent to the processing of their personal information under the changed policies. This is why we urge companies to maintain publicly accessible change logs, which clearly show changes made to the different versions of policy documents.

52 Changes to the MTN privacy policy clause available at https://www.mtn.zm/privacy-policy-2/

53 Econet privacy policy available to https://www.econet.co.zw/privacy-policy

Recommendations

We recommend that:

- Privacy policies be published in locally accessible languages.[54]
- Companies maintain publicly available change logs, which show the changes made to their privacy policy.
- Companies explain some of the possible outcomes resulting from the processing of users' personal information.

Collection of user information

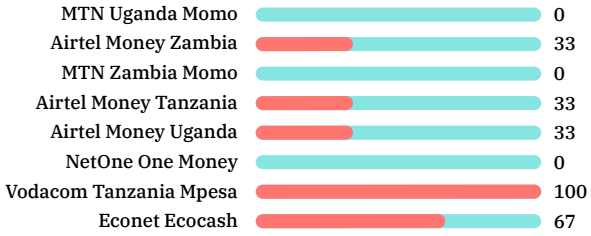
The eight telecommunications companies in this report collect information in several ways. The most common is when a new subscriber provides the company with their name, address, national identity information, and other personal information. When the subscriber begins to use the company's services, the company will collect usage data, which shows how the user is using the prepaid service and or mobile money service. Usage data will in most cases include metadata, which refers to information about other data. For example, this may be in the form of the numbers a user calls or messages, and the length of each of the calls. Usage data also reveals patterns and habits that may be useful in user profiling for purposes of serving those users with targeted ads.

In the four countries focused on in this report, telecommunications companies have a legal duty to intercept communications sent over their networks, due to the application of interception of communications laws, but none of the companies discloses this.
Their privacy policies mainly disclose the collection of user information either through the contact page on the company's website or when a user contacts a service provider for an inquiry. Only the privacy policies from Vodacom Tanzania and MTN Zambia contained a range of information collected by the telecommunications companies.

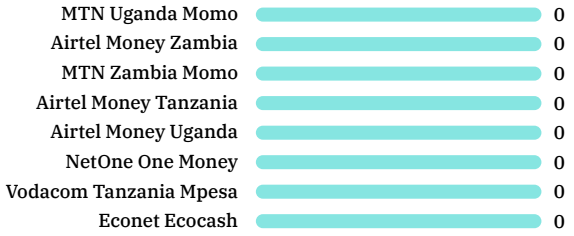
54 "Dutch DPA: TikTok fined for violating children's privacy." European Data Protection Board. July 22, 2021. https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en

Privacy Indicator scores for mobile money services

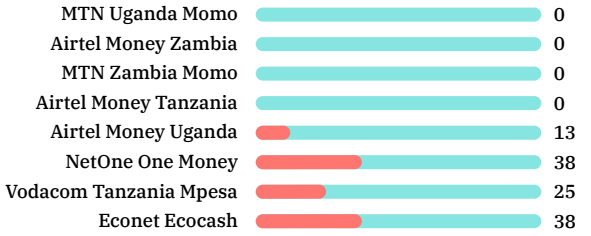
Access to privacy policies



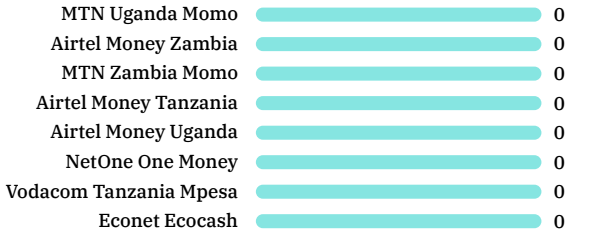
Access to algorithmic system development policies



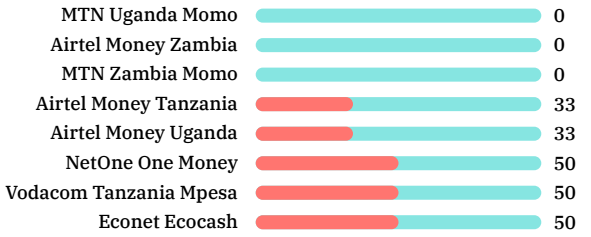
Changes to privacy policies



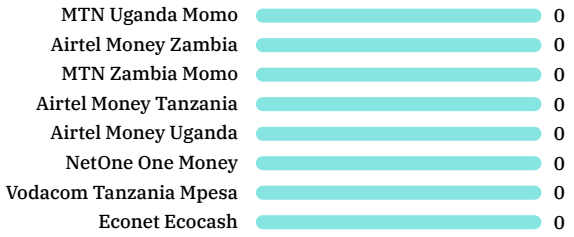
Changes to algorithmic system development policies



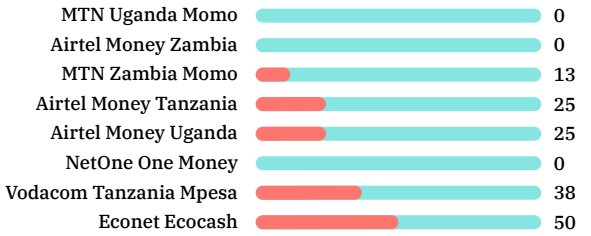
Collection of user information



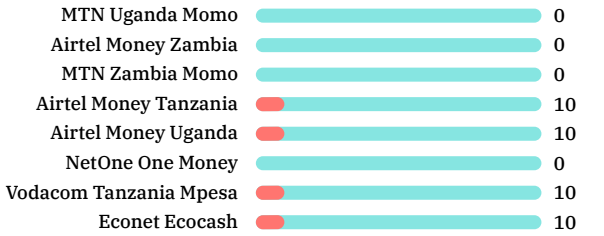
Inference of user information



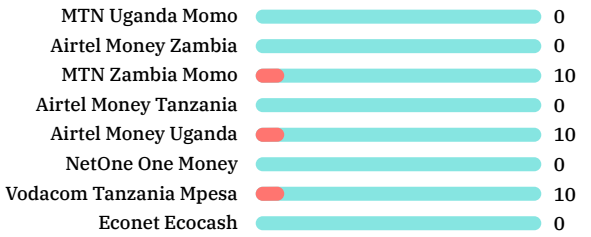
Sharing of user information



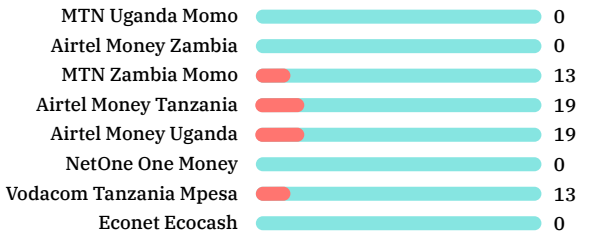
Purpose for collecting, inferring, and sharing user information

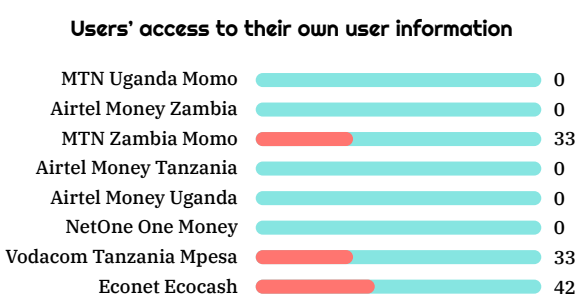


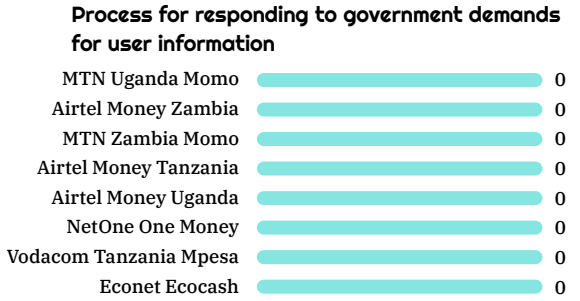
Retention of user information

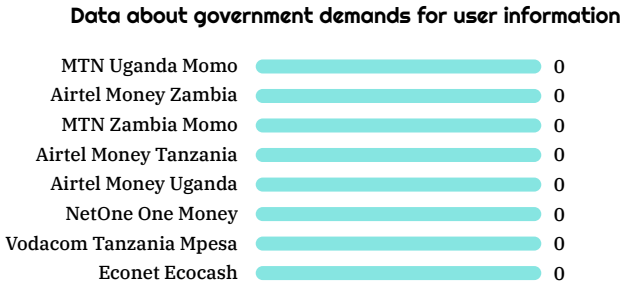


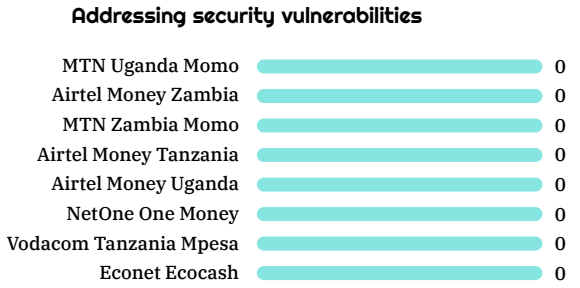
Users' control over their own user information

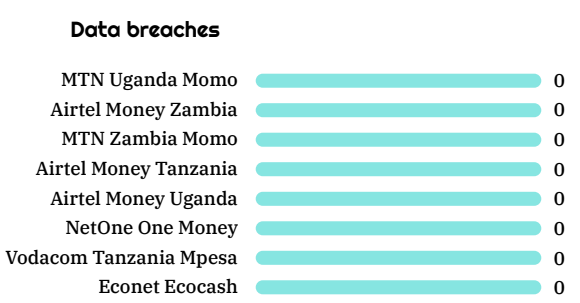


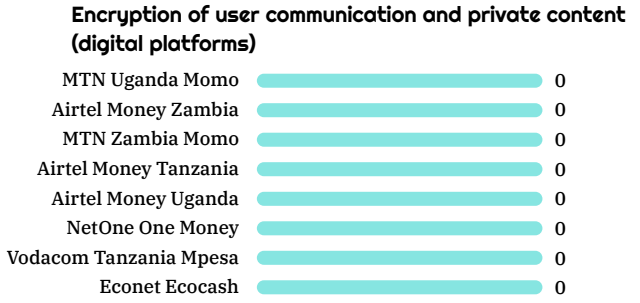


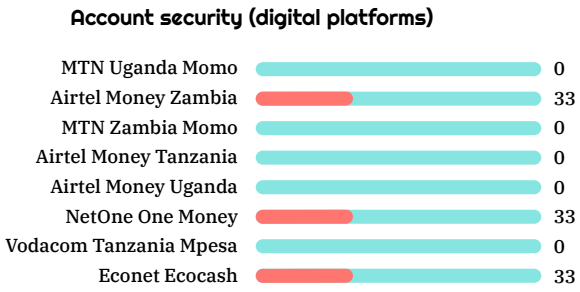


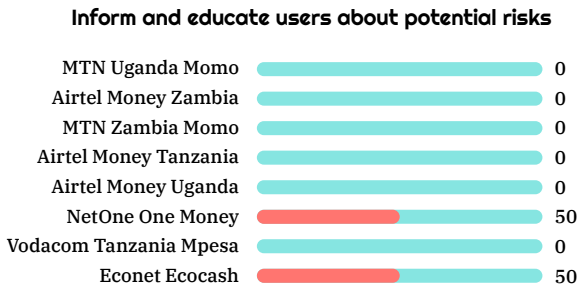












Inference of user information

None of the companies discloses policies on how they make inferences about user information.

Sharing of user information

Neither Airtel Uganda nor Airtel Tanzania discloses whether they share user information with any third parties. Other companies disclose that they share user information with third parties, mainly for marketing purposes; for example, Vodacom Tanzania reveals that they share anonymized user data with third parties. MTN Zambia's privacy policy discloses that it may engage third parties to facilitate services and in such instances those third parties will have access to users' personal information. Neither Econet and NetOne discloses whether they share information with third parties.

Vodacom Tanzania and the Airtel companies disclose that they share user information with law enforcement and government agencies when required to do so by law. Unfortunately, investigations under indicators P10(a) and P11(a) reveal that none of the eight telecommunications companies disclose their respective processes for responding to government demands for user information, or the circumstances under which they will decline government requests for user information. Such information would ideally be contained in a transparency report but none of the companies profiled in this research publishes any transparency reports. See also the discussion under indicator P11(a) below.

Purpose of collecting, inferring, and sharing user information

The main reason for collecting information given by the two MTN companies, the three Airtel companies, and Vodacom Tanzania is to contact the service user. The second most popular disclosed reason is that usage data is collected for the purpose of improving service delivery and for direct marketing. The most popular reason for sharing user information is for marketing purposes. The second most common reason among the eight telecommunications companies for sharing information is to comply with the law. None of the companies discloses that they collect or share inferred user information.

Retention of user information

None of the companies discloses how long they retain user information. The various privacy policies reviewed for this research instead disclose that companies will keep user and usage information for the length of time required by the law. None of the policies refers to any national legislation or other limits given within that law. MTN Zambia and Vodacom Tanzania refer to retaining usage information for as long as the law requires or permits it.

None of the companies discloses how the termination of a service agreement for either their prepaid services or mobile money services would affect data retention, or the limits placed on how long they could keep user information after service has been terminated.

Recommendations

We recommend that:

- Telecommunications companies disclose the different types of user information they collect and how they collect that data.
- Companies disclose fully in their user information the identity of third parties with access to user information.
- Companies give users greater control over who the company shares their personal information with.

Users' control over and access to their own user information

All the eight companies except NetOne invite users to contact them with inquiries regarding personal information the telecommunications companies collect from them. The privacy policies state that in certain (undisclosed) circumstances, users could ac-

cess their user information and where there were errors, require that those errors be corrected.

However, none of the policies set out what format the requested information would be shared in. Econet, in its privacy policy, states that a service user may in some undisclosed circumstances be required to pay to access some of their information. None of the disclosed privacy policies contains information on the process users must follow when requesting a copy of their information. Similarly, none of the disclosed policies mention the timelines within which the requested information would be shared, or a response given. None of the policies discloses whether it is possible for a user to transfer their personal information from one service provider to another.

Data about government demands for user information

As has been mentioned elsewhere in this report, none of the eight telecommunications companies have disclosed that they publish transparency reports, which would contain, among other things, data about government demands for user information. According to Access Now, "disclosing threats to privacy and free expression via transparency reports is one of the best ways for companies to communicate to their users and the public the steps they take to respect human rights."[55]

Although the eight companies do not publish transparency reports, there are some reported cases indicating that telecommunications companies operating in the four countries covered in this report do share information with government agencies, particularly state security agents.

Case study: Turning over information to state security agents

In Tanzania, the third largest mobile network operator, Tigo, testified in court against own of its own subscribers, who was charged with acts of terrorism. The accused, Free-

55 Oribhabor, I. "The what, why, and who of transparency reporting." *Access Now*. April 2, 2020. https://www.accessnow.org/the-what-why-and-who-of-transparency-reporting/

man Mbowe, is the leader of CHADEMA, a Tanzanian opposition political party. During his trial, Tigo's legal counsel Freddy Kapala made submissions as a state witness, including allegedly remarking that "Tigo's priority isn't to protect customers' privacy." Kapala also made disclosures about Mbowe's personal information, which had been collected by virtue of him being a Tigo service user. Kapala was a witness in another case involving a defendant named Abdul Nondo, who was charged with false publication of information in 2018.[56]

In Zimbabwe, the government has used location information acquired from Econet to dispute allegations made by opposition political party members that they had been abducted and tortured by state security agents.[57] Three members of the country's main opposition party reported that they were abducted and tortured by people suspected of being supporters of the ruling party.[58] The state disputed these allegations and instead charged the three women with treason.[59] As part of investigations against the three, the state produced what it claimed was their location data accessed from their respective mobile network providers. This location data was used to dismiss the women's abduction claims.[60]

Addressing security vulnerabilities

None of the companies covered in this report discloses any policies on whether non-staff members could approach the company to point out security vulnerabilities identified on their network, services, or platforms. Closely related to this, none of the companies discloses any information relating to the reporting or disclosure of data breaches (indicator P15).

56 "Freeman Mbowe, three others have a case to answer, Court rules." *Africa Press, Tanzania*. February 18, 2022. https://www.africa-press.net/tanzania/all-news/freeman-mbowe-three-others-have-a-case-to-answer-court-rules

57 ZimLive. "State closes case in Mamombe, Chimbiri 'fake' abduction." *Zimbabwe News Now*. August 17, 2022. https://www.zimlive.com/2022/08/state-closes-case-in-mamombe-chimbiri-fake-abduction/

58 Burke, J., & Chingono, N. "Zimbabwean MDC activists "abducted and sexually assaulted." *The Guardian*. May 17, 2020.https://www.theguardian.com/world/2020/may/17/zimbabwean-mdc-activists-abducted-and-sexually-assaulted

59 BBC News. "Zimbabwe's MDC "abductees arrested for lying about torture."" June 11, 2020. https://www.bbc.co.uk/news/world-africa-53005447

60 "Kazembe cornered over MDC 'abductees' case." Nehanda Radio. June 26, 2020. https://nehandaradio.com/2020/06/26/kazembe-cornered-over-mdc-abductees-case/

The companies also do not disclose whether they use encryption on their services and platforms. We did not find any disclosures to show that the companies use any advanced security methods to keep mobile money accounts secure. Mobile money services are based on the USSD platform and only secured via a PIN, with no possibility for added layers of security such as two-factor authentication 2FA (indicator P17). There is no disclosed policy from any of the companies on educating service users about their safety and security (indicator P18).

Recommendations

We recommend that companies:

- Publish regular transparency reports that disclose, among other information, the number of government requests for user information within a given period.
- Disclose the circumstances under which they will hand over user information to governments.
- Publish policies that permit security experts to report any identified vulnerabilities.
- Disclose policies on responses to data breaches.
- Commit to training and educating their users on cybersecurity practice.

Annex: List of indicators used in this research

Governance category indicators

G1. Policy Commitment

- G1.1: Does the company make an explicit, clearly articulated policy commitment to human rights, including to freedom of expression and information?
- G1.2: Does the company make an explicit, clearly articulated policy commitment to human rights, including to privacy?
- G1.3: Does the company disclose an explicit, clearly articulated policy commitment to human rights in its development and use of algorithmic systems?

G4(a). Impact assessment: governments and regulations

- G4a.1: Does the company assess how laws affect freedom of expression and information in jurisdictions where it operates?
- G4a.2: Does the company assess how laws affect privacy in jurisdictions where it operates?
- G4a.3: Does the company assess freedom of expression and information risks associated with existing products and services in jurisdictions where it operates?
- G4a.4: Does the company assess privacy risks associated with existing products and services in jurisdictions where it operates?
- G4a.5: Does the company assess freedom of expression and information risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
- G4a.6: Does the company assess privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions? G4a.7: Does the company

conduct additional evaluation whenever the company's risk assessments identify concerns?

- G4a.8: Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
- G4a.9: Does the company conduct assessments on a regular schedule?
- G4a.10: Are the company's assessments assured by an external third party?
- G4a.11: Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organisation?

G4(b). Impact assessment: processes for policy enforcement

- G4b.1: Does the company assess freedom of expression and information risks of enforcing its terms of service?
- G4b.2: Does the company conduct risk assessments of its enforcement of its privacy policies?
- G4b.3: Does the company assess discrimination risks associated with its processes for enforcing its terms of service?
- G4b.4: Does the company assess discrimination risks associated with its processes for enforcing its privacy policies?
- G4b.5: Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?
- G4b.6: Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
- G4b.7: Does the company conduct assessments on a regular schedule?
- G4b.8: Are the company's assessments assured by an external third party?
- G4b.9: Is the external third party that assures the assessments accredited to a relevant and reputable human rights standard by a credible organisation?

G4(c). Impact assessment: targeted advertising

- G4c.1: Does the company assess freedom of expression and information risks

associated with its targeted advertising policies and practices?

- G4c.2: Does the company assess privacy risks associated with its targeted advertising policies and practices?
- G4c.3: Does the company assess discrimination risks associated with its targeted advertising policies and practices?
- G4c.4: Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?
- G4c.5: Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
- G4c.6: Does the company conduct assessments on a regular schedule?
- G4c.7: Are the company's assessments assured by an external third party?
- G4c.8: Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organisation?

G5. Stakeholder engagement and accountability

- G5.1: Is the company a member of one or more multi-stakeholder initiatives that address the full range of ways in which users' fundamental rights to freedom of expression and information, privacy, and non-discrimination may be affected in the course of the company's operations?
  G5.2: If the company is not a member of one or more such multi-stakeholder initiatives, is the company a member of any organisation that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy issues?
- G5.3: If the company is not a member of one of these organisations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose rights to freedom of expression and information and to privacy are directly impacted by the company's business?

G6(a). Remedy

- G6a.1: Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their freedom of expression and information rights have been adversely affected by the company's policies or

practices?

- G6a.2: Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their privacy has been adversely affected by the company's policies or practices?
- G6a.3: Does the company clearly disclose its procedures for providing remedy for freedom of expression and information-related grievances?
- G6a.4: Does the company clearly disclose its procedures for providing remedy for privacy-related grievances?
- G6a.5: Does the company clearly disclose timeframes for its grievance and remedy procedures? G6a.6: Does the company clearly disclose the number of complaints it receives related to freedom of expression?
- G6a.7: Does the company clearly disclose the number of complaints it receives related to privacy?
- G6a.8: Does the company clearly disclose evidence that it is providing remedy for freedom of expression grievances?
- G6a.9: Does the company clearly disclose evidence that it is providing remedy for privacy grievances?

Freedom of expression and information category indicators

F1(a). Access to terms of service

- F1a.1: Are the company's terms of service easy to find?
- F1a.2: Are the terms of service available in the primary language(s) spoken by users in the company's home jurisdiction?
- F1a.3: Are the terms of service presented in an understandable manner?

F1(b). Access to advertising content policies

- F1b.1: Are the company's advertising content policies easy to find?
- F1b.2: Are the company's advertising content policies available in the primary language(s) spoken by users in the company's home jurisdiction?
- F1b.3: Are the company's advertising content policies presented in an understandable manner?

F1(c). Access to advertising targeting policies

- F1c.1: Are the company's advertising targeting policies easy to find?
- F1c.2: Are the advertising targeting policies available in the primary language(s) spoken by users in the company's home jurisdiction?
- F1c.3: Are the advertising targeting policies presented in an understandable manner?

F1(d). Access to algorithmic system use policies

- F1d.1: Is the company's algorithmic system use policies easy to find?
- F1d.2: Are the algorithmic system use policies available in the primary language(s) spoken by users in the company's home jurisdiction?
- F1d.3: Are the algorithmic systems use policies presented in an understandable manner?

F2(a). Changes to terms of service

- F2a.1: Does the company clearly disclose that it directly notifies users about all changes to its terms of service?
- F2a.2: Does the company clearly disclose how it will directly notify users of changes?
- F2a.3: Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to such changes coming into effect?
- F2a.4: Does the company maintain a public archive or change log?

F2(b). Changes to advertising content policies

- F2b.1: Does the company clearly disclose that it directly notifies users about changes to its advertising content policies?
- F2b.2: Does the company clearly disclose how it will directly notify users of changes?
- F2b.3: Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
- F2b.4: Does the company maintain a public archive or change log?
- F2(c). Changes to advertising targeting policies
- F2c.1: Does the company clearly disclose that it directly notifies users about changes to its advertising targeting policies?
- F2c.2: Does the company clearly disclose how it will directly notify users of changes?
- F2c.3: Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
- F2c.4: Does the company maintain a public archive or change log?

F2(d). Changes to algorithmic system use policies

- F2d.1: Does the company clearly disclose that it directly notifies users about changes to its algorithmic system use policies?
- F2d.2: Does the company clearly disclose how it will directly notify users of changes?
- F2d.3: Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
- F2d.4: Does the company maintain a public archive or change log?

F3(b). Advertising content rules and enforcement

- F3b.1: Does the company clearly disclose what types of advertising content it does not permit?
- F3b.2: Does the company clearly disclose whether it requires all advertising content to be clearly labelled as such?
- F3b.3: Does the company clearly disclose the processes and technologies it uses to identify advertising content or accounts that violate the company's rule?
- F3(c). Advertising targeting rules and enforcement
- F3c.1: Does the company clearly disclose whether it enables third parties to target its users with advertising content?
- F3c.2: Does the company clearly disclose what types of targeting parameters are not permitted?
- F3c.3: Does the company clearly disclose that it does not permit advertisers to target specific individuals?
- F3c.4: Does the company clearly disclose that algorithmically generated advertising audience categories are evaluated by human reviewers before they can be used?
- F3c.5: Does the company clearly disclose information about the processes and technologies it uses to identify advertising content or accounts that violate the company's rules?

F4(a). Data about content restrictions to enforce terms of service

- F4a.1: Does the company publish data about the total number of pieces of content restricted for violating the company's rules?
- F4a.2: Does the company publish data on the number of pieces of content restricted based on which rule was violated?
- F4a.3: Does the company publish data on the number of pieces of content it restricted based on the format of content? (e.g., text, image, video, live video)?
- F4a.4: Does the company publish data on the number of pieces of content it restricted based on the method used to identify the violation?
- F4a.5: Does the company publish this data at least four times a year?
- F4a.6: Can the data be exported as a structured data file?

F4(b). Data about account restrictions to enforce terms of service

- F4b.1: Does the company publish data on the total number of accounts restricted for violating the company's own rules?
- F4b.2: Does the company publish data on the number of accounts restricted based on which rule was violated?
- F4b.3: Does the company publish data on the number of accounts restricted based on the method used to identify the violation?
- F4b.4: Does the company publish this data at least four times a year?
- F4b.5: Can the data be exported as a structured data file?

F4(c). Data about advertising content and advertising targeting policy enforcement

- F4c.1: Does the company publish the number of advertisements it restricted to enforce its advertising content policies?
- F4c.2: Does the company publish the number of advertisements it restricted based on which advertising content rule was violated?
- F4c.3: Does the company publish the number of advertisements it restricted to enforce its advertising targeting policies?
- F4c.4: Does the company publish the number of advertisements it restricted based on which advertising targeting rule was violated?
- F4c.5: Does the company publish this data at least once a year?
- F4c.6: Can the data be exported as a structured data file?

F9. Network management (telecommunications companies)

- F9.1: Does the company clearly disclose a policy commitment to not prioritize, block or delay certain types of traffic, applications, protocols or content for reasons beyond assuring quality of service and reliability of the network?
- F9.2: Does the company engage in practices such as offering zero-rating programmes that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network?
- F9.3: If the company engages in network prioritisation practices for reasons beyond assuring quality of service and reliability of the network, does it clearly

disclose its purpose for doing so?

F10. Network shutdown (telecommunications companies)

- F10.1: Does the company clearly disclose the reason(s) why it may shut down service to a particular area or group of users?
- F10.2: Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?
- F10.3: Does the company clearly disclose its process of responding to government demands to shut down a network or restrict access to a service?
- F10.4: Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?
- F10.5: Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?
- F10.6: Does the company clearly disclose the number of network shutdown demands it receives?
- F10.7: Does the company clearly disclose the specific legal authority that makes the demands?
- F10.8: Does the company clearly disclose the number of government's demands with which it complied?

F11. Identity policy

- F11.1: Does the company require users to verify their identity using their government-issued identification, or with other forms of identification that could be connected to their offline identity?

Privacy category indicators

P1(a). Access to privacy policies

- P1a.1: Are the company's privacy policies easy to find?
- P1a.2: Are the privacy policies available in the primary language(s) spoken by users in the company's home jurisdiction?

- P1a.3: Are the privacy policies presented in an understandable manner?

P1(b). Access to algorithmic system development policies

- P1b.1: Are the company's algorithmic system development policies easy to find?
- P1b.2: Are the algorithmic system development policies available in the primary language(s) spoken by users?
- P1b.3: Are the algorithmic system development policies presented in an understandable manner?
- P2(a). Changes to privacy policies
- P2a.1: Does the company clearly disclose that it directly notifies users about all changes to its privacy policies?
- P2a.2: Does the company clearly disclose how it will directly notify users of changes?
- P2a.3: Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
- P2a.4: Does the company maintain a public archive or change log?

P2(b). Changes to algorithmic system development policies

- P2b.1: Does the company clearly disclose that it directly notifies users about all changes to its algorithmic system development policies?
- P2b.2: Does the company clearly disclose how it will directly notify users of changes?
- P2b.3: Does the company clearly disclose the time frame within which it directly notifies users of changes prior to these changes coming into effect?
- P2b.4: Does the company maintain a public archive or change log?

P3(a). Collection of user information

- P3a.1: Does the company clearly disclose what types of user information it collects?
- P3a.2: Does the company clearly disclose how it collects each type of user information?

- P3a.3: Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?

P3(b). Inference of user information

- P3b.1: Does the company clearly disclose all the types of user information it infers on the basis of collected user information?
- P3b.2: For each type of user information the company infers, does the company clearly disclose how it infers that user information?
- P3b.3: Does the company clearly disclose that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?

P4. Sharing of user information

- P4.1: For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
- P4.2: For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?
- P4.3: Does the company clearly disclose that it may share user information with government(s) or legal authorities?
- P4.4: For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information?

P5. Purpose for collecting, inferring, and sharing user information

- P5.1: For each type of user information the company collects, does the company clearly disclose its purpose for collection?
- P5.2: For each type of user information the company infers, does the company clearly disclose its purpose for the inference?
- P5.3: Does the company clearly disclose whether it combines user information from various company services and if so, why?
- P5.4: For each type of user information the company shares, does the company

clearly disclose its purpose for sharing?
- P5.5: Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred?

P6. Retention of user information

- P6.1: For each type of user information the company collects, does the company clearly disclose how long it retains that user information?
- P6.2: Does the company clearly disclose what de-identified user information it retains?
- P6.3: Does the company clearly disclose the process for de-identifying user information?
- P6.4: Does the company clearly disclose that it deletes all user information after users terminate their account?
- P6.5: Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?

P7. Users' control over their own user information

- P7.1: For each type of user information the company collects, does the company clearly disclose whether users can control the company's collection of this user information?
- P7.2: For each type of user information the company collects, does the company clearly disclose whether users can delete this user information?
- P7.3: For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can control if the company can attempt to infer this user information?
- P7.4: For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can delete this user information?
- P7.5: Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?
- P7.6: Does the company clearly disclose that targeted advertising is off by default?
- P7.7: Does the company clearly disclose that it provides users with options to control how their user information is used for the development of algorithmic systems?

- P7.8: Does the company clearly disclose whether it uses user information to develop algorithmic systems by default, or not?

P8. Users' access to their own user information

- P8.1: Does the company clearly disclose that users can obtain a copy of their user information?
- P8.2: Does the company clearly disclose what user information users can obtain?
- P8.3: Does the company clearly disclose that users can obtain their user information in a structured data format?
- P8.4: Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?
- P8.5: Does the company clearly disclose that users can access the list of advertising audience categories to which the company has assigned them?
- P8.6: Does the company clearly disclose that users can obtain all the information that a company has inferred about them?

F9. Network management (telecommunications companies): The company should clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.

- F9.1: Does the company clearly disclose a policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?
- F9.2: Does the company engage in practices, such as offering zero-rating programs, that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network?
- F9.3: If the company does engage in network prioritization practices for reasons beyond assuring quality of service and reliability of the network, does it clearly disclose its purpose for doing so?

P10(a). Process of responding to government demands for user information

- P10a.1: Does the company clearly disclose its process of responding to non-judicial government demands?
- P10a.2: Does the company clearly disclose its process of responding to court orders?
- P10a.3: Does the company clearly disclose its process of responding to government demands from foreign jurisdictions?
- P10a.4: Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?
- P10a.5: Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?
- P10a.6: Does the company commit to push back on inappropriate or overbroad government demands?
- P10a.7: Does the company provide clear guidance or examples of implementation of its process for government demands?

P11(a). Data about government demands for user information

- P11a.1: Does the company list the number of government demands it receives by country?
- P11a.2: Does the company list the number of government demands it receives for stored user information and for real-time access to communications?
- P11a.3: Does the company list the number of accounts affected?
- P11a.4: Does the company list whether a demand sought communications content or non-content or both?
- P11a.5: Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?
- P11a.6: Does the company include government demands that come from court orders?
- P11a.7: Does the company list the number of government demands it complied with, broken down by category of demand?
- P11a. 8: Does the company list what types of government demands it is prohibited by law from disclosing?

- P11a. 9: Does the company report this data at least once per year?
- P11a.10: Can the data reported by the company be exported as a structured data file?

P14. Addressing security vulnerabilities

- P14.1: Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?
- P14.2: Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities?
- P14.3: Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?

P15. Data breaches

- P15.1: Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?
- P15.2: Does the company clearly disclose its process of notifying data subjects who might be affected by a data breach?
- P15.3: Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?

P16. Encryption of user communication and private content (digital platforms)

- P16.1: Does the company clearly disclose that the transmission of user communications is encrypted by default?
- P16.2: Does the company clearly disclose that transmissions of user communications are encrypted using unique keys?
- P16.3: Does the company clearly disclose that users can secure their private content using end-to-end encryption, or full-disk encryption (where applicable)?
- P16.4: Does the company clearly disclose that end-to-end encryption, or full-disk encryption, is enabled by default?

P17. Account security (digital platforms)

- P17.1: Does the company clearly disclose that it deploys advanced authentication methods to prevent fraudulent access?
- P17.2: Does the company clearly disclose that users can view their recent account activity?
- P17.3: Does the company clearly disclose that it notifies users about unusual account activity and possible unauthorised access to their accounts?

P18. Inform and educate users about potential risks

- P18.1: Does the company publish practical materials that educate users on how to protect themselves from cybersecurity risks relevant to their products or services?

Bibliography

"Freeman Mbowe, three others have a case to answer, Court rules." Africa Press, Tanzania. February 18, 2022. https://www.africa-press.net/tanzania/all-news/freeman-mbowe-three-others-have-a-case-to-answer-court-rules

African Financials Digital Team. "Airtel Networks Zambia customer base stands at 6.771 million, up 16.02% Y-o-Y." African Financials. March 12, 2021. https://african-financials.com/airtel-networks-zambia-customer-base-stands-at-6-771-million-up-16-02-y-o-y/

"Zimbabwe imposes internet shutdown amid crackdown on protests." News | Al Jazeera. January 18, 2019. https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests

Anthonio, F. "Shutdown in Zambia on election day: How it affected people's lives and wellbeing." Access Now. September 21, 2021. https://www.accessnow.org/shutdown-in-zambia-on-election-day-how-it-affected-peoples-lives-and-wellbeing/

"Zimbabwe's MDC 'abductees arrested for lying about torture.'" BBC News. June 11, 2020. https://www.bbc.co.uk/news/world-africa-53005447

Burke, J., & Chingono, N. "Zimbabwean MDC activists "abducted and sexually assaulted."" The Guardian. May 17, 2020. https://www.theguardian.com/world/2020/may/17/zimbabwean-mdc-activists-abducted-and-sexually-assaulted

Delaporte, A. "The state of mobile internet connectivity in Sub-Saharan Africa: Why addressing the barriers to mobile internet use matters now more than ever." Mobile for Development. January 4, 2022. https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-internet-connectivity-in-sub-saharan-africa/

Dheere, J. "The new shape of the RDR Corporate Accountability Index." Ranking Digital Rights. March 15, 2022. https://rankingdigitalrights.org/2022/02/23/new-corporate-accountability-index-big-tech-scorecard/

"Dutch DPA: TikTok fined for violating children's privacy." European Data Protection Board. https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en

Electronic and Postal Communications (SIM Card Registration) Regulations (the SCR Regulations), 2020. Tanzania

"Govt should prioritise internet affordability as a human right." MISA Zimbabwe. May 11, 2020. https://zimbabwe.misa.org/2020/05/11/govt-should-prioritise-internet-affordability-as-a-human-right/

GSMA Mobile Internet Connectivity 2020: Sub-Saharan Africa Factsheet. 2020. GSMA. https://www.gsma.com/r/wp-content/uploads/2020/09/Mobile-Internet-Connectivity-SSA-Fact-Sheet.pdf

Interception of Communications Act, Zimbabwe

"MTN Has Over 50% Market Share in 10 African Countries." Connecting Africa. September 2, 2019. https://www.connectingafrica.com/author.asp?doc_id=753808

"MTN Uganda Hands over UGX 15 million to its 15 millionth subscriber as the Telecom Celebrates its 15 million Customer Base." MTN Uganda. August 3,2021. https://www.mtn.co.ug/mtn-uganda-hands-over-ugx-15-million-to-its-15-millionth-subscriber-as-the-telecom-celebrates-its-15-million-customer-base/

Muhamba, V. "CBZ Bank joins the zero-rate revolution." Techzim. May 17, 2021. https://www.techzim.co.zw/2021/05/cbz-bank-joins-the-zero-rate-revolution/

Muhamba, V. "The dominos are falling fast; NMBConnect is now zero-rated." Techzim. June 15, 2021. https://www.techzim.co.zw/2021/06/the-dominos-are-falling-fast-nmb-connect-is-now-zero-rated/

Muller, R. "Vodacom prepaid customers hit by airtime theft." July 27, 2020. https://mybroadband.co.za/news/cellular/361389-vodacom-prepaid-customers-hit-by-airtime-theft.html

My Broadband. "Vodacom's results inflated by fraudulent subscriptions." August

23, 2022. https://mybroadband.co.za/news/cellular/457587-vodacoms-results-in-flated-by-fraudulent-subscriptions.html

Nehanda Radio. Kazembe cornered over MDC 'abductees' case. Nehanda Radio. June 26, 2020. https://nehandaradio.com/2020/06/26/kazembe-cornered-over-mdc-abductees-case/

O'Grady, V. "Airtel Tanzania grows subscriber numbers and expands 4G coverage." Developing Telecoms. February 4, 2020. https://developingtelecoms.com/telecom-technology/wireless-networks/9165-airtel-tanzania-grows-subscriber-numbers-and-expands-4g-coverage.html

OHCHR. International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

OHCHR. Universal Declaration of Human Rights. https://www.ohchr.org/en/udhr/pages/introduction.aspx

Oribhabor, I. "The what, why, and who of transparency reporting." Access Now. April 2, 2020. https://www.accessnow.org/the-what-why-and-who-of-transparency-reporting/

Postal and Telecommunications Act, Zimbabwe

Postal and Telecommunications Regulatory Authority of Zimbabwe Abridged Postal and Telecommunications Sector Performance Report Third Quarter 2021. POTRAZ https://www.techzim.co.zw/wp-content/uploads/2021/12/Abridged-Sector-Performance-Report-Q3-2021-HMed.pdf

Postal & Telecommunications (Subscriber Registration) Regulations, 2014 (SI 95 of 2014). Zimbabwe

Regulatory directive issued by the Uganda Communications Commission in terms of Uganda's Communications Act, 2014

Sakpa, D. "Tanzania restricts social media during election." DW. October 29, 2020. https://www.dw.com/en/tanzania-restricts-social-media-during-election/a-55433057

Ssessanga, I. “Tanzania: Internet slowdown comes at a high cost.” DW. November 5, 2020. https://www.dw.com/en/tanzania-internet-slowdown-comes-at-a-high-cost/a-55512732

Statista. Share of mobile subscriptions Uganda 2015-2022, by operator. October 20, 2021. https://www.statista.com/statistics/671666/mobile-subscription-share-in-uganda-by-operator/

Statutory Instrument on the Registration of Electronic Communication Apparatus No. 65 of 2011. Zambia

The GNI Principles. Global Network Initiative. https://globalnetworkinitiative.org/gni-principles/

The promotion, protection, and enjoyment of human rights on the Internet (A/HRC/47/L.22) http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/47/L.22&Lang=E

The 2022 Ranking Digital Rights Big Tech Scorecard. Ranking Digital Rights. https://rankingdigitalrights.org/index2022/

“Uganda 2021 general elections: The internet shutdown and its ripple effects.” Association for Progressive Communications. January 25, 2021. https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects

UNHRC, Draft resolution: The promotion, protection, and enjoyment of human rights on the Internet, 47th Sess, 2021, (A/HRC/47/L.22) http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/47/L.22&Lang=E

United Nations Guidelines for Consumer Protection https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf

United Nations Guiding Principles on Business and Human Rights https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-hu-

man-rights

"Zanu-PF, Econet dragged to court over SMS." Bulawayo24 News. July 13, 2018. https://bulawayo24.com/index-id-news-sc-national-byo-140387.html

ZimLive. "State closes case in Mamombe, Chimbiri 'fake' abduction." Zimbabwe News Now. August 17, 2022. https://www.zimlive.com/2022/08/state-closes-case-in-mamombe-chimbiri-fake-abduction/

101: SIM Card Registration https://privacyinternational.org/explainer/2654/101-sim-card-registration

2020 Indicators. Ranking Digital Rights. June 15, 2022. https://rankingdigitalrights.org/2020-indicators/

2020 Ranking Digital Rights Corporate Accountability Index. Ranking Digital Rights. https://rankingdigitalrights.org/index2020/methodology

2023