INTERNET SANSFRONTIÈRES

DIGITAL RIGHTS IN SUB SAHARAN AFRICA

ANALYSIS OF PRACTICES BY ORANGE IN SENEGAL AND SAFARICOM IN KENYA

January 2018

https://internetwithoutborders.org

ACKNOWLEDGEMENTS 4

INTRODUCTION 5

METHODOLOGY 7

PRESENTATION OF COMPANIES 11

1. 1. Terms of use of Orange Senegal and Safaricom 12

1.1 Unpublished and unclear terms of use of Orange Senegal (Sonatel) and Safaricom's prepaid services 12

1.1.1 Inaccessibility of the terms and conditions of Orange Senegal's prepaid services 12

1.1.2 Safaricom’s vague terms of use 13

1.2 Consequences of lacking or unclear terms of use 15

1.2.1 Freedom of expression online weakened in Senegal 16

1.2.2 Possibility of an Internet shutdown in Kenya 18

2. Privacy policies of Orange Senegal and Safaricom 20

2.1 The lack of publication of Orange Senegal and Safaricom’s privacy policies 21

2.1.1 Lack of access to Orange's privacy policies Senegal 21

2.1.2 Safaricom’s concise privacy policy 23

2.2 Impact on privacy 26

2.2.1 Orange Senegal's products, raise questions about the impact on privacy 26

2.2.2 Privacy and gender based violence committed on Safaricom's network 27

3 Conclusion and recommendations 27

Internet Without Borders is a non-profit organization, and a network of non-governmental organizations, promoting and defending a free, open Internet, accessible to all without discrimination.

This study was funded by a grant from Access Now. The content of this study is available under creative commons license CC-BY-4.0.

ACKNOWLEDGEMENTS

Internet Without Borders thanks the following institutions and persons, whose help and support made this publication possible:

The Ranking Digital Rights Project team, for its invaluable support, advice and trust: in particular the Director Rebecca Mackinnon;

The Access Now Grants team for the generous support: Billie Goodman and Kevin Willits.

In Senegal :
- The Digital and New Media Lab, at the School of Journalism, Internet and Communications (EJICOM). Special thanks to the Director, Hamadou Tidiane Sy, and Sahite Gaye, lecturer and researcher;
- Senegal's Personal Data Commission;

In Kenya:
- Deep appreciation to the IAWRT Kenya team led by Racheal Nakitare for tireless effort in ensuring we secured the required interviews and got the relevant information for the study.

- Safaricom officer for finding time to grant us the interview:
Agnes Okello, principal Officer, Public Policy
Sandra Ojiambo, Head of Corporate Responsibility
Karimi Ruria, Senior Manager, Public Policy

- KICTANET for hosting the online engagement with Safaricom Corporate Affairs Manager Samuel Chege on which we participated and also extracted some of the responses for our study.

- John Walubengo - ICT lecturer (Multi Media University)
- Alice Munyua - Convenor . Kenya ICT action Network (KICTANet)
- Sharon Mungai - Communications Authority

INTRODUCTION

Since the early 2010s, the African continent witnesses one of the fastest connectivity growth, after years in the shadow: According to the Internet Society, in 2005, the Internet penetration rate in Europe was nearly 20 times that of Africa. In 2014, it was less than 4 times[1]. The youth of the African population helps explain this rapid growth.

This connectivity leap has advantages: not a day goes by without the latest African innovation being featured. The application market is experiencing unparalleled vitality: faced with development issues, many use their creativity to offer digital solutions[2].

Although they were among the first to understand the digital opportunities, young African citizens are no longer alone. A growing number of states have announced the gradual transition of their country towards a digital economy. Internet companies, such as Facebook or Twitter, and telecom operators like Orange and Vodafone, are changing their strategy to target the African market, and provide services that meet its needs.

Paradoxically, digital rights of African Internet users have never been in such jeopardy[3].

Although lacking scientific definition, digital rights have a wikipedia definition[4]: they are "*rights that allow individuals to access, use, create and publish digital media or access and use of computers, other electronic devices or communications networks.* " These rights are specifically related "to the protection and realization of existing rights, such as the right to privacy or freedom of expression in the context of new digital technologies, particularly the Internet", the definition adds.

For the United Nations, human rights offline must also be protected online. These rights include in particular freedom of expression and the right to privacy[5].

Recent reports on the state of human rights in Africa online show a worrying situation on the continent. According to the Freedom of the Net ranking, set up every year by Freedom House, only 2 out of 14 African countries assessed have a free Internet[6].

Although they are primarily responsible for this poor situation, governments are not the only ones involved.

Internet Intermediaries are important actors of digital rights. As defined by the OECD, “Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services

---

[1]Internet development and Internet governance in Africa - Towela Nyirenda-Jere & Tesfaye Biru https://www.internetsociety.org/sites/default/files/Internet%20development%20and%20Internet%20governance%20in%20Africa.pdf

[2]Can the Internet reboot Africa? - The Guardianhttps://www.theguardian.com/world/2016/jul/25/can-the-internet-reboot-africa

[3]See report by Paradigm Initiative - Choking the pipe: How Governments Hurt Internet Freedom on a Continent that Needs Access http://pinigeria.org/2016/wp-content/uploads/documents/research/Digital%20Rights%20In%20Africa%20Report%202016%20%28LR%29.pdf

[4]https://en.wikipedia.org/wiki/Digital_rights

[5]ResolutionA/HRC/26/L.24 https://documents-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement

[6]Freedom of the Net 2016 https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf

originated by third parties on the Internet or provide Internet-based services to third parties"[7]. This definition includes, for example, companies, which provide email services or social network; or telecommunications operators, which provide Internet access.

In 2011, the United Nations Human Rights Council adopted the Guiding Principles on Business and Human Rights[8] (UNGPs), which apply to all sectors of the economy, including telecommunications and Internet. Based on three pillars, Protect - Respect - Repair these principles define norms of practice for two actors; first, the States have the duty to protect against human rights abuses by third parties, including businesses. The latter should respect human rights by exercising due diligence in their business. Finally, States and companies should put in place effective remedy mechanisms available to victims of human rights abuse.

The guiding principle n°11 provides that,

"Companies should respect human rights. This means they should avoid infringing other people's human rights and address the negative impact on human rights in which they have a responsibility."

This text, although not binding, raises a standard of practice that should be adopted by companies, particularly those operating in the sector of digital, and new information and communications technologies.

Do Companies operating on the Internet respect the standards set out in the UN Guiding principles? In particular, do these firms respect online freedom of expression and privacy of their users in Africa? **More broadly, what is the responsibility of Internet intermediaries in the poor state of digital rights observed on the African continent?**

To answer these questions, Internet Without Borders turned to a tool created in 2015 to assess the corporate accountability of telecommunications companies: *the corporate accountability index*. Created by the Ranking Digital Rights Project team (hereinafter RDR)[9], this index ranks digital companies on how they respect the freedom of expression and the right to privacy of their users. The Index focuses on how companies behave on their native markets. For example, Facebook is assessed on its practices on the US market, Yandex on the Russian market, etc.

This ranking is now recognized by the companies themselves as an innovative tool enabling them to improve their responsibility on freedom of expression and privacy[10].

Internet Without Borders explored the applicability of the RDR methodology to companies operating on the digital market in sub saharan Africa. To assess the relevance of this index, Internet Without Borders focused on two companies leading the telecommunications market: Orange and Vodafone.

Internet Without Borders chose these companies for two reasons. They were both evaluated in 2015 and 2017 in the corporate accountability

---

[7]See OECD publication https://www.oecd.org/internet/ieconomy/44949023.pdf

[8]UN Guiding principles on Business and Human Rightshttp://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[9]https://rankingdigitalrights.org/

[10]In its 2016 annual report, the South African company MTN said it had initiated internal changes, including the publication of an internal guide for the human rights risk assessment of its products, following its assessment in The 2015 index https://rankingdigitalrights.org/index2017/companies/mtn/

index: Orange was evaluated on the services offered to its users in France, Vodafone in the UK. Both obtained honorable scores in the 2017 index , particularly Vodafone, which topped all telecommunications operators[11].

In addition, both have taken unequivocal commitments to respect freedom of expression and right to privacy, as members of the Telecom Industry Dialogue[12] and the Global Network Initiative[13]. These two self-regulatory platforms, bringing together representatives of the digital industry, invite members to adopt practices directly inspired from the UNGP, to strengthen the protection of freedom of expression and the right to privacy online.

Internet Without Borders asked whether the ranking of these two companies in the 2017 corporate accountability index, would be reflected on the sub saharan African market, which is important to Orange[14] and Vodafone[15].

The case study which follows focuses on the case of Orange in Senegal and Vodafone Kenya, through the shares it holds in the capital of the operator Safaricom.

Do these companies respect the norms and international standards on privacy and freedom of expression when operating on the African continent?

Our study demonstrates that despite clear commitments at the group level on privacy and freedom of expression, Vodafone and Orange can do better when it comes to protecting freedom of expression and privacy of their users through their subsidiaries in Senegal and Kenya.

The combination of weak legal environments in Sub saharan Africa, regulators with limited means of action, uneducated civil society on the issue of digital rights, helps explain why both companies are not stimulated to better perform in the protection of freedom of expression and the right to privacy of their users.

We hope this paper will allow them to complement their analysis of the dysfunctions of their policies to respect the human rights of their users. Especially freedom of expression and privacy online.

METHODOLOGY

For the purposes of this study, we applied the RDR methodology[16].

The objective is to evaluate the transparency and clarity of each company's policies and practices on Freedom of expression and privacy.

The methodology is based on three categories, divided into 35 indicators:

- Governance (G): this category contains 6 indicators measuring company disclosure of their commitments to freedom of expression and privacy principles and standards at the corporate governance level.
- Freedom of Expression (F): this category

[11]See ranking in 2017https://rankingdigitalrights.org/index2017/

[12]http://www.telecomindustrydialogue.org/about/

[13]https://globalnetworkinitiative.org/about/index.php

[14]Orange à la conquête de l'Afrique - Les Echos 24/02/2016 https://www.lesechos.fr/idees-debats/cercle/cercle-154427-strategie-dorange-en-afrique-le-grand-retour-1202599.php

[15]Vodafone Group Plc, annual report 2017https://www.vodafone.com/content/annualreport/annual_report17/downloads/Vodafone-strategic-report-2017.pdf

[16] The 2017 index methodology is available here https://rankingdigitalrights.org/2017-indicators/

contains 11 indicators measuring company disclosure of their policies and practices that affect users' freedom of expression rights.
● Privacy (P): this category contains 18 indicators measuring company disclosure of their policies and practices that affect users' privacy rights.

All companies are evaluated with the same indicators, with a slight difference for telecoms operators, which are assessed on their prepaid, postpaid and fixed services.

The research team focused here on the prepaid services of the companies studied: indeed, prepaid plans constitute almost all of the 15 million SIM cards sold by Orange in Senegal[17]; at Safaricom, prepaid services account for 96% of customer SIM cards[18].

Our team selected relevant indicators relating to the protection of privacy and freedom of expression, with the aim of a preliminary analysis, which would precede a full implementation of a corporate accountability index in Sub saharan Africa.

For this study, our analysis followed four steps:

1. We first analyzed the content of companies' websites, to identify terms of use or privacy policies, corresponding to indicators F1, F2, P1 and P2. We wanted to know if companies respected the right to information of their users, by publishing these important legal documents.

F1. Access to terms of service
The company should offer terms of service that are easy to find and easy to understand. Elements:
1. Are the company's terms of service easy to find?
2. Are the terms of service available in the language(s) most commonly spoken by the company's users?
3. Are the terms of service are presented in an understandable manner?

F2. Changes to terms of service
The company should clearly disclose that it provides notice and documentation to users when it changes its terms of service.
Elements:
1. Does the company clearly disclose that it notifies users about changes to its terms of service?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the timeframe within which it provides notification prior to changes coming into effect?
4. Does the company maintain a public archive or change log?

P1. Access to privacy policies
The company should offer privacy policies that are easy to find and easy to understand. Elements:
1. Are the company's privacy policies easy to find?
2. Are the privacy policies available in the language(s) most commonly spoken by the company's users?
3. Are the policies presented in an understandable manner?

P2. Changes to privacy policies
The company should clearly disclose that it provides notice and documentation to users when it changes its privacy policies.
Elements:
1. Does the company clearly disclose that it notifies users about changes to its privacy policies?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the time frame within which it provides notification prior to changes coming into effect?
4. Does the company maintain a public archive or

[17]Activities of Orange Senegal, published on May 4, 2017 https://www.orange.com/fr/Groupe/Presence-mondiale/Pays/Les-activites-d-Orange-Senegal

[18]Safaricom Annual report 2017, p. 22 p. 22 https://www.safaricom.co.ke/images/Downloads/Resources_Downloads/Safaricom_Limited_2016_Annual_Report.pdf

change log?

2. Once the existence of terms of use and privacy policy was identified on the website, we sought to evaluate the accuracy of these policies: the more precise they are, the more the company is transparent by disclosing as much information as possible to the users. We continued our analysis with indicators F3, P3, P4, P5.

F3. Process for terms of service enforcement
The company should clearly disclose the circumstances under which it may restrict content or user accounts.
Elements:
1. Does the company clearly disclose what types of content or activities it does not permit?
2. Does the company clearly disclose why it may restrict a user's account?
3. Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?
4. Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?
5. Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?
6. Does the company clearly disclose its process for enforcing its rules?
7. Does the company provide clear examples to help the user understand what the rules are and how they are enforced?

P3. Collection of user information
The company should clearly disclose what user information it collects and how.
Elements:
1. Does the company clearly disclose what types of user information it collects?
2. For each type of user information the company collects, does the company clearly disclose how it collects that user information?
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?

P4. Sharing of user information
The company should clearly disclose what user information it shares and with whom.
Elements:
1. For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
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?
3. Does the company clearly disclose that it may share user information with government(s) or legal authorities?
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 and sharing user information
The company should clearly disclose why it collects and shares user information.
Elements:
1. For each type of user information the company collects, does the company clearly disclose its purpose for collection?
2. Does the company clearly disclose whether it combines user information from various company services and if so, why?
3. For each type of user information the company shares, does the company clearly disclose its purpose for sharing?
4. Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected?

On the privacy indicators, the research though it was important to look for disclosures on the security measures taken to protect the personal data of their users: this corresponds to the P13 indicator:

P13. Security oversight
The company should clearly disclose information about its institutional processes to ensure the security of its products and services.
Elements:
1. Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information?
2. Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services?
3. Does the company clearly disclose that it commissions third-party security audits on its products and services?

The analysis of the practices and public policies of the companies allowed us to highlight certain shortcomings and flaws.

3. We also took into consideration the legal and regulatory environment of the countries where the two companies respectively operate. Indeed,

according to the UNGP, which underpin the RDR methodology, States have the responsibility to protect human rights against violations committed by third parties, including business. States can do so by establishing appropriate legal and regulatory frameworks.The absence of relevant regulatory framework, and weak public policies of companies on freedom of expression and privacy make serious violations possible.

4. It is the possibility that violations of freedom of expression and privacy occur that the research team studied fourthly: What is the impact of the non-publication of information relating to privacy and the freedom of expression by Internet intermediaries? What are the consequences for users to have his/her personal data accessed by third parties, without his/her consent?

PRESENTATION OF COMPANIES

Name: Orange Senegal or Sonatel

Sonatel is the historic operator of Senegal. It is now the name of the a group, composed of Orange Senegal (Sonatel), Orange Mali, Orange Guinea, and Orange Ginea Bissau.

Shareholders: State of Senegal (27%) - Orange Group (42%) - Private shareholders

CEO: Alioune Ndiaye

Chairman of the Board: Bruno Mettling, CEO Orange Middle East Africa

Market share: Leader of the mobile phone market with 58% shares; Leader of mobile internet with 80% shares[19].

Name: Safaricom Limited

Shareholders: State of Kenya (35%) - Vodacom, a subsidiary of Vodafone Group (35%) - Vodafone (5%)

CEO: Robert Collymore

Market share: 69% of the mobile market in Kenya as of January 20, 2017[20]

[19]Sonatel's press release on ARTP's quarterly analysis report on the telecommunications market http://www.sonatel.com/rapport-d-analyse-trimestriel-de-l-artp-sur-le-marche-des-telecommunications/

[20]Kenya: Safaricom Market Share Increases To Nearly 70%https://www.african-markets.com/en/stock-markets/nse/kenya-safaricom-market-share-increases-to-nearly-70

1. Terms of use of Orange Senegal and Safaricom

1.1 Unpublished and unclear terms of use of Orange Senegal (Sonatel) and Safaricom's prepaid services

1.1.1 Inaccessibility of the terms and conditions of Orange Senegal's prepaid services

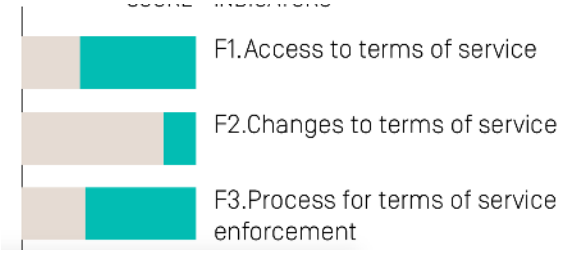
The terms and conditions are important documents in the relationship between a user of mobile services and an operator. They represent the contract between these two parties. It allows the customer to know what she/he is entitled to on the operator's network, and allows the latter to explain what circumstances could lead to a suspension of service, or suppression of a content published by the user. In case of dispute, this document shall prevail. That is why it must be accessible to the customer, but also to the future customer, who will thus get a clear idea of the operator's policies before she/he subscribes to services.

The availability of the terms of use is the first element analyzed in the RDR methodology. It is on the basis of this document that the effectiveness of the policy to respond to Internet shutdown requests, or any other form of censorship, can be gauged.

We first investigated whether Orange Senegal met the requirements of the F1 indicator on the accessibility of its terms of use.
It is clear from our analysis that the terms of use of prepaid mobile services are not available on the website www.orange.sn or on www.sonatel.com, the website of the group.

A lack of transparency in sharp contrast with the practices of Orange in France.

In the 2017 corporate accountability index, Orange France secured 67% of credits allocated for indicator F1:



Source : Corporate Accountability Index 2017

The only terms of use available on www.orange.sn are those of Orange Money, the money transfer and mobile payment service, and flagship of Orange Group, which has hit in 2017 30 million users in Africa[21].

This lack of availability and accessibility of terms and conditions of Orange Senegal's prepaid services is contrary to the UNGPs, especially principle 15, which provides that:

"In order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes appropriate to their size and circumstances"

And principle n°21 which provides that:

"In order to account for how they address their human rights impacts, business enterprises should be prepared to communicate this externally, particularly when concerns are raised by or on behalf of affected stakeholders.

[21]Orange Group, financial information for the first quarter of 2017, see p. 2 "In Africa, Orange Money crossed this quarter 30 million customers, growing by 74% over one year."https://www.orange.com/fr/content/download/42362/1298551/version/2/file/CP_Orange_Q1_2017.pdf

Business enterprises whose operations or operating contexts pose risks of severe human rights impacts should report formally on how they address them."

The research team asked repeatedly Orange Senegal and Orange Group for clarifications on the publication of the conditions of service of Orange Senegal. To date, our requests remain unanswered.

Without any published terms of use, we could not continue the analysis of indicators F2, and F3.

Conclusion: The lack of publication of terms of use on Orange Senegal's website allows the research team to conclude that if the corporate accountability index were applied to the company, it is very likely that it would gain no credit for F1 and F2 indicators. This conclusion is particularly disturbing: indeed, risks for freedom of expression online are increasing in Senegal.

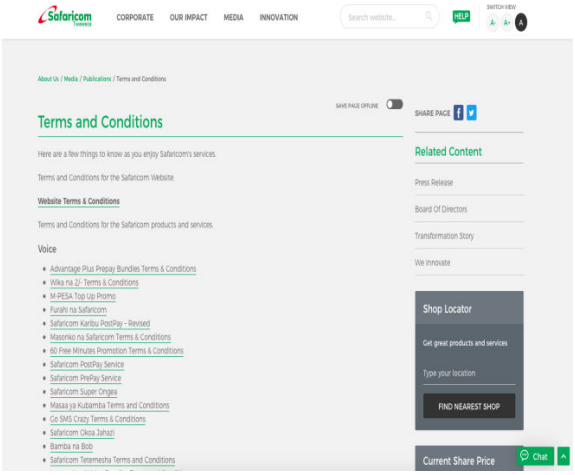
Recommendation: Orange Senegal should urgently publish the terms of use of its services to allow users to know their rights and duties when using the company's prepaid services.

1.1.2 Safaricom's vague terms of use

The research team looked primarily at whether terms and conditions of Safaricom's prepaid services were accessible on the website of the company, based on the analysis of F1 indicator.

The RDR methodology considers that for a company to get maximum credit for this indicator, the terms of use must be easily accessible on the website of the company, within two clicks away from the homepage. They should be available in all languages commonly spoken in the country of operation. Finally, the conditions must be accessible to the understanding of the general public, that is to say that the words used must be clear, the technical expressions explained, including through examples; the font size, the existence of a plan are also part of the body of evidence for determining the accessibility of terms of use.

Safaricom's terms of use are easy to identify on the website, on the homepage, at the bottom left. They are organized by type of service: Voice, SMS, Internet, prepaid or postpaid, Mpesa, the mobile money service, etc. This organization, which is reminiscent of the architecture adopted on the Vodafone UK site[22], Guides the user.



Source: Terms of use of Safaricom services (last visited on January 12, 2018)

The terms of use start with a definition of important terms and expressions used by the company[23]: for instance, the user is informed that the term "Network" means *"the mobile cellular network operated by [Safaricom] and covering those areas as*

[22]See http://www.vodafone.co.uk/terms-and-conditions/index.htm

[23]Terms of use of Safaricom's prepaid serviceshttps://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

stipulated by us from time to time";
These are good points for the company.

However, the terms and conditions are not available in Swahili, the other official language of Kenya.The Safaricom public policy team, whom the research team met, argued that good standard Swahili is harder to decipher for an ordinary person, than English. They added that someone who cannot read simple instructions in English would find it harder to read those same instructions in Swahili. The company ended by explaining that for personalized services, like the e-service on mobile phones, gives users the option to transact in either English or Swahili.

A thorough reading of prepaid terms of use highlights a lack of precision, which could cause harm to the user.
Contrary to the requirements of indicator F2, the company did not specify how it notifies users of changes to its terms of use, and in what period of time the notification is made:

section 7, paragraph b:

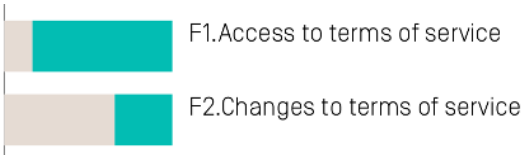
"We may make changes to these Conditions of Use from time to time and/or introduce new terms from time to time if there are changes to the law or to the terms of our telecommunications licence"

Another concerning inaccuracy lies in the fact that definition of words and phrases by the company is sometimes vague or incomplete. For instance, the network definition, mentioned above, uses the expression "from time to time", which doesn't give much information to the users. More preoccupying, in section 2, "Services", provides that Safaricom *"can to [its] discretion and without notice, discontinue the provision of the service or any part thereof without incurring any liability to [the user]"*. In section 5 "Suspension and disconnection of services," the company informs the user that it may:

"(a) suspend (bar), restrict or terminate the provision of the Services (in whole or in part) without informing [the user] and without any liability whatsoever (although, we will, where possible, try to inform [the user] that such action is or may be taken) under the following circumstances:
(...)
iv. If we believe you are making calls or sending data which is classified in our sole opinion as being illegal, a nuisance, abusive, a hoax, menacing or indecent (including any calls or messages relayed to our customer service operators);
(...)
viii. For reasons beyond our control.

The circumstances listed above are problematic for several reasons:
- They allow the operator to decide unilaterally to discontinue service to subscribers, without providing any explanation;
- They give no details to the user on the internal procedures in place to decide on a suspension of mobile services. The UNGPs encourages companies to establish *"A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;"* (Principle No. 15 b);
- These terms of use do not provide remedy mechanisms in case of violation of the freedom of expression of users; in case of content suppression or suspension of service. However the UNGP No. 22 encourages companies to *"provide for or cooperate in their remediation through legitimate processes."*

Conclusion: In view of this analysis, we believe that if the corporate accountability index were applied to Safaricom, for F1 indicator, the company would lose points on the accessibility of the terms of use in the language commonly spoken by users, and gain in the availability and the good location of the terms of use on the website. In addition, the company would not have obtained credit on indicator F2, given the lack of precision on the user notification process on changes to its terms of use.
For the F1 indicator, Vodafone, Safaricom shareholder, received 83% of credit:



Source : Corporate Accountability index 2017

Recommendation: Safaricom should translate its terms of use in Swahili, the other language commonly spoken in Kenya. In addition, the company should explain precisely how it notifies the user of changes in terms of use. Finally, Safaricom should be more precise about the procedures that allows it to enforce its terms of use: how the company decides to suspend the service to one or more users, on what legal basis, etc.

1.2 Consequences of lacking or unclear terms of use

An unpublished or unclear contract, has consequences for the user.

Initially, this research aimed to highlight the possible use by Orange Sénégal and Safaricom of network discrimination: in contradiction with the net neutrality
principle, this practice allows ISPs to prioritize certain contents, through free offers, like Facebook's free basics[24], or by transmitting certain contents with faster Internet speed.

It seemed relevant to focus on the growing phenomenon of Internet shutdowns, for several reasons. Indeed, at the time of publication of this study, nor Safaricom in Kenya or Orange in Senegal proposed prioritized content. Moreover, while the issue of net neutrality should be addressed on the continent, we cannot ignore the other worrying trend, which has developed considerably over the past two years. Internet shutdowns threaten the very idea of being able to enjoy rights and freedoms on the Internet, in particular freedom of expression, and they reveal the role of Internet service providers: as operator of the network, they are the first asked by governments to shutdown access to Internet.

Given this situation, the 2017 corporate accountability index of companies included a new indicator:
Internet Shutdowns.

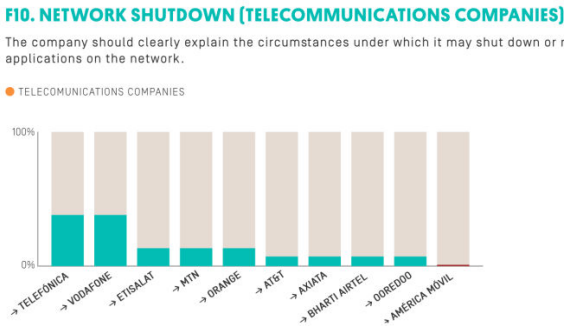
F10. Network shutdown (telecommunications companies)

The company should clearly explain the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.
Elements:
1. Does the company clearly explain the reason(s) why it may shut down service to a particular area or group of users?
2. Does the company clearly explain 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?
3. Does the company clearly explain its process for responding to requests to shut down a network or restrict access to a service?
4. Does the company commit to push back on requests to shut down a network or restrict access to a service?
5. Does the company clearly disclose that it notifies users directly when it shuts down the network or restricts access to a service?
6. Does the company list the number of network shutdown requests it receives?
7. Does the company clearly identify the specific

[24]Free basics in real life: Six case Studies on Facebook's Internet "on ramp" initiative, from Africa, Asia and Latin America - July 27, 2017 https://advox.globalvoices.org/wp-content/uploads/2017/07/FreeBasicsinRealLife_FINALJul27.pdf

legal authority that makes the request?
8. Does the company list the number of requests with which it complied?

No company in 2017 received enough credit on this indicator. Vodafone received 38% of and Orange 13%:



Source : Corporate Accountability Index 2017

Given the weak policies of parent companies on the prevention of Internet shutdowns, the research team analyzed the behavior of the African subsidiaries. In this research, we concluded that Orange Senegal's terms of use are not published on the company's website, and that Safaricom's lack precision.

In the following paragraphs, we will analyze the impact of these deficiencies on user's online freedom of expression, and we will question the robustness of terms and conditions of both companies in the event of Internet shutdowns demands from authorities.

1.2.1 Freedom of expression online weakened in Senegal

The UN guiding principles, which guide the standards applied by the corporate accountability index, target companies but also the States. The first principles are directed to the latter, the first part of the document being entitled *"The State duty to protect protect human rights"*.
States must protect human rights by putting in place the necessary legislative framework, and by avoiding infringing human rights guaranteed in international law. In the absence of state protection of human rights, companies can hide behind the lack of national protection legislation, to justify the violation of the UNGPs. This justification paves the way for abuses[25].

In Senegal, national law enshrines unequivocally and repeatedly freedom of expression: Article 8 of the Constitution of 22 January 2001 enshrines freedom of expression as a fundamental right of every citizen[26].
Senegal is a signatory of many international texts protecting this right, including the Universal Declaration of Human Rights and the Covenant on Civil and Political Rights. Article 19 of the Universal Declaration of Human Rights states that *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."*

Furthermore, Article 19 of the International Covenant on Civil and Political Rights 1966 (ICCPR) imposes legal obligations on States parties and reaffirms among others the

[25]In response to a request for explanation from civil society organizations, including Internet Without Borders and Access now, Orange, parent company of Orange Cameroon, explained that its subsidiary obeyed the national legislation to justify 94 days of Internet shutdown in Cameroon:https://www.business-humanrights.org/en/oranges-response

[26]Constitution of Senegal http://mjp.univ-perp.fr/constit/sn2001.htm

importance of freedom of expression in terms very similar to those of the UDHR:

"1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[27]*"*

The Telecommunications Code of Senegal, adopted in 2011, provides that operators and ISPs must *"respect the international conventions and agreements on telecommunications and ICTs, including conventions and agreements to which Senegal adheres."*
Based on this provision, regardless of the telecommunications service provided, the licensee must respect the international commitments of Senegal, in ICT, in particular Article 33 of the Constitution of the International Telecommunication Union, which protects the right to correspond with international public correspondence service. This important legislative provision, seems to anticipate the resolution A/HRC/32/L.20 of the UN Human Rights Council, adopted unanimously on 1st July 2017, which affirms that "*the same rights that people have offline must also be protected online*"[28]. Thus freedom of expression is the same offline and online.

Despite this strong proclamation in the Senegalese legal corpus, several Human Rights organizations call for vigilance in the light of some recent events in the country.

Like many countries of the Economic Community of West African States (ECOWAS), Senegal has increased its vigilance against potential terrorist attacks; this necessity, given the numerous attacks in neighboring Mali, raises questions about the potential effects on freedoms.

In its 2016-2017 report on Senegal, Amnesty International[29] refers to the adoption of the Law No. 2016-29 of November 8, 2016[30], which amends the Criminal Code to include in its Chapter III a vague definition of terrorism. According to this definition, *"offenses related to information and communications technology"* are treated as acts of terrorism. Title IV of the Law gives a definition of "ICT-related offenses": the production and delivery of "immoral" content on the Internet is now considered as a misdemeanor.

FOCUS: Morality and image of the president as limits to freedom of expression in Senegal

Recent events have highlighted limitations to online freedom of expression, and demonstrate a weakening of the latter. While Orange Senegal hasn't played any role in none of the three cases mentioned, the ISP could see these examples as additional items for a self assessment of the robustness of its content

[27]The text of the law can be accessed here: Journal Officiel n°6576 du Lundi 14 mars 2011 http://www.jo.gouv.sn/spip.php?article8858

[28] Download the full text of the resolution here https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20

[29]https://www.amnesty.org/en/countries/africa/senegal/report-senegal/

[30]Text of the law can be accessed here: Journal Officiel du Sénégal du 25 Novembre 2016 http://www.jo.gouv.sn/spip.php?article11003

policy, and measure the consequences of not publishing its terms of use.

In June 2016, Senegalese rapper Major Déesse was arrested[31] following a complaint from the Committee for the Defense of moral values: she was accused of having published, on the social network Snapchat, a video in which she allegedly damaged the "moral and religious values" of Senegal. The case was later on dropped.
The image of President Macky Sall is another limit to freedom of expression online: in May 2017, four young people were taken to court[32], accused of insulting the President of the Republic, for sharing in a group Whatsapp a montage featuring the head of state. On 3 August 2017, a famous Senegalese singer was arrested[33], for "insulting the head of state and spreading fake news": she shared video in a Whatsapp. group, in which she criticizes the President. Following her arrest, the prosecutor warned the "bad people who use social networks (...) to broadcast obscene, offensive and even ethnic images"[34].

Conclusion: Despite a protective legal environment, many fear that the new terrorism laws could threaten online freedom of expression. In particular, the vagueness of the legal definitions of offenses related to the use of ICT, coupled with the lack of transparency of Orange Senegal on the terms of use of its services give no guarantee that in case of a censorship request, from the authorities, or request of Internet shutdown, the ISP will be able to respond to them, while preserving its user's rights[35].

Recommendation: It is urgent for Orange Senegal to demonstrate greater transparency on the terms of use of its services: in particular, the ISP should specify the internal procedure that could lead Internet service suspension on request of the government, and how the company would assess the legality of the received censorship order, its proportionality, that it emanates from a judicial authority, and is necessary to the legitimate aim pursued.

1.2.2 Possibility of an Internet shutdown in Kenya

Kenya has a legal framework to protect human rights, in respect of the first pillar of the UNGPs on the duty to protect. The 2010 Kenyan Constitution affirms in Article 2, paragraphs 5 and 6 that international law is an integral part of national law. Section 33 of the Supreme text enshrines freedom of expression. Limitations to the rights and freedoms enshrined in the Constitution are detailed: according to Article 24 these limitations must be prescribed by law, and must be *"reasonable and justifiable in an open and democratic society based on human dignity , equality and freedom, taking into account all relevant factors. "* Finally, such limitations must be authorized by a judicial authority, court or tribunal.

Despite these safeguards, voices expressed fears of an Internet shutdown, especially as the

[31]Senegal: Singer arrested for indecencyhttp://freemuse.org/archives/12283

[32]Senegal Charges 4 over Doctored Whatsapp Photo of Senegalese President Macky Sall http://www.ndtv.com/world-news/senegal-charges-4-over-doctored-whatsapp-photo-of-senagalese-president-macky-sall-1707537

[33] Senegalese Singer Arrested for Criticizing President Sall http://punchng.com/senegalese-singer-arrested-for-criticising-president-sall/

[34]These remarks remind of the justification given by the Cameroonian government in January 2017, a few days before Internet shutdown in the anglophone regions of Cameroon.

[35]See for instance the ten principles on necessity and proportionality, which provide means to verify the legality of demands received https://necessaryandproportionate.org/fr/about

August 8, 2017 general elections approached[36], in the light of observed erosion of freedom of expression online in recent years[37], and the increased number of Internet shutdowns during elections on the African continent.

Internet shutdowns have generally been justified by the necessity to protect public order.

In addition to the existing legal framework, companies must also adopt mechanisms to respect human rights while doing business. If the Kenyan leading operator, Safaricom, had robust terms of use, which guaranteed continuity in access to Internet, the ISP could better respond to any demand of Internet censorship.

In the case of Safaricom, the vagueness of the terms of use, as demonstrated above, leave little guarantees to the user that the company has put everything in place to respond effectively to any censorship orders. Moreover, Safaricom's terms of use do not require that the company provides information to its users in case of unavailability of its services.

In a report published on October 29, 2017, analysis conducted by the Center for Intellectual Property and Information Technology Law at the University of Strathmore in Kenya suggest the possibility that Safaricom may have quietly throttled the speed of its network during the repeat presidential election. of October 26, 2017. The Center calls for further transparency from the operator[38].

In April 2017, the operator faced an Internet shutdown, which remains unexplained today.

FOCUS: The partially unexplained disruption of Safaricom network

On April 24, 2017, many users of the Safaricom network expressed their difficulty in making phone calls, texting, or to connect to the Internet[39]. In a brief statement[40], the operator explained that it had identified the cause of the failure, and assured its users that everything was done to restore connectivity. Given the little information provided, the regulatory authority urged Safaricom to provide detailed explanations of what had happened[41].
To date, we have no knowledge of such document issued by the Kenyan operator.

Conclusion: Despite the existence of a protective environment for online freedom of expression of Kenyan citizens, concerns remain about the likelihood of an Internet shutdown in Kenya, particularly on the response that Safaricom could oppose if it received such request from the Kenyan authorities. The terms of use of the Kenyan operator lack precision on the reception and treatment of shutdown orders and any other form of censorship.

Recommendation: Internet Without Borders

[36]Kenyans Fear a Possible Internet Shutdown during 2017 Presidential Election https://advox.globalvoices.org/2017/01/12/kenyans-fear-a-possible-internet-shutdown-during-2017-presidential-election/

[37]See Freedom House 2017 report on Kenyahttps://freedomhouse.org/report/freedom-net/2016/kenya

[38] Internet Speed Throttling Surrounding Repeat Election? http://blog.cipit.org/2017/10/29/internet-speed-throttling-surrounding-repeat-election/

[39]Safaricom experience countrywide network outage https://www.standardmedia.co.ke/business/article/2001237498/safaricom-experiences-countrywide-network-outage

[40]Statement by Safaricom CEO Bob Collymore on Network outage http://smedigest.co.ke/statement-safaricom-ceo-bob-collymore-network-outage/

[41]Communication Authority gives Safaricom 7 days to explain outage http://www.capitalfm.co.ke/business/2017/04/ca-gives-safaricom-7-days-to-explain-outage/

encourages Safaricom to propose new conditions for the use of its services, which are more accurate, which detail the procedure for processing censorship requests, and puts in place remedy mechanisms, in case of violation of users' rights. This will help the operator, pursuant to the principles outlined in the second pillar of UNGPs, respect the freedom of expression of its millions of users.

FOCUS: The risks associated with the SIM card registration in Senegal and Kenya

In Senegal and Kenya, operators are under a legal obligation to register their subscribers. This means that any user must provide an official ID to be able to subscribe to the operator's services.In Senegal, it is by virtue of Decree No. 2007-937 of 7 August 2007 that operatorsneed to register subscribers.
In Kenya, Article 5 of the Kenya Information and Communication Act (Registration of Subscribers of Telecommunications Services) 2014 details the information that must be collected from the user.Other countries in Sub saharan Africa, such as Madagascar, Uganda, Cameroon, Nigeria, and Gabon, impose the same obligation in the name of the fight against terrorism, or protection of public order.

For RDR methodology, the requirement to provide proof of identity undermines freedom of expression: "The use of a real name online, or requiring users to provide a company with identifying information, provides a link between online activities and a specific person. This presents human rights risks to those who, for example, voice opinions that don't align with a government's views or who engage in activism that a government does not permit. (…)[42]». In addition to this risk, Internet Without Borders raises concerns about privacy, in the sub saharan Africa context. A growing number of governments use databases of telcos to send unsolicited SMS to subscribers: in Kenya, for example, many users have complained of receiving unsolicited messages from politicians[43]. It was the same in Cameroon, where in January 2017, the government used the network operators to send SMS reminding the risk of spreading false information on the Internet[44].How and where are stored the information collected during the registration of SIM cards? Do privacy protection bodies have a say on this collection of user information? Are these files shared with authorities, and if so, under what conditions?**So many questions to be answered by a corporate accountability index specific to telecommunications operators in sub saharan Africa.**

2. Privacy policies of Orange Senegal and Safaricom

The digital age is also the age of data, including users' personal data. They are a significant part of the business model of many companies.

In its methodology, Ranking Digital Rights uses the term "user information: *"any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques."*.

The research team adopts this definition for the purposes of this study.

ISPs must be transparent about the data they collect on their users, if and how third parties can access them: this is required by the fact that they hold sensitive information about their users, and the security threat is increasing.

According to the RDR methodology, it is through the publication of privacy policies that companies demonstrate that they implement

[42]See indicator F11 of the RDR methodology, p. 26 https://rankingdigitalrights.org/wp-content/uploads/2016/09/2017Indexmethodology.pdf

[43]These complaints surfaced during a meeting organized by the Kenyan organisation « Kictanet » and IAWRT, between Safaricom and consumer, users' rights associations.

[44]Regional Internet Blackout in Cameroon https://internetwithoutborders.org/fr/regional-internet-blackout-in-cameroon/

concrete measures for the respect of the right to privacy of their users, as enshrined in the universal Declaration of human rights, the International Covenant on civil and political rights and other international human rights instruments.

In the following paragraphs, we will see that neither Orange Senegal nor Safaricom publish adequate privacy policies. These deficiencies have serious consequences for the privacy of their users.

2.1 The lack of publication of Orange Senegal and Safaricom's privacy policies

2.1.1 Lack of access to Orange's privacy policies Senegal

The P1 indicator of RDR methodology focuses on the availability and accessibility of company privacy policies: the duty to inform users on a company's privacy policies is a prerequisite required by international instruments and is often transposed in national law: in fact, the user must consent to the collection of personal data. This consent is informed only if the user has received clear information on the data collection.

Senegal adopted in 2008 a law on the protection of personal data[45]. Article 37 provides that *"The principle of transparency implies a mandatory information from the personal data collecting agent."*

Yet, despite this clear legislation, the Privacy Policy related to the use of the Orange Senegal's service is not available on the website.

Orange Légal

Catalogue d'interconnexion

Cliquez ici pour télécharger le catalogue d'interconnexion approuvé Sonatel 2016

Couverture réseau

Cliquez ici pour accéder à la couverture réseau 2G, 3G, ADSL, CDMA & EVDP

Mentions légales

Cliquez ici pour lire les mentions légales

Conseils d'utilisation des terminaux mobiles

Cliquez ici pour retrouver tous nos conseils

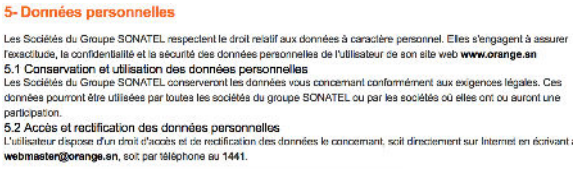
Conditions générales d'utilisation Orange Money

Cliquez ici pour retrouver les conditions d'utilisation

Source: https://www.orange.sn/2/particuliers/1/3/orange-legal-285.html

(page visited on July 15, 2017)

The research team went through www.orange.sn site, and could only identify the privacy policy related to the use of the website, in the "Orange Legal" section.



5- Données personnelles

Les Sociétés du Groupe SONATEL respectent le droit relatif aux données à caractère personnel. Elles s'engagent à assurer l'exactitude, la confidentialité et la sécurité des données personnelles de l'utilisateur de son site web **www.orange.sn**

5.1 Conservation et utilisation des données personnelles

Les Sociétés du Groupe SONATEL conserveront les données vous concernant conformément aux exigences légales. Ces données pourront être utilisées par toutes les sociétés du groupe SONATEL ou par les sociétés où elles ont ou auront une participation.

5.2 Accès et rectification des données personnelles

L'utilisateur dispose d'un droit d'accès et de rectification des données le concernant, soit directement sur Internet en écrivant à **webmaster@orange.sn**, soit par téléphone au **1441**.

The existence of this specific privacy policy for the use of the company's website would not help Orange Senegal obtain credit for the P1 indicator. Furthermore, the company provides no information in Wolof.

Following investigations by Internet Without Borders and its partner in Dakar, the research team notes that no document entitled privacy policy is given to the user at the time of the activation of a SIM card, or the opening of a Mobile Money account.

It is therefore impossible to verify which data are collected, with whom they are shared, and whether all safety measures are taken to ensure that such data is protected from any

[45]Text of the law can be accessed here http://www.wipo.int/wipolex/fr/text.jsp?file_id=181186

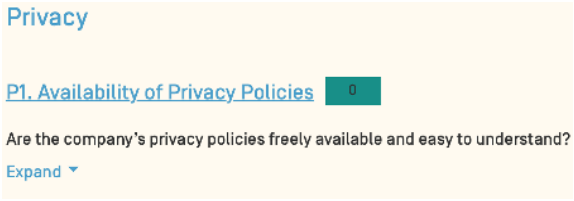
malicious third party.

On the security issue, which is assessed thanks to indicator P13, the only information released by the operator is in the code of ethics of Sonatel[46], which applies to all companies that make up the group: Orange Senegal (Sonatel), Orange Mali, Orange Guinea and Orange Guinea Bissau. It simply provides that: "Each director or employee shall ensure compliance with the legal obligation of Sonatel to protect personal data it collects from its customers, its suppliers and its employees. This data must be protected against any form of disclosure or unauthorized use. "

The group does not specify the existence of regular audits to verify the robustness of the safety systems, or that it has set up a control mechanism of employee access to users' data.

This failure to publish privacy policies contrasts with the behavior of Orange in France.

The case of the latter on the issue of user privacy is interesting and demonstrates the importance of vigilance tools like the corporate accountability index: in 2015, when the first index was launched, Orange received no credit on the publication of its Privacy policies:



Source : Orange France in 2015 https://rankingdigitalrights.org/index2015/companies/orange/

In 2017, Orange received 100% of credits for the same indicator: in fact, the company now devotes an entire section of its website to personal data. The company provides a video in which it explains how it collects and uses data collected on users[47]. Orange also gives advice on how users can better protect their data online:

Source : www.orange.fr

In addition, on the homepage of its site, the user can click on a tab named "Personal Data", which gives access to the Orange's personal data Charter, in which the company commits *"as part of its activities and according to the laws in France and Europe, to ensure the protection, confidentiality and security of personal data of users of its services, and to respect their privacy. "*

There is a **clear contrast between the transparency of Orange France and Orange Senegal** on the collection and sharing of information about users: in France, Orange is committed to compliance with French and European obligations. In Senegal, despite the obligations imposed by national law, despite the commitments of the Orange Group on privacy, as a member of the Telecom Industry Dialogue and the Global Network Initiative, Orange Senegal does not publish its privacy policy.

Conclusion: If corporate accountability index were applied to Orange Senegal, the company would have received no credit for the P1

[46]Charte de déontologie http://www.sonatel.com/Charte-de-deontologie-Sonatel-2016.pdf

[47]Personal data : How are they used ? (Vidéo by Orange) https://bienvivreledigital.orange.fr/actu/video%20privacy

indicator on the accessibility of its privacy policy. The company does not meet expected standards under international law, in particular the UNGPs; In addition, Orange Senegal violates Senegalese law.

Recommendation: Orange Senegal should publish its privacy policies for all its services, in French and Wolof. It should specify what information it collects from users, for what purpose, third parties who have access to the data collected, especially shed light on the security measures taken to protect the information collected.

FOCUS: Senegal's Personal Data Commission (CDP), a regulator with little resources

The Personal Data Commission (CDP) was established in 2008 by Law No. 2008/12 on the protection of personal data. The CDP is composed of 11 members. The President of the Republic appoints the President of the Commission (Article 7). CDP ensures that the obligations on personal data processing are met: in particular the CDP verifies that an entity or person, which practices data collection, has requested the consent, and informed users on the collection, the purpose of the collection, and whether all necessary measures are taken to protect the data collected. In an interview, the new President of the CDP, Awa Ndiaye, acknowledges that her administrative authority has **insufficient means compared to the importance of its mission.** This greatly hinders action, she adds[48]. For example, the CDP has not yet started verifications on the ground, to make sure that all companies respect the law on personal data. A control *a posteriori* would allow the CDP to see that the obligation to inform the person of the collection and processing of his/her data is not respected by Orange Senegal (Sonatel).

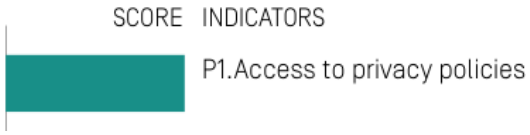
The low number of sanctions against Sonatelshould also be noted. The latest sanction against the operator seems to date back to April 30, 2014[49]. In addition, during a visit to Sonatel, the President of the CDP congratulated Sonatel, speaking of a *"business attached to the respect of standards, especially those concerning the protection of personal data of its customers"*[50]. Asked about these points by the research team, a representative of the CDP explained the scarcity of decisions against Sonatel by the little number of complaintsreceived from users.

2.1.2 Safaricom's concise privacy policy

In Eastern Africa, Safaricom, a subsidiary of Vodafone, performs a little bit better than Orange in Senegal on the P1 indicator, related to the accessibility of privacy policies.

Safaricom does not have a specific document entitled Privacy Policy.

Vodafone, one of Safaricom shareholders, received in 2017 100% credit for this indicator, just like in 2015:



Source: https://rankingdigitalrights.org/index2017/companies/vodafone/

In an interview with our research team, Safaricom explained the the lack of a specific document on privacy policy by the inexistence of a law on personal data protection in Kenya.

[48]Mrs Awa Ndiaye : "Everything must also be done in the near future so that the *a posteriori* control can be carried out" - IT Mag http://www.itmag.sn/focus/mme-awa-ndiaye-presidente-de-la-commission-de-protection-des-donnees-personnelles-il-faut-faire-egalement-dans-un-avenir-proche-pour-que-le-controle-a-posteriori-puisse-se-faire/

[49]CDP - Deliberation No. 2014-017 of 30 April 2014 calling SONATEL for breach of the provisions of the legislation on personal data, relating to direct prospectinghttp://cdp.sn/sites/default/files/CDP-Mise%20en%20demeure_Sonatel.pdf

[50]Press release: CDP visits Sonatel http://www.sonatel.com/visite-de-la-commission-de-protection-des-donnees-personnelles-cdp-a-sonatel/

The company added that this does not prevent Safaricom from caring about protection of users' personal data: it argued that it focuses more on *"the implementation of its privacy policy"*. Safaricom's 2016 annual report seems to back up this claim: in the Risk Management section of the report, the company explains how it prevents and mitigates privacy related risks[51]. But this document is primarily intended for investors.Safaricom assured that it will work in the future to make its privacy policy more easily accessible by users.

The research team has identified information on Safaricom's personal data policy. The terms of use of prepaid services, paragraph 2.g. provide that the user agrees that:

"We may disclose and/or receive and/or record any details of your use of the Services including but not limited to your calls, emails, SMS's, data, your personal information or documents obtained from you for the purposes below:
i. Fraud prevention and law enforcement;
ii. For reasonable commercial purposes connected to your use of the mobile service, such as marketing and research related activities;
iii. Use in our telephone directory enquiry service in printed or electronic format;
iv. To comply with any legal, governmental or regulatory requirement;
v. For use by our lawyers in connection with any legal proceedings;
vi. In business practices including but not limited to quality control, training and ensuring effective systems operation."

According to these terms, Safaricom collects user data in the circumstances listed above. These seem limited, but facing the generality of the terms used, the user is not able to understand precisely which data is collected, by what means, whom they are or could be shared with. In addition, the purpose of the collection is vague. For example, Safaricom says that data can be collected *"For reasonable commercial purposes connected to your use of the mobile service, such as marketing and research related activities"*, which suggests that other commercial purposes, which are not mentioned, could justify the collection of data. In another example, the user is informed that he/she accepts that his/her data can be collected, shared, according to a legal requirement, governmental or regulatory. Here again, the terms are vague and unclear: the company does not specify under what law it may have to undertake the collection, data sharing, or recording of the activity of its users.

This lack of transparency can be detrimental to users' privacy.

Safaricom should specifically explain to users that, notwithstanding the prohibition in principle to monitor and disclose user data imposed by Article 15 of the Kenya Information And Communications Act (Consumer Protection Regulations, 2010)[52], it may be required to do so by the law: in its submission on Kenya to the

[51]See 2016 annual report p. 50https://www.safaricom.co.ke/images/Downloads/Resources_Downloads/Safaricom_Limited_2016_Annual_Report.pdf

[52]Read the Act here http://admin.theiguides.org/Media/Documents/Kenya%20Information%20Communications%20Act.pdf

Human Rights Council in 2014[53], NGO Privacy International identified that Article 13 of the 2014 act on registration of subscribers[54], amending Kenya Information and Communications Act, now requires telecommunications operators to provide access *"to its systems, premises, facilities, records, registers and other data"*, without mentioning the prior recourse to the authorization of a judicial authority, in accordance with international requirements. Safaricom does not specify the procedures in place to determine the legality of a request for access to user data, presented by the authorities.

Safaricom's subscriber registration form, available in English and Swahili on the website of the company, provides additional information on Safaricom's privacy policy, particularly on the content of some of the information collected from user. The latter is asked to provide name, sex, age, address, and an official ID:


INDIVIDUAL

SUBSCRIBER SIM REGISTRATION FORM

ONLINE FORM

FIRST NAME / JINA LA KWANZA:

MIDDLE NAME / JINA LA KATI:

LAST NAME / JINA LA MWISHO:

GENDER / JINSIA: Male / Mume ☐ Female / Mke ☐

DATE OF BIRTH / TARIKHE YA KUZALIWA: DD...../ MM...../ YY.....

NATIONALITY / URAIA: (KENYAN)..... OTHERS / WENGINE (SPECIFY COUNTRY / TAJA NCHI):

Identification type ..... (e.g. National ID, Alien ID, Military ID, Passport, Diplomatic ID)

Identification Number ..... (Give number of identification document used)

POSTAL ADDRESS / SANDUKU LA POSTA:

POSTAL CODE / KODI:

TOWN / CITY / MJI / JIJI:

PHYSICAL ADDRESS / ANUANI YA MAKAO:

LANDMARK / PAHALI KARIBU NA ANUANI YAKO PANAPO JULIKANA:

REGISTERED M-PESA CUSTOMER / MTEJA WA M-PESA: YES / NDIO ☐ NO / LA ☐

REQUIRE M-PESA REGISTRATION / UNATAKA KUSAJILI NA M-PESA: YES / NDIO ☐ NO / LA ☐

Source: https://www.safaricom.co.ke/personal/plans/getting-started/sim-registration

Safaricom seems to apply strictly the obligations imposed by the 2014 Act on registration of subscribers. The level of accuracy of the information collected bears the question of security. While the aforementioned 2014 act, requires operators to share information about the security measures taken to ensure the protection of these data, no obligation seems to exist on the obligation to inform users of these measures.

The research team lookedfor a document in which Safaricom explains security measures it takes, pursuant to P13 indicator of the RDR methodology. Again, the company provides this information to its investors, not directly to its users: in its 2016 annual report, a paragraph explains the security measures taken[55].

However, the right to privacy is fundamental to the exercise of other rights and freedoms: in its annual report on 22 May 2015 at the Human Rights Council, the Special Rapporteur on freedom of expression, reminds that *"privacy is a gateway to the enjoyment of other rights, particularly freedom of opinion and expression.[56]"*

Conclusion: In the terms of use of its services, Safaricom provides a paragraph on its personal data policy. The company does not have a specific document entitled privacy policy, which makes this difficult for users to access. The said privacy policy is not available in Swahili, does not specify exhaustively what information is

[53]The right to privacy in Kenya https://www.privacyinternational.org/sites/default/files/UPR%20Kenya.pdf

[54]The text of the Act can be accessed here http://kenyalaw.org/kl/index.php?id=4215

[55]See p. 50 of Safaricom's Annual report: *« Our ISO 27001 Information Security Management System certi cation is an independent confirmation to our customers that we have implemented appropriate processes and controls relating to our cloud services, billing and customer support services to protect the privacy of their information. In addition, we have expanded the scope to include mobile data and mobile money services. »*

[56]Read report here A/HRC/29/32 http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

collected about the user, or third parties who may have access to this data. Finally, the company gives no information on audits performed to ensure the security of the data collected. Safaricom explains the brevity of its privacy policy by the absence of specific domestic legislation on the protection of personal data. This justification is not enough, UNGPs require the companies to respect human rights, even in the absence of state protection. **If the corporate accountability index of companies were applied to Safaricom on the date of this study, the company would fall short of credit for indicators P1, P2, P3, P4, P5 and P13.**

Recommendation: Internet Without Borders encourages Safaricom to make available to its users a complete privacy policy, clear, and detailed on the data it collects, if and how access to data by third party or employees is controlled. Safaricom should also explain what measures are taken to ensure data security.

2.2 Impact on privacy

The non-publication of Orange Senegal's privacy policy, and the lack of clarity of Safaricom's, have direct effects on the privacy of their users. We will study some of them in the following paragraphs.

2.2.1 Orange Senegal's products, raise questions about the impact on privacy

As the leader of the local telecommunications market, Orange Senegal continues to develop and regularly announces new products and services. For each announcement, questions about the impact on privacy are expressed without ever really receiving adequate response, from the operator.

For instance, the announcement in December 2015 of Sonatel group's will to create a common operating center for Orange Group's subsidiaries in sub saharan Africa generated much debate. Named GNOC (Global network Operating Center), this project aims to pool the operation of networks and service platforms of Sonatel (i.e. Orange Senegal, Orange Mali, Orange Guinea, and Orange Guinea Bissau), Orange Cameroon, Orange Côte d'Ivoire, Orange Niger, and Orange DRC[57]. The implementation and management of the GNOC is outsourced to Chinese company Huawei[58].

Part of the discussion focused on how security of users' data would be maintained in this outsourcing operation.
In its 2nd quarterly review of 2015, the Personal Data Commission expressed concerns about the implications for privacy of Sonatel's outsourcing projects. The Commission wrote that:

"(...) technically, the practice of outsourcing remains a concern. This presents an additional challenge for data protection in the sense that the data controller no longer has full control of

[57]Orange announces a joint network operation center in Dakar as of 1 February 2016 (report in French) http://www.agenceecofin.com/infrastructures/1412-34540-orange-annonce-un-centre-commun-dexploitation-de-reseau-a-dakar-des-le-1er-fevrier-2016

[58]Huawei and Orange Inaugurate Global Network Operation Center (GNOC) in Dakar and Abidjan http://www.huawei.com/en/news/2016/11/Huawei-Orange-GNOC-Dakar-Abidjan

his information system. "

In November 2016, the GNOC was inaugurated in Dakar. In an interview with the research team, a representative of the CDP confirmed that the CDP was present at the inauguration, and trained agents of Sonatel. Despite laconic statements in the Senegalese press, Sonatel hasn't so far clearly responded to concerns about users' personal data security.

2.2.2 Privacy and gender based violence committed on Safaricom's network

In a report released in July 2014[59], the Kenyan chapter of the International Association of Women Journalists in Radio and Television (IAWRT), which collaborated to the drafting of this study, highlighted the increase in violence through the use of technologies, mostly against women. These attacks can be committed through various channels, including telecommunications network of operators such as Safaricom.

One of the identified cases is that of a young woman who was the subject of numerous death threats sent to her mobile phone by her former companion, including after changing the phone number. The assumption made by the entourage of the victim, and associations that supported her, is that the individual may have had access to her new number through a Mpesa reseller. Mpesa, the mobile money service, is the flagship of Safaricom. Registration is done upon activation of the SIM card: user is asked to provide personal information and official ID. In addition, each transaction made through the Mpesa service requires to enter the name, phone number, and provide proof of identity. Questioned by the research team, Safaricom affirmed its zero tolerance for illegal use of data of its users, but the company did not provide details on the internal procedure to control employee access to data.

This case is not isolated: according to a study conducted by IAWRT and the Web Foundation, 1 out of 5 Kenyan woman has already experienced harassment while using the Internet[60].

Internet service providers, including industry leader Safaricom, should take action against this scourge, and provide a privacy policy that addresses risks such as gender based violence.

3. Conclusion and recommendations

The purpose of this study was to examine the compliance with national legal obligations and international standards on privacy and online freedom of expression of Orange Senegal (Sonatel) and Safaricom, respectively subsidiary of Orange Group and Vodafone Group. To this purpose, we used the methodology of the Ranking Digital Rights project, and analyzed the terms of use and privacy policy of prepaid services of these two companies.

Our study demonstrates that Orange Senegal and Safaricom do not meet international standards, and even national ones, in the protection of freedom of expression online, and user privacy.

Orange Senegal, or Sonatel, does not publish on its website the terms of use of its prepaid services, and personal data policy. This practice

[59]End violence: Women's rights and safety online Technology-related violence against women in Kenya http://www.genderit.org/sites/default/upload/flow_research_report_kenya.pdf

[60]Women's Rights Online - Kenya Report card http://webfoundation.org/docs/2016/09/WF_GR_Kenya.pdf

is not only contrary to international standards, outlined in the UN guiding principles on business and human rights, but also to national law, including the law on the protection of personal data: indeed, the latter imposes to the operator a duty to inform its users' of the data collection.

While it is true that, contrary to Orange Senegal, Safaricom publishes conditions for its prepaid services, these are concise and do not accurately explain the circumstances under which the operator may have to suspend its service. We especially think of Internet shutdowns, or content removed from Safaricom network. Similarly, the operator's privacy policy is very basic, and provides very few details on the nature of the data collected, third parties who have access to this data, the security measures implemented by the operator to protect the data of its users.

These practices clearly contrast with those from their parent companies: Orange and Vodafone were both assessed in the 2017 corporate accountability index: they achieved encouraging scores on the publication of their terms of use and privacy policy.

These shortcomings have direct consequences on online freedom of expression and user privacy: in our study, we particularly refer to cases of harassment committed through fraudulent access to personal data of users of Safaricom.

In addition, our study proved that by not meeting International standards on freedom of expression and privacy, both companies remain fragile in case of illegal requests from authorities: we have shown in particular that neither operators details the internal processes in place to respond to any Internet shutdown request.

This is highly problematic, operators may find themselves accomplices of Internet shutdowns, a trend that has grown exponentially on the African continent in the recent years.

Finally, none of the operators provides remedy mechanisms, to mitigate violation of their users freedom of expression and privacy that they could cause, contrary to the guidelines of the UN Guiding Principles.

Our study demonstrates that the failures observed to date have not been subject of national sanctions: this can partly be explained by the lack of means of regulators regulators and the fact that very few users report bad practices of their operators.

For the research team, the corporate accountability index and its methodology, developed by the ranking digital rights project, represent responses to the concerns raised: if made available to both citizens and regulators, they give clear vision of international standards that should be met by operators to ensure respect and protection of human rights in the telecommunications sector. In addition, the corporate accountability index allows companies to visualize and identify the points on which they should focus their efforts to better respect human rights.

Recommendations:

For Civil Society

African and international civil society should urgently work on the adaptation of the corporate accountability index to companies operating in sub-Saharan Africa. This index should be adapted to the specific risks identified in this study: The index for Sub-Saharan Africa should take into account the weakness of legislative

and regulatory framework for digital rights protection; it should also examine the relationship between the companies and telecommunications regulatory authorities in each country, and question the consistency of practice in digital rights and symmetry of obligations between parent and subsidiary companies.

For telecommunications operators

Telecommunications operators should exercise greater transparency, including making public and accessible their terms of use and privacy policy.

For Governments

States should strengthen the national legal framework for the protection of human rights. In particular, they should include specific obligations for telecommunications operators. Finally, governments should give more resources and power to the telecommunications sector regulators.