



# RANKING DIGITAL RIGHTS

February 10, 2022

## **Input for OHCHR report on internet shutdowns and human rights to the fiftieth session of the Human Rights Council**

### **Introduction**

Ranking Digital Rights (RDR) welcomes this opportunity to provide input ahead of OHCHR’s forthcoming report on internet shutdowns and human rights. We work to promote freedom of expression and privacy on the internet by researching and analyzing how global information and communication companies’ business activities meet, or fail to meet, international human rights standards.<sup>1</sup> We focus on these two rights because they enable and facilitate the enjoyment of the full range of human rights comprising the Universal Declaration of Human Rights (UDHR), especially in the context of the internet.<sup>2</sup> Our work also evaluates good corporate governance of human rights risks at the structural level, highlighting the extent to which respect for human rights is embedded in companies’ operations and overarching business models.

Network shutdowns and their impact on human rights have been a central focus of the RDR methodology<sup>3</sup> since the inception of our program. Companies—particularly telecommunications companies—have a pivotal role to play in preventing shutdowns, but also in resisting them when they do occur, informing those affected, and mitigating their impact. However, as the most frequent recipients of shutdown orders, they have also become the key nodes in the process of imposing network disruptions. This transforms the stewards of billions of people’s communication channels into conduits for government repression. Regrettably, our research shows that, far too often, companies embrace this role unquestioningly, exercise a policy of silent compliance, and fail to report on any aspect of their involvement.

In a network shutdown, the mass violation of freedom of expression and information is typically only the first in a cascade of human rights harms that follow. The danger of these disruptions lies not only in the direct harms they inflict upon individuals, communities, and economies, but in the ripple effects they cause, many of which are hidden or unreported. People are rendered

---

<sup>1</sup> See <https://www.rankingdigitalrights.org> for more details.

<sup>2</sup> United Nations. Universal Declaration of Human Rights (1948), <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

<sup>3</sup> Ranking Digital Rights. *2020 indicators* (2019), <https://rankingdigitalrights.org/2020-indicators/>

unable to communicate with loved ones, obtain vital news and health information,<sup>4</sup> or call for help in emergencies, putting their right to life in peril.<sup>5</sup> Shutdowns can also hide evidence of killings<sup>6</sup> and even send the disconnected directly into the line of fire.<sup>7</sup> In many cases, shutdowns blend into a “tapestry of crises” marked by armed conflict, poverty, and displacement—a trend exacerbated by the COVID-19 pandemic.<sup>8</sup>

Disrupting communication channels creates the illusion of public safety and government control, but the true governing force is chaos. Falsehoods do not stop circulating in a disrupted information environment,<sup>9</sup> while verified information is often buried in the same currents of rumor that find their expression online. Disconnection triggers indignation and opposition, often fomenting or exacerbating violence as those affected scramble to react.<sup>10</sup> In short, the lack of connectivity can precipitate a catastrophic cascade of harms, rife with collateral damage, whose endpoint is impossible to predict.

### **How should companies respond to government demands?**

Civil society, academics, and network traffic experts have worked tirelessly to expose the occurrence of shutdowns and their impact. However, the complete lack of transparency that most governments have displayed in this domain underscores an urgent need for the private sector to fulfill its own responsibilities.

---

<sup>4</sup> Abrougui, Afef. Global Voices. “South Asian governments keep ordering internet shutdowns – and leaving users in the dark” (2018), <https://globalvoices.org/2018/09/07/south-asian-governments-keep-ordering-mobile-shutdowns-and-leaving-users-in-the-dark/>.

<sup>5</sup> Access Now. “Shattered dreams and lost opportunities: A year in the fight to #KeepItOn” (2021) [https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data\\_Mar-2021\\_3.pdf](https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf). Rydzak, Jan. Global Network Initiative. “Disconnected: A human rights-based approach to network disruptions” (2019), <https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf>.

<sup>6</sup> Amnesty International. “A web of impunity: The killings Iran’s internet shutdowns hid” (2020), <https://iran-shutdown.amnesty.org/>.

In July 2020, when the government of Ethiopia imposed a complete network shutdown during a wave of violent unrest in the Oromia region, researchers were unable to pinpoint the dates, locations, and casualties resulting from the clashes as a direct result of the disruption. The Armed Conflict Location & Event Data Project. Ethiopia Peace Observatory (2021), <https://epo.acleddata.com/2021/06/03/introducing-the-ethiopia-peace-observatory/>.

<sup>7</sup> Audu, Ola’. *Premium Times*. “Borno residents want phone network restored as Boko Haram gets deadlier” (2013), <https://www.premiumtimesng.com/news/145640-borno-residents-want-phone-network-restored-boko-haram-gets-deadlier.html>.

<sup>8</sup> Rydzak, Jan & Elizabeth M. Renieris. Ranking Digital Rights. “Context before code: Protecting human rights in a state of emergency” (2020), <https://rankingdigitalrights.org/index2020/spotlights/context-before-code>.

Berkman Klein Center. “Lockdown and shutdown: Exposing the impacts of recent network disruptions in Myanmar and Bangladesh” (2021), <https://clinic.cyber.harvard.edu/files/2021/01/Lockdowns-and-Shutdowns.pdf>.

<sup>9</sup> Bajoria, Jayshree. Human Rights Watch. “India internet clampdown will not stop misinformation” (2019), <https://www.hrw.org/news/2019/04/24/india-internet-clampdown-will-not-stop-misinformation>.

<sup>10</sup> Rydzak, Jan. “Of blackouts and bandhs: The strategy and structure of disconnected protest in India” (2019), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3330413](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413).

The International Covenant for Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) guarantee individuals an array of rights, including the right to effective remedy. Governments violate many of these rights when they impose sweeping blackouts. In practice, however, state actors' consideration for the human rights impact of shutdowns is minimal, and no robust mechanisms exist that would compel them to report on it. High-level declarations such as the G7 Open Societies statement<sup>11</sup> only condemn "politically motivated" shutdowns, which entrenches the false notion that shutdowns ostensibly motivated by public safety have no political underpinnings. In light of governments' failure to police themselves, additional pressure is needed from states that aspire to maintain a high standard of human rights protection. This may include, for instance, states with no record of implementing shutdowns introducing mandatory transparency and due diligence requirements for telecom operators, covering the steps they take to address and mitigate the impact of shutdowns. Such requirements should apply to the global operations of telecom firms headquartered within the country in question.

Regardless of the regulatory environment, companies have a duty to their users to maximize their efforts to resist shutdowns. But under the UNGPs, their core responsibility is to protect their employees' physical safety. Because shutdowns are often carried out in volatile sociopolitical circumstances, staff on the ground can face extreme legal and physical risk. This tension explains companies' compliance with shutdown orders.

Nonetheless, the UNGPs also stipulate that companies have the duty to adopt mitigation and transparency measures in response to repressive measures such as network shutdowns.<sup>12</sup> Applying these measures and adopting strong policies to guide them sets the expectation that the indiscriminate use of shutdowns will be met with resistance and exposure. While company pushback alone is not enough to eradicate the use of shutdowns, it is a fundamental part of a strong collective response.

All private sector actors should generate friction to curb the use and impact of shutdowns. However, telecommunications operators often act as the direct executors of government orders and therefore have a unique duty to serve as models of responsible and transparent practice for all companies. Public disclosure is a critical component of their response for two reasons. First, it enables individual and collective responses to counter government impunity. Transparency on the processes, policies, legal bases, and actors involved—as well as on the orders themselves—provides an evidence base that ultimately brings users and civil society closer to holding the responsible parties accountable. Second, it can protect users from the harmful effects of shutdowns by raising awareness of an unfolding crisis, highlighting the risk of future disruptions, and offering an opportunity to anticipate the impact.

---

<sup>11</sup> G7 Cornwall. "2021 Open Societies Statement" (2021), <https://www.g7uk.org/wp-content/uploads/2021/06/G7-2021-Open-Societies-Statement-PDF-355KB-2-pages.pdf>.

<sup>12</sup> Voule, Clément. "Ending internet shutdowns: a path forward. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association to the Human Rights Council." A/HRC/47/24/Add.2. (2021), [https://reliefweb.int/sites/reliefweb.int/files/resources/A\\_HRC\\_47\\_24\\_Add.2\\_E.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_47_24_Add.2_E.pdf)

Companies should publish at least **eight key pieces of information** about their approach and response to network shutdown orders. All of them are captured in a set of questions comprising an indicator that evaluates the quality of companies' disclosures about such disruptions.

Companies should:<sup>13</sup>

Information needed	Example
Describe the circumstances under which they may shut down their service completely	<b>Orange</b> specifies that a government may force it to interrupt some or all of its services in certain circumstances, such as before, during, and after elections. <sup>14</sup>
Describe the circumstances under which they may shut down specific services (e.g., social media)	<b>Vodafone</b> spells out the circumstances under which government authorities can order telecom operators to shut down specific communication services. <sup>15</sup>
Outline their process for responding to shutdown demands	<b>Orange</b> indicates that its process for responding to network shutdown demands consists of requesting a formal, traceable request, written and signed by a competent public authority with the appropriate jurisdiction and based on a regulatory text. <sup>16</sup>
Disclose a commitment to push back	<b>MTN</b> commits to pushing back against demands and orders that can affect their users' human rights. <sup>17</sup>
Commit to notifying users directly ahead of a shutdown	<b>MTN</b> states that it was able to alert those affected by a shutdown in advance of some of the disruptions that took place in 2019. <sup>18</sup>
Report on the number of shutdown demands received	<b>Telenor</b> specifies the number of network shutdown requests received in each country where it operates, unless bound by regulatory restrictions on transparency. <sup>19</sup>

<sup>13</sup> Ranking Digital Rights. *2020 indicators: F10* (2019), <https://rankingdigitalrights.org/index2020/indicators/F10>.

<sup>14</sup> Orange S.A. "Orange transparency report on freedom of expression and protecting privacy: 2020 data" (2021), [https://gallery.orange.com/\\_h/Rays3G](https://gallery.orange.com/_h/Rays3G).

<sup>15</sup> Vodafone Group plc. "Freedom of expression and network censorship" (nd), [https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone\\_drf\\_freedom\\_expression\\_network\\_censorship.pdf](https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone_drf_freedom_expression_network_censorship.pdf).

<sup>16</sup> Orange S.A. "Orange transparency report on freedom of expression and protecting privacy: 2020 data" (2021), [https://gallery.orange.com/\\_h/Rays3G](https://gallery.orange.com/_h/Rays3G).

<sup>17</sup> MTN Group Limited. "Digital human rights" (2020), <https://www.mtn.com/wp-content/uploads/2020/09/MTN-position-on-Digital-Human-Rights-1.pdf>.

<sup>18</sup> MTN Group Limited. "Sustainability report for the year ended 31 December 2019" (2020), <https://www.mtn.com/wp-content/uploads/2020/03/MTN-Sustainability-report.pdf>.

<sup>19</sup> Telenor Group. "Authority request disclosure report 2020" (2021), <https://www.telenor.com/wp-content/uploads/2021/05/Telenor-Authority-Requests-Disclosure-report-2020.pdf>.

Disclose the legal authorities that make demands	<b>Telefónica</b> lists the competent authorities that are empowered by the law of each country to make shutdown demands. <sup>20</sup>
Report on the number of shutdown demands with which they complied	<b>Telenor</b> discloses compliance rates for network shutdown demands for each country where it operates, unless bound by regulatory restrictions on transparency. <sup>21</sup>

Table 1 List of disclosures expected of companies with regard to network shutdown orders based on Indicator F10 (Network shutdowns) in the 2020 RDR Index.<sup>22</sup>

**Unfortunately, companies largely fail to fulfill these standards.** Poor company transparency continues to undercut efforts to hold governments accountable. RDR’s evaluation of 12 global telecom companies, which together provide internet and telecommunications services in more than 120 countries, illuminates these gaps. Only a handful of companies outline how they handle shutdown orders, and nearly none commit to pushing back, pledge to notify their users prior to or during a shutdown, or disclose which government entities are vested with the authority to order a shutdown.<sup>23</sup>

As shown below, this pattern of opacity holds regardless of geography or incidence of shutdowns, as companies headquartered in countries with shutdown-prone governments (e.g., Bharti Airtel in India) are often just as silent about their approach to disruptions as telecom titans whose user base has never experienced a shutdown (e.g., AT&T in the United States). While operators occasionally argue that the risk of shutdowns occurring in the markets where they operate is low, this does not justify the absence of a policy, which should precede the emergence of a crisis rather than arise in the scramble to address it. Companies that are not under continuous public scrutiny are likely to have an even poorer record of disclosure, with fewer vectors of pressure to compel them to act responsibly. Previous research has also shown that state ownership of internet service providers (ISPs), which are often mobile and fixed internet operators, is tied to the likelihood of shutdowns.<sup>24</sup>

<sup>20</sup> Telefónica, S.A. “Report on transparency in communications 2021” (2021), <https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/08/Report-on-Transparency-in-Communications-2021.pdf>.

<sup>21</sup> Telenor Group. “Authority request disclosure report 2020” (2021), <https://www.telenor.com/wp-content/uploads/2021/05/Telenor-Authority-Requests-Disclosure-report-2020.pdf>.

<sup>22</sup> Ranking Digital Rights. *2020 indicators: F10* (2019), <https://rankingdigitalrights.org/index2020/indicators/F10>.

<sup>23</sup> *Ibid.*

<sup>24</sup> Freyburg, Tina & Lisa Garbe. “Blocking the bottleneck: Internet shutdowns and ownership at election times in Sub-Saharan Africa.” *International Journal of Communication*, Vol 12 (2018), 3896–3916. <https://ijoc.org/index.php/ijoc/article/view/8546>

Company	E1	E2	E3	E4	E5	E6	E7	E8
AT&T	Orange	Gray	Gray	Gray	Gray	Orange	Gray	Gray
América Móvil	Gray	Gray	Gray	Gray	Gray	Gray	Gray	Gray
Axiata	Orange	Gray	Gray	Gray	Gray	Gray	Gray	Gray
Bharti Airtel	Orange	Gray	Gray	Gray	Gray	Gray	Gray	Gray
Deutsche Telekom	Orange	Orange	Gray	Gray	Gray	Gray	Gray	Gray
Etisalat	Orange	Orange	Gray	Gray	Gray	Gray	Gray	Gray
MTN	Orange	Gray	Orange	Green	Orange	Gray	Gray	Gray
Ooredoo	Orange	Gray	Gray	Gray	Gray	Gray	Gray	Gray
Orange	Green	Gray	Green	Gray	Gray	Gray	Gray	Gray
Telefónica	Orange	Orange	Green	Orange	Gray	Green	Green	Green
Telenor	Green	Gray	Green	Green	Gray	Green	Green	Green
Vodafone	Green	Green	Green	Green	Gray	Gray	Gray	Gray

*Table 2* Evaluation of company transparency on network shutdown policies and practices based on the 2020 Ranking Digital Rights Corporate Accountability Index (Indicator F10: Network shutdowns). Elements in the top row correspond to the eight components of good disclosure listed in Table 1. Gray indicates no disclosure, orange indicates partial (insufficient or vague) disclosure, and green indicates full (sufficient) disclosure.

Despite this long-standing and widespread lack of transparency, some positive shifts have occurred in corporate responses to large-scale disruption. Companies that have faced numerous shutdowns in their operating markets are beginning to publish more information on their process and the volume of demands received in their transparency reports.<sup>25</sup> Operators headquartered in Latin America<sup>26</sup> and Sub-Saharan Africa<sup>27</sup> have recently published their first reports of this kind, incorporating information on shutdowns to varying degrees and setting a precedent for their peers in the region. While overall progress remains slow, these developments create space for further improvement.

These tentative successes cannot be taken for granted. The tumultuous withdrawal of Norwegian operator Telenor from Myanmar following the February 2021 coup and subsequent shutdowns shows that even relatively responsible corporate actors can be forced into

<sup>25</sup> Telenor Group. “Authority request disclosure report” (2020), <https://www.telenor.com/wp-content/uploads/2021/05/Telenor-Authority-Requests-Disclosure-report-2020.pdf>

<sup>26</sup> América Móvil. “Communications transparency report 2020” (2020), <http://img1.telcel.com/amx/communications-transparency-report.pdf>.

<sup>27</sup> MTN Group Limited. “Transparency report 2019” (2020), [https://www.mtn.com/wp-content/uploads/2020/11/MTN-Transparency-Report-2020\\_Final.pdf](https://www.mtn.com/wp-content/uploads/2020/11/MTN-Transparency-Report-2020_Final.pdf).

submission.<sup>28</sup> Their successors—and other future entrants into emerging economies marked by conflict—are at even greater risk of being co-opted in service to repressive governments. It is therefore vital that companies build on the tenuous successes of their peers, build up their policies, and contribute more actively to the collective campaign to end network shutdowns.

Thank you again for the opportunity to participate in this call for input. We look forward to engaging further with OHCHR on these matters. We can be reached by email at [policy@rankingdigitalrights.org](mailto:policy@rankingdigitalrights.org).

Sincerely,

Jan Rydzak, PhD  
Company & Investor Engagement Manager

Nathalie Maréchal, PhD  
Senior Policy & Partnerships Manager

---

<sup>28</sup> Meaker, Morgan. *Wired*. “Myanmar’s fight for democracy is now a scrap over phone records” (2022), <https://www.wired.com/story/telenor-myanmar-phone-records/>.