7. Telecommunications disconnect

Most of the changes by telecommunications companies came from Global Network Initiative members.

In March 2017, **Orange**, **Telefónica**, and **Vodafone** joined the Global Network Initiative (GNI), along with four other members of the now-disbanded Telecommunications Industry Dialogue (TID).[84] As Figure 17 illustrates, over the past year those three GNI companies implemented substantial and meaningful changes to their disclosed policies affecting users' freedom of expression and privacy. Other telecommunications companies evaluated for the Index remained largely static over the past year—including AT&T, which was previously a member of the TID and held GNI observer status for one year, but did not join GNI along with its European peers.

Improvements by these companies occurred in the absence of significant legal and regulatory change, with the exception of Europe's new data protection regulations that come into force in May 2018 (hence, requirements for greater disclosure and more responsible data handling practices under these regulations, discussed in Chapter 3, were not yet fully implemented by companies when Index research ended in January 2018).[85] It appears that GNI membership was the main driver of the improvements by Orange, Telefónica, and Vodafone in the 2018 Index—and that it is a catalyst and framework for multinational telecommunications companies to improve their commitments, policies, and disclosures affecting users' freedom of expression and privacy rights, at least in relation to corporate governance and responses to government demands.

Yet the GNI framework is incomplete: it is focused primarily on increasing transparency and accountability around government demands for shutdowns, censorship, and surveillance. Commercial practices that also affect global information flows, along with commercial data protection and privacy issues, have generally fallen outside GNI's scope of work. Thus it is not surprising that the three GNI telecommunications companies made their greatest gains in the Governance category of the Index (see Chapter 3 for a full analysis of 2018 governance scores). In the Freedom of Expression and Privacy categories, improvements were found mainly in transparency reporting: specifically, improved disclosure of data and policies related to government requests to restrict information flows or requests to hand over user data.

How were telecommunications companies selected and evaluated?

The 10 telecommunications companies in the Index were selected due to their global footprints—with operations across multiple countries—and geographical diversity of their "home" countries. Added together, the operations of these multinational companies span across developing and major OECD markets. These companies own operating subsidiaries in multiple markets, and must comply with specific regulatory regimes on a country-by-country basis, but also answer to the group-level corporation. Due to resource limitations, RDR evaluated only the home country operating company of each telecommunications company group. We evaluated global group-level policies for relevant indicators plus the home-country operating subsidiary's pre-paid and post-paid mobile service, and fixed-line broadband service, where offered.

For more about Index scoring and evaluation, see Section 1.4.

Telecommunications companies provide the fixed-line and mobile internet service necessary for users to access the platforms and services offered by internet and mobile ecosystem companies. Governments can require that such companies block users' access to blacklisted websites. Most countries block child exploitation material, while others block a broader set of content, which can include political and religious material. Some governments require telecommunications companies to block users' access to specific internet or mobile ecosystem companies' applications or websites if those companies fail to comply with content-removal demands to their satisfaction. The long-term blocking of Facebook, Twitter, and YouTube in China is just one example of this. Governments can also compel telecommunications companies to shut down all access to fixed-line or mobile internet services. (See Section 7.2 below for further discussion of network shutdowns.)

In a 2017 report, David Kaye, U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted that governments increasingly exercise power over telecommunications companies in ways that violate human rights norms by being over-broad, non-transparent, unaccountable, and lacking due process.[86] Unlike internet and mobile ecosystem companies which can serve users remotely, telecommunications companies must be present on the ground and are obliged to uphold domestic laws as well as the terms of their license agreements with the host government. These companies can also face "extra legal intimidation, such as threats to the safety of their employees and infrastructure in the event of non-compliance."[87]

Telecommunications companies in this Index are under pressure to comply with an increasing number of government demands to shut down networks or block access to websites, combined with pressure from civil society to be more accountable about when and why they do so. Laws—and regulatory ambiguity—in many countries prevent telecommunications companies from performing well in the Index. Individual company report cards identify specific ways that the law hinders each company from respecting users' rights. Yet we have also identified ways that all telecommunications companies in the Index can improve their commitment and disclosure, even under current regulatory and legal realities.

7.1. Chokepoints for global information flows ## {#section-71}

Lack of transparency by telecommunications companies makes it impossible for people to understand why, how, and under whose authority, their speech and access to information is blocked or restricted through their mobile or fixed-line internet service provider.

When a person suddenly cannot access news websites through their phone or office internet connection, who do they hold responsible? The internet service provider or their government? When a candidate for an opposition party does not know how, when, by whom, and under what authority she may be tracked and monitored through her smartphone, the implications for human rights and accountable governance in her country are serious. Yet, to varying degrees, that is the reality for users of all the telecommunications companies evaluated by the Index.

The 2018 Index includes eight indicators evaluating how transparent telecommunications companies

are about policies and practices for policing content and access—both as a result of enforcement of their own private rules and as a result of compliance with external requests from governments and other third parties. We expect companies to clearly disclose what types of content and activities they prohibit (F3), and to publish data about the volume and nature of content and accounts they removed or restricted for violating these rules (F4). Companies should also clearly disclose policies for responding to government and private requests to restrict content and user accounts (F5), and publish data about the types of such requests they received and with which they complied (F6, F7). We expect companies to disclose that they notify users when they have removed content, restricted a user's account, or otherwise restricted access to content or a service (F8).

Results of the 2018 Index show that these companies reveal little about their content-blocking activities—whether as a result of enforcing their own rules, or demands from governments and other external entities to block websites or shut down networks (Figure 18).

As Figure 18 shows, there were few improvements. **Telefónica** demonstrated the most improvements of any telecommunications company, clarifying reasons it may not comply with government requests (F5), and disclosing more detail about the number of government requests that it received to restrict content or accounts that it received and the number of those requests with which it complied (F6). The company, along with **AT&T**, **Orange**, and **Vodafone**, also improved disclosure of its handling of government demands to shut down networks (F10).

Disappointingly, **Axiata** and **Vodafone** were less transparent than in the 2017 Index about whether they have policies of notifying users when they block content or restrict a user's account (F8). Vodafone's most recent Law Enforcement Disclosure report,[88] which outlines the company's approach to handling content restriction requests from governments and law enforcement, did not specify whether it notifies users who attempt to access content that it has been restricted, whereas the previous version of this report did.

No company improved disclosure about its network management policies and practices (F9). Bharti Airtel's score even declined on that indicator (see company report card in Chapter 10 for details).

7.2. Network shutdowns ## {#section-72}

Despite small improvements, a lack of disclosure from companies on network shutdown policies leaves users in the dark about this human rights threat.

Network shutdowns pose a threat to human rights. When telecommunications companies cut off access to their networks, millions of people can be left without the ability to communicate. This threat is particularly acute during times of political crisis, when the ability to communicate is most vital and when authoritarian governments more often impose such restrictions. In June 2016, the United Nations Human Rights Council adopted a resolution condemning network shutdowns and other intentional restrictions on access as violations of international human rights law.[89]

According to the global advocacy group Access Now there were more than 116 network shutdowns documented around the world between January 2016 and September 2017.[90] The Software Freedom Law Center documented 70 shutdowns in 2017 in India alone.[91] The issue has received global attention thanks to persistent civil society campaigning, including a multi-year campaign by Access Now. The Global Network Initiative (GNI) has committed to conduct policy advocacy to end the practice,[92] and the governmental Freedom Online Coalition has declared network shutdowns to be a violation of human rights.[93]

While telecommunications companies cannot stop governments from demanding shutdowns and threatening their staff, the Index rewards those that disclose their policies and practices for responding to government shutdown demands. Ideally companies should also report data about the volume and nature of shutdown orders received, and the number complied with.

There is a long way to go: the average score on this indicator was just 18.75 percent, with all companies failing to provide sufficient information about how they respond to such demands.[94] While four telecommunications companies—**AT&T**, **Orange**, **Telefónica**, and **Vodafone**—improved their disclosure of how they deal with government requests to shut down networks, all companies still lacked transparency.

An examination of company disclosure reveals the following:

- **Telefónica** and **Vodafone**, both Global Network Initiative (GNI) members, disclosed more than the rest of their peers about policies and practices for handling network shutdown orders by authorities.

- **Telefónica** was the only company to disclose the number of shutdown orders it received and to clearly list the legal authority in each country from which it received shutdown orders. The company also clarified why it may push back against, or reject, a network shutdown demand and provided some data about its compliance with these types of orders. It disclosed information on the circumstances under which it would restrict access to its service or restrict certain types of traffic, although its disclosure was not as comprehensive as Vodafone's.

- **Vodafone** was the only company to clearly disclose its process for responding to these types of government demands and to clearly commit to push back against demands when possible. The company also disclosed clear policies about the circumstances under which it would restrict access to its service or restrict certain types of traffic and clarified how the company weighs the the freedom of expression risks associated with these types of requests.

- While only **Telefónica** disclosed the number of shutdown requests it received, **AT&T** improved its disclosure in this regard by stating that it would disclose the number of shutdown requests it received if it had received any.

- **Orange** improved its disclosure by detailing an example from 2011 in which it pushed back on a shutdown request from the Egyptian authorities.

Several companies had particularly low levels of disclosure, and made no improvements since the 2017 Index, including **Bharti Airtel**, **Axiata**, **Ooredoo**, and **América Móvil**.

- **Bharti Airtel** disclosed almost nothing about how it responds to government requests to shut down its networks, aside from very broad language about reasons why service might be disrupted. While Indian law prevents companies from disclosing information about specific government shutdown orders,[95] there is no legal obstacle to disclosing clear reasons why the company may have to shut down its networks or company policies for evaluating and responding to shutdown requests, and there is also no obstacle to having a policy to notify

users about shutdowns.

- **Axiata** and **Ooredoo** also disclosed only very broad or vague reasons why their service might be disrupted. Neither company's home jurisdiction has laws restricting disclosure of the company's process for responding to these types of requests. Both companies could be more transparent about how they respond to shutdown requests, the reasons why shutdowns might occur, and whether they have a policy of notifying users about shutdowns.

- **América Móvil** disclosed no information whatsoever about its handling of network shutdown requests, even though no laws in Mexico bar such disclosure.

7.3. Policing access to information ## {#section-73}

Telecommunications companies disclose almost nothing about how they handle or comply with government and private requests to block content or user accounts.

Just four companies—**AT&T**, **Etisalat**, **Telefónica**, and **Vodafone**—disclosed anything about their process for handling government requests to block content (Figure 20). Only two companies—**AT&T** and **Telefónica**—supplied data about such requests.

Vodafone disclosed more than its peers about its process for handling third-party requests, but then disclosed no data about its compliance with these requests. No telecommunications company provided any data about private requests it received to restrict content or accounts.

While most telecommunications companies disclosed some information about what types of content or activities are prohibited on their services, none disclosed any information about what actions they take to enforce these terms.

Telecommunications companies have the ability to block content or access to their services, according to their own internal rules and in line with the regulations of the country in which they operate.

Most telecommunications companies provide some information about their rules in their terms of service, however, Index results show that most companies failed to provide enough information about these rules in order for users to understand what actions companies take to enforce them (Figure 21). As gatekeepers to the internet, these companies should be more transparent about the role they play in policing users' access to information.

No telecommunications company made any improvement on indicators related to terms of service enforcement in the 2018 Index. None published any data about the volume of content or URLs it blocks or user accounts it otherwise restricts or suspends, as a result of breaches to those terms.

While every telecommunications company in the Index disclosed some information about the policies for enforcing its terms of service, disclosure is inadequate across the board, with some companies disclosing very little. As Figure 21 shows, **Orange France** disclosed more than any other telecommunications company, followed by **Telefónica Spain**, **AT&T**, and **Vodafone UK**.

Results also show:

- Six out of the 10 telecommunications companies—**Telcel (América Móvil)**, **Etisalat UAE**, **Ooredoo Qatar**, **Orange France**, **Telefónica Spain**, and **Vodafone UK**—received full credit for their disclosure of what types of content or activities they prohibit, and the reasons why they may restrict a user's account. **AT&T** also earned high scores on these elements but fell short of comprehensive disclosure for its post-paid mobile service.

- **Telcel (América Móvil)**, **AT&T**, **Etisalat UAE**, **Orange France**, **Telefónica Spain**, and **Vodafone UK** each disclosed at least some information about its process for enforcing its rules, including steps it may take when a user violates its terms.

- **AT&T**, **Telefónica Spain**, and **Vodafone UK** provided some information about how they identify content or activities that violates their rules, though none fully disclosed how they identify these breaches.

- The lowest scoring companies—**Celcom (Axiata)**, **Airtel India (Bharti Airtel)**, **Ooredoo Qatar**, and **MTN South Africa**—disclosed no information other than the types of content or activities they prohibit and why they may restrict a user's account.

7.4. Privacy problems: surveillance and data protection ## {#section-74}

Users don't know much about who has access to their information, for what purposes, under whose authority, and under what circumstances.

As providers of fixed-line and mobile data services, telecommunications companies know what websites and applications people access. They have direct access to all of their users' unencrypted communications. All of this information can be shared with governments, commercial partners, and other third parties.

Without transparency about what information is collected, how long it is retained, what is shared with whom, and for what purposes and under whose authority, there is neither accountability nor basic checks against abuse. If people's information is used for surveillance purposes that violate basic international human rights norms, they cannot to hold their abusers accountable. If personal information is shared without users' knowledge and consent with parties who use it for commercial purposes, it is difficult to identify perpetrators and obtain redress when the user falls victim to predatory or discriminatory economic, financial, social, or political targeting.

While there are legitimate national security and law enforcement reasons why users should not be notified in real time when their information is shared with authorities, people have a right to know the circumstances under which they can expect their information to be shared, and with whom. People have a right to know that companies have rigorous policies in place to prevent access to personal data that is not requested lawfully. Furthermore, there are no legitimate public interest reasons why companies should not be transparent about the sharing of information with commercial and non-governmental parties.

Given the amount of sensitive information telecommunications providers may have access to about people who use their services, it is reasonable to expect companies to publish the privacy policies

that govern how they handle this information. Users should be able to assess and compare the privacy policies of different companies and services *before* they make a choice to subscribe and hand over their user information, and other interested parties, like investors, should be able to evaluate a company's data handling policies in order to gauge potential risks. Companies should also publicly commit to notify users of any changes to their privacy policy and to make these changes public, so that users are fully aware of any shifts in how a company collects, shares, uses, or retains their information.

Our researchers did not identify any legal or regulatory reasons why all of the telecommunications companies in the Index should not earn full credit for publicly disclosing clear and accessible privacy policies, and for notifying users of changes to those policies. Yet as Figure 22 shows, even such basic disclosure is a challenge for many.

The privacy policies for **Telcel (América Móvil)**, **Celcom (Axiata)**, and **Telefónica Spain** were easy to find and available in the primary languages of their home markets, but these policies were not presented in a way that would be easy for most consumers to understand. The privacy policy for **Airtel India (Bharti Airtel)** was easy to find, but was not available in languages other than English and was divided across several separate documents, making it difficult for users to comprehend the scope of the terms. **MTN South Africa's** privacy policy was presented in a more easily read manner than Bharti Airtel's, but was not as straightforward to find on the company's website, and was not available in the primary languages (other than English) of MTN's home market.

AT&T was the only telecommunications company to commit to notify users of changes to its privacy policy. It provided users with a timeframe for notice, but failed to disclose that it would directly notify users of these changes, instead opting to post them on its website, which is not considered a form of direct notification.

Etisalat UAE and **Ooredoo Qatar** were the only two telecommunications companies for which researchers were unable to locate a publicly available privacy policy for their services.

Opacity in the Arab region The absence of publicly disclosed privacy policies by Etisalat UAE and Ooredoo Qatar is an example of how telecommunications companies lack transparency across the Arab region. Research by Social Media Exchange (SMEX), a Beirut-based media development and digital rights organization, found that of the region's 66 mobile operators, only seven published privacy policies. Of these seven companies, two are subsidiaries of the Vodafone group, a GNI member: Vodafone Egypt and Vodafone Qatar. None of the five subsidiaries of Orange, also a GNI member, published privacy policies. These subsidiaries are Orange Egypt, Orange Jordan, Orange Morocco, Orange Tunisia, and a joint venture company Korek Telecom (Iraq). There are no apparent legal factors preventing Orange from publishing its privacy policies in these countries. For example, the SMEX report found that other operators in Tunisia and Jordan, LycaMobile Tunisia and Zain Jordan, published privacy policies. **Read more at:** "Dependent Yet Disenfranchised: The Policy Void That Threatens the Rights of Mobile Users in Arab States," The Social Media Exchange (SMEX), January 2018, https://smex.org/dependent-yet-disenfranchised-the-policy-void-that-threatens-the-rights-of-mobile-users-in-arab-states/.

Surveillance accountability: Companies fail to provide maximum, legally permissible transparency about how they handle third-party requests for user information.

Many countries have over-broad surveillance laws that do not require basic transparency and accountability on the part of government authorities. These laws also often prevent telecommunications companies from disclosing even general information about the companies' processes for complying with demands and what information is shared with authorities. Thus, some companies have their home governments—and laws that breach international human rights standards—to blame for their lack of transparency regarding how they handle government requests for user information. Nonetheless, there are ways that each and every one of the telecommunications companies in this Index can improve their scores on these indicators.

Index data shows that of the 10 telecommunications companies evaluated, seven disclosed some information about their process for evaluating and responding to requests to hand over user information—and only four of these companies provided any data on the number of such requests they received, or the number with which they complied (Figure 23).

Results revealed the following:

- **Orange** and **Telefónica** both improved their disclosure of how they handle government requests for user information. Orange disclosed data about the number of requests it received from French authorities for real-time and stored communications data. Telefónica disclosed some data about the number of accounts affected by government requests and its compliance rates.

- Three companies—**Axiata** (Malaysia), **Ooredoo** (Qatar), and **Etisalat** (UAE)—disclosed no information whatsoever about their processes for responding to government and private requests for user information. Yet all three of these companies could make significant improvements to their disclosure without changes to the laws in their home jurisdictions. In Qatar and the UAE, telecommunications companies may be required to give government officials direct access to their networks, so while they may not have precise data about the number of times government officials accessed user information, there is nothing in the law preventing Ooredoo and Etisalat from disclosing information about these processes.[96] And while Malaysia's Official Secrets Act may prohibit some disclosure of government requests, nothing prevents Axiata from publishing at least some information about how it handles third-party requests for user information.[97]

- The highest-performing companies—**AT&T** and **Vodafone**—each disclosed clear information about how they respond to judicial and non-judicial government requests and requests from foreign jurisdictions, the legal basis under which they comply with such requests, and a commitment to conduct due diligence and push back against overbroad government requests. However, neither company disclosed information about their processes for responding to private requests, or data about such requests that they received, even though there are no specific legal barriers preventing them from doing so.

- **América Móvil** and **Bharti Airtel** disclosed very minimal information about their processes for responding to requests for user information. There are no legal barriers in Mexico preventing América Móvil from disclosing information about how it evaluates and responds to such requests. Indian law prevents companies like Bharti Airtel from publishing data on government

requests for user information but does not prevent them from disclosing their processes for responding to these requests.

No telecommunications company disclosed information about their policies for notifying users when their information is requested. While laws may prohibit companies from notifying users when a government official demands a user's information, most companies could still at least disclose the situations in which they are prohibited from notifying users, and their notification policies for private requests.

Data protection: Telecommunications companies fail to disclose clear information about collection, use, and sharing of personal information

The 2018 Index includes six indicators evaluating corporate transparency about handling of user information.[98] We expect companies to disclose what information they collect (P3), what information they share and the types and names of the third parties with whom they share it (P4), the purpose for collecting and sharing user information (P5), and for how long this information is retained (P6). Companies should also provide clear options for users to control what information is collected and shared, including for the purposes of targeted advertising (P7). We expect companies to clearly disclose how users can obtain all public-facing and internal data they hold on users, including metadata (P8).

Results of the 2018 Index show that telecommunications companies were generally less transparent than internet and mobile ecosystem companies about their handling of user information, including what data they collect, share and for what purpose, whether users have any control over what is shared, and whether users can obtain all the information a company holds on them.

As in the 2017 Index, **AT&T** disclosed more than any other telecommunication company, including the three European companies (Orange, Telefónica, and Vodafone) about its handling of user information (Figure 24).

There was little improvement across these indicators for the 2018 Index: two companies—**AT&T** and **Orange**—improved disclosure of options users have to access their information (although none disclosed that users can access all of the information a company holds on them). Telecommunications companies disclosed particularly little about data retention policies: only two companies, **AT&T** and **Vodafone**, disclosed any information, and what they did disclose is scant.

While **AT&T** disclosed little regarding its handling of user information, it performed better on this set of indicators than all of the other telecommunications companies evaluated in the Index. The company was slightly more transparent about what user information it collects, as compared to what it shares, and the purposes for doing so. AT&T provided little information on how long it retains user information, but was the only company other than Vodafone to provide any relevant information.

It is notable that, even with Europe's strong data protection laws, EU-based telecommunications companies had insufficient and inconsistent disclosure of how they collect, share, retain, and otherwise handle user information, particularly next to their U.S. peer, AT&T. While these companies may be communicating with regulators about data collection, handling, and sharing to ensure compliance with the law, as of January 2018 when research for this Index was concluded, these companies were still not communicating clearly with the public. As Europe's new privacy regulations come into force in the middle of 2018 we hope to see further improvement in European companies' disclosure about how they handle user information.

Several jurisdictions lack adequate data protection laws, and companies headquartered in these

jurisdictions tend to disclose no more than the law requires, resulting in low Index scores. In the UAE, where **Etisalat** is headquartered, there is no data protection law or general privacy law. In other places the law provides wide loopholes: in Qatar, where **Ooredoo** is headquartered, companies are exempt from complying with the data protection law if they are executing a court order, collecting information pertaining to a crime per police request, or other exceptions. (As noted previously in this chapter, privacy policies of Etisalat and Ooredoo are not made publicly available.) In South Africa, where **MTN** is headquartered, the company's low privacy score appears related to the fact that the Protection of Personal Information Act (POPI) still has not yet entered into force, even though it was signed into law in 2013.[99] In India, the Supreme Court's 2017 ruling that privacy is a fundamental constitutional right has become the basis for development of a new data protection law that has potential to drive improved disclosure by Indian ICT-sector companies, including **Bharti Airtel**, in the near future.

7.5. Recommendations for telecommunications companies ## {#section-75}

- **Work with civil society and legislators to enact legal reforms aimed at ensuring that the law enables maximum respect for users' privacy rights.** In particular, companies should use every opportunity available to encourage governments to move away from mass surveillance and institute meaningful oversight over national security and law enforcement authorities, in accordance with The International Principles on the Application of Human Rights to Communications Surveillance.[100]

- **Where the law does not explicitly mandate it, refrain from requiring users to register their identity**, such as by providing a government-issued document or a credit card (other than for billing purposes, if applicable).

- **Commit to push back against network shutdown requests, and disclose data regarding the number of such requests received.** Network shutdowns continue to threaten users' ability to exercise their rights. Given these growing threats, companies must endeavor to disclose as much information as possible about their processes and principles for responding to such requests, and confirm the number of requests they received.

- **Publish comprehensive transparency reports.** Companies should publish regular information and data on their official websites that helps users and other stakeholders understand the circumstances under which personal information may be accessed, or when access to service may be blocked or restricted. Such disclosures should include the volume, nature, and legal basis of requests made by governments and other third parties to access user information or restrict speech. Disclosures should include information about the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own terms of service.

- **Disclose meaningful data about government requests to restrict content or accounts.** While some companies disclose some data about these requests, more disclosure is needed. In particular, companies should disclose the number of requests they receive per country as well

as the number of requests with which they comply.

- **Clarify private processes through which websites may be blocked or accounts may be restricted.** Compared to their disclosure about government requests, companies disclose less about how they respond to private requests to restrict content or accounts, and what types of private requests they will consider. Companies should therefore improve their disclosure by clarifying under what circumstances they will respond, and by confirming that they conduct due diligence on such requests.

- **Commit to notifying users of censorship events.** Companies should disclose their policies for notifying users when they restrict their content or accounts, including the reason for doing so.

- **Disclose meaningful data about terms of service enforcement.** Companies should issue transparency reports, ideally every six months, showing the number of actions they took to remove content or restrict accounts that violated their rules, and the reasons for doing so (e.g. the number of accounts restricted for posting extremist content, the number of items removed for containing hate speech, etc).

- **Provide examples of how rules are enforced.** Even when companies publish their rules, it is very unclear how they are enforced. Reports of arbitrary blocking or inconsistent restrictions on accounts make it all the more difficult to understand how platforms are being policed. Clearer disclosure on this front will help restore trust between users and the services on which they rely, and could help empower users to understand and seek remedy when their content or accounts have been unfairly restricted.

Footnotes

[84] See “Global Network Initiative Adds Seven Companies in Milestone Expansion of Freedom of Expression and Privacy Initiative | Global Network Initiative,” Global Network Initiative, March 27, 2017, https://www.globalnetworkinitiative.org/news/global-network-initiative-adds-seven-companies-milestone-expansion-freedom-expression-and.

[85] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),” (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

[86] “A/HRC/35/22: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression” (United Nations Human Rights Council, March 30, 2017), https://ccdcoe.org/sites/default/files/documents/UN-170726-AHRC3522.pdf.

[87] “A/HRC/35/22: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression” (United Nations Human Rights Council, March 30, 2017), https://ccdcoe.org/sites/default/files/documents/UN-170726-AHRC3522.pdf.

[88] “Law Enforcement Disclosure Statement: Digital Rights and Freedoms,” Vodafone, May 2017, http://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_statement.pdf.

[89] “Resolution A/HRC/32/L.20 on the Promotion, Protection and Enjoyment of Human Rights on the Internet” (United Nations Human Rights Council, June 30, 2016), https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

[90] “Launching STOP: the #KeepItOn internet shutdown tracker,” Access Now, November 16, 2017, https://www.accessnow.org/keepiton-shutdown-tracker/.

[91] “Internet Shutdowns,” Software Freedom Law Center, accessed March 21, 2018, https://www.internetshutdowns.in/.

[92] “Global Network Initiative and Telecommunications Industry Dialogue Joint Statement on Network and Service Shutdowns,” Global Network Initiative, July 12, 2016, https://globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-joint-statement-network-and.

[93] “The Freedom Online Coalition Joint Statement on State Sponsored Network Disruptions” (Freedom Online Coalition, 2017),

https://www.freedomonlinecoalition.com/wp-content/uploads/2017/03/FOCJointStatementonStateSponsoredNetworkDisruptions.docx.pdf.

[94] See “Network Shutdowns” in the 2017 Index: “Network Shutdowns: Users Are in the Dark about Why They’re Cut Off,”https://rankingdigitalrights.org/index2017/findings/networkshutdowns/.

[95] “License Agreement for Provision of Internet Services” (Government of India Ministry of Communications & IT), accessed March 14, 2018, http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf, “License Agreement for Provision of United Access Services after Migration from CMTS” (Government of India Ministry of Communications & IT, December 3, 2009), http://www.auspi.in/policies/UASL.pdf, and “License Agreement for Unified License” (Government of India Ministry of Communications & IT), accessed March 14, 2018, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.

[96] “Public Telecommunications License No. 1/2006” Telecommunications Regulatory Authority, accessed March 15, 2018, https://www.tra.gov.ae/assets/03VgXUV3.pdf.aspx and “CLFR - Qatar,” Global Network Initiative, January 8, 2018, https://globalnetworkinitiative.org/content/clfr-qatar.

[97] “Official Secrets Act 1972,” Act 88 (1972), http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%2088.pdf.

[98] See the 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/.

[99] Michalsons, “Protection of Personal Information Act Summary,” Michalsons, accessed March 20, 2018, https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia.

[100] “International Principles on the Application of Human Rights to Communications Surveillance,” Necessary and Proportionate, accessed March 22, 2018, https://necessaryandproportionate.org/.