access

# TELCO ACTION PLAN

## RESPECTING HUMAN RIGHTS: TEN STEPS AND IMPLEMENTATION OBJECTIVES FOR TELECOMMUNICATIONS COMPANIES

# TELCO ACTION PLAN

## RESPECTING HUMAN RIGHTS: TEN STEPS AND IMPLEMENTATION OBJECTIVES FOR TELECOMMUNICATIONS COMPANIES

## INTRODUCTION

From Cairo to San Francisco, and London to Côte d'Ivoire, telecommunications companies ("telcos") increasingly encounter human rights considerations in their work. Under the United Nations Guiding Principles on Business and Human Rights implementing the Ruggie Framework, all companies have the responsibility to respect human rights and remedy violations. Without clear guidelines, however, the telecommunications sector faces particular challenges when navigating these emerging issues and responding to stakeholders as diverse as national and international governing bodies, national security services, civil society, consumers, and corporate investors.

In early 2011, Access (AccessNow.org) drafted a 5-step Action Plan to assist telcos seeking to conduct their operations in a way that ensures the protection of fundamental human rights. The initial Telco Action Plan was developed, in part, as a reaction to the responses of several companies to requests received from Middle Eastern and North African ("MENA") governments during the Arab Spring uprisings.

Nearly a year later, Access has drafted this revised Action Plan as a platform for continued dialogue with telcos seeking to operate in political and legal contexts that pose threats to the rights of freedom of expression, access to information, and privacy. This iteration further aims to guide companies, in a pragmatic manner, on how to mitigate the risks associated with operating in all countries, including those with a high propensity for human rights abuses. Benefits will include less liability for the companies and their investors, enhanced relationships with customers, and smoother and more predictable relations with host countries, particularly during times of crisis.

Uprisings around the world continue to pose complex challenges to companies that seek to operate in a rights-respecting manner. At the same time, it is important to recognize that users' rights to access, freedom of expression, and privacy are threatened not just in the MENA region but in countries around the world. Access is committed to protecting users' rights no matter where those users reside and, with this revised Action Plan, seeks to engage telcos as responsible partners in this effort.

While we often focus on moments of crisis and limits to the enjoyment of rights, Access believes it is important to acknowledge the extraordinary role that the telecommunications sector has played in enhancing the communications capabilities of billions of people. By delivering networks, services and open access, telcos are not simply service providers, but also 'freedom providers'.

# TEN STEPS EVERY RIGHTS-RESPECTING TELCO SHOULD UNDERTAKE

**Telcos shall:**

1. Operate in a manner that respects the fundamental human rights of all users, including the rights of freedom of expression, access to information, and privacy.
2. Seek to ensure that users' access to telecommunications networks is maintained at all times.
3. Conduct ongoing due diligence on the human rights-related risks associated with their operations in consultation with local and international stakeholders, including independent human rights experts.
4. Integrate the findings from human rights due diligence efforts into the management of their operations in order to prevent adverse human rights impacts.
5. Requests from governments and partners to restrict users' access, freedom of expression, or privacy should be presumptively rejected.
6. Insist that any restrictions on users' rights strictly comply with international human rights laws and standards and the rule of law, and are necessary and proportionate to achieve a clearly defined and legitimate public purpose.
7. Be transparent with all stakeholders regarding current or likely restrictions on users' access, freedom of expression, or privacy.
8. Engage in unilateral and multi-stakeholder dialogue, and advocacy as needed, with governments and business partners to ensure that users' rights are protected at all times and to strictly limit the human rights-related risks associated with the provision of telecommunications services.
9. Ensure that all users have access to appropriate public and/or private remedies, including accessible grievance mechanisms, to seek redress in the event that restrictions are imposed on their fundamental human rights of freedom of expression, access to information, and privacy.
10. Submit to independent assessment of corporate activities and compliance with human rights standards, such as through the Global Network Initiative.

# IMPLEMENTATION OBJECTIVES

**A. Engagements with Governments**

Consistent with the Ten Steps stated above, telcos will:

1. **Avoid restrictions on users' access, freedom of expression, or privacy.**

   a. Companies will assess the potential for restrictions on users' access, freedom of expression, or privacy in each operating environment in which they do or plan to do business. These assessments will follow a rights-respecting, public statement of policy approved by the senior leadership of the company.

      i. Such assessments will include engagement with local and international stakeholders; independent human rights experts; and internal or external counsel with specific knowledge of relevant local laws and regulatory requirements. The scope of such assessments will include a specific review of domestic legislation that may provide the basis for potential government requests seeking to restrict telecommunications services, access user data, and/or block content. This review will include an evaluation of:

         1. Whether relevant legislation is vague, overbroad, inadequate, or inaccessible to the public; and

         2. Whether the goals of the legislation are legitimate public purposes; and

         3. Whether the means proposed are necessary and proportionate to achieve the law's stated goals.

      ii. Companies will be as transparent as possible about the nature and scope of these assessments as well as their findings with regard to likely restrictions on users' access, freedom of expression, or privacy.

      iii. Through such assessments, companies will evaluate their capacity to avoid or limit the potential for such restrictions.

      iv. Companies should avoid pursuing business in operating environments in which users' access, freedom of expression, or privacy are subject to egregious restrictions inconsistent with international human rights law and the rule of law.

   b. Companies will seek to embed provisions consistent with respect for fundamental human rights into their operating licenses with governments and their contractual agreements with business partners, and will reject, for example, provisions enabling unrestricted "backdoor" authority to access the network.

      i. Companies will seek to renegotiate and renew any existing licenses or contractual agreements in accordance with this requirement.

   c. Companies will seek to ensure that provisions are included in operating licenses and

other contractual agreements to protect and maintain users' access to networks during times of emergency and crisis.

i. Companies will strictly limit the grounds upon which governments can exercise any existing "kill switch" authority, whether through legal authority or technical means, to shut down access to vital forms of electronic communications. Companies will reject any requests to restrict users' access to emergency services.

**2. It is imperative that all telcos conduct an evaluation of any government request for restrictions on users' access, freedom of expression, or privacy and respond in a way so as to best avoid or limit the expected impacts on users. Requests to filter for political, social, or conflict purposes, especially during moments of political turmoil, merit particular vigilance. The evaluation and response shall include the following steps:**

a. First, companies will scrutinize a government request to ensure that it is compliant with all relevant legal or regulatory requirements.

i. Companies will require that a government request: be submitted in writing; explain the legal basis for the request; and identify the official making the request by name and title. Companies will insist that each government request be based on a valid court order or warrant from a valid legal authority.

b. Second, companies will evaluate the potential to avoid or limit responses to government requests through unilateral or multi-stakeholder advocacy, negotiation, litigation, or ultimately direct resistance.

i. Companies will ensure that any restrictions requested by government authorities be consistent with international human rights laws and standards and the rule of law, and necessary and proportionate to achieve a clearly defined and legitimate public purpose, such as protecting the rights or reputation of others, national security, public order, and/or public health. [Note: these exceptions are strictly construed, require a showing of direct and immediate connection between the requested action and its purpose, and cannot be used to justify arbitrary or broad limitations on the right to freedom of expression].

c. Third, companies will then review the request in consultation with internal human rights experts and internal or external counsel with specific, relevant knowledge, and respond to the request as follows:

i. At all times, companies will narrowly interpret and enforce a government request in the least restrictive means and shortest duration possible so as to maximize the protection of users' access, freedom of expression, and privacy.

ii. If a government request is unclear in its scope, or the legal basis for the request is vague, companies will interpret such requests as narrowly as possible, seek clarification from government authorities, or use such vagueness as grounds for a legal challenge to the request.

iii. If a government request is inconsistent with local law, regulatory requirements, or contractual provisions, the request will be rejected.

iv. If a government request is consistent with local law, but inconsistent with international human rights law and/or made during a time of political turmoil, a company will take the following steps before determining the nature and scope of its response:

1. Conduct an evaluation of the human rights-related risks associated with responding to the request;

2. Conduct an evaluation of the legal and operational risks associated with resistance to the request; and

3. Utilize unilateral and multi-stakeholder advocacy to push back on the nature and/or scope of the request.

d. In genuine emergency situations, meaning a company has a good faith belief there exists a specific, credible threat to life or employee security, it may not be possible to follow all other steps in this Telco Action Plan. Companies will develop specific policies and review procedures to respond to government requests in these scenarios.

e. Companies will document and publish responses to government requests, to the extent that this is legally permitted, and will conduct regular reviews of these responses to ensure that all appropriate measures were taken to mitigate the actual or likely impacts on users.

i. In conducting such reviews, companies should also conduct periodic evaluations of the appropriateness of continuing to operate in specific environments in light of the overall nature and frequency of a government's requests and the company's capacity to respond to such requests in a responsible manner.

**3. Companies will refuse demands seeking to have the company serve as a "spokesperson" or "mouthpiece" for a government.**

a. Companies will refuse to deliver any communications to users on behalf of government authorities unless such communications are consistent with international human rights laws and standards, the rule of law, and necessary and proportionate to achieve a clearly defined and legitimate public purpose.

b. Companies may permit government use of a network for emergency instructions, or AMBER Alert-like messages, but will insist that all such messages be sent by the provider itself and be clearly attributed to the sender.

**4. Engage in unilateral and multi-stakeholder advocacy with the intent of limiting the legal or regulatory bases for restrictions on users' access, freedom of expression, and privacy.**

a. Companies will consult, formally and informally, with multiple stakeholders, including civil society and governments, in conducting such advocacy.

**B. Engagements with Users**

Consistent with the Ten Steps and section A above, telcos will respect the human rights of all users, and:

1. **Be as transparent as possible with users regarding any and all likely or actual restrictions on access, freedom of expression, and privacy.**

   a. As expeditiously and transparently as possible, companies will notify users of the imposition of restrictions on access, freedom of expression, and/or privacy. Such notifications will indicate whether restrictions were imposed in response to the request of government authorities and/or business partners. To the extent legally permitted, companies will also publish their responses to government requests, including the nature and scope of their internal reviews of such requests.

   b. Companies will notify users and relevant government authorities as expeditiously as possible in the event of a data breach or unauthorized processing of personal data.

   c. Companies will disclose the terms and conditions of their operating licenses to the maximum extent permitted by law.

   d. Companies will use clear, accessible, and accurate language to communicate terms of use, privacy policies, and other forms of user guidelines. Companies will translate terms of use and/or user guidelines into local languages.

   e. Companies will provide clear warnings to users who are subject to likely account deactivation or content removal, including references to communications channels by which users can respond to such warnings. Companies will ensure that their account-deactivation guidelines include intermediate steps, internal reviews, and escalation processes.

   f. Companies will use clear, accessible, and accurate language to communicate the features of services available to users (e.g. actual download/upload speeds).

2. **Provide users with appropriate and accessible channels to communicate questions, concerns, and grievances about terms of use, company policies, and/or restrictions on access, freedom of expression, and privacy.**

   a. As relevant, companies will provide users with the ability to appeal the imposition of specific restrictions on access, freedom of expression, and privacy. Companies will respond to such appeals as expeditiously as possible. Corporate review of such appeals will include consultation with internal experts with specific knowledge of the relevant human rights and legal context.

   b. Companies will review and improve the adequacy of these channels in consultation with relevant stakeholders, including a survey of users' awareness of such channels and the extent to which users feel that the company is responsive to their concerns.

3. **Treat all data traffic on an equitable basis no matter its origin, type, or content.**

a. Service providers will refrain from any interference with internet users' freedom to access content and use applications of their choice from any device of their choice, unless such interference is strictly necessary and proportionate to:

   i. Mitigate the consequences of congestion, while treating the same kinds of traffic in the same manner;

   ii. Safeguard the integrity and safety of the network, the service, or a terminal device of the user (e.g. blocking viruses and DDOS-traffic);

   iii. Block the delivery of unsolicited commercial messages (spam), but only if the subscriber has given prior consent;

   iv. Execute a legal statute or court order; or

   v. Comply with an explicit request from the subscriber, provided the subscriber may revoke the request without any increase in subscription fee at any time.

b. Companies will seek to provide as much control over traffic management and any filtering measures as possible to the users themselves.

**C. Integration of Human Rights into System Design and Implementation**

Consistent with the Ten Steps and sections A and B stated above, telcos will:

1. **Protect user privacy and security through the encryption and anonymization of user data, and the transmission of user data over encrypted channels, whenever and wherever possible.**

2. **Refrain from filtering internet technologies (e.g. VoIP services and circumvention software).**

3. **Collect as little data as possible from their users and retain such data for the shortest period permitted by law.**

4. **Commit to using spectrum allocations in each country in which they do business in as judicious and equitable a manner as possible.**

   a. Companies will share spectrum allocations to maximize the benefit to a country's inhabitants and to promote innovation and economic growth.

   b. Companies will sell or return at cost to country governments any unused spectrum.

5. **Where telcos are required by law to develop joint ventures, voluntarily partner with local companies, or acquire an ownership stake in a local company, these relationships must be subject to human rights impact assessment. The Telco Action Plan and the results of that assessment should inform how the partnership is structured, what provisions and conditions are built into the agreement, and the nature of the ongoing operations.**

# CASE STUDIES

**1. The Egyptian Network Shutdown**

On the evening of Thursday, January 27, 2011 — just two days after large-scale anti-government protests erupted across Egypt — officials in the beleaguered government of Hosni Mubarak ordered the operators of the country's main internet and mobile phone providers to "pull the plug" on their services. Egypt's four main ISPs (Telecom Egypt, Link Egypt, Vodafone/Raya, and Etisalat Misr) and its three main mobile phone companies (Vodafone Egypt, Mobinil, and Etisalat) promptly complied with this government order.

The new communications technologies that had played a key role in Egypt's democratic uprising fell silent across most of the country. None of the millions of ordinary Egyptians who relied on internet and mobile phone connectivity to organize, publicize, and stay safe during the protests received any advance warning of this communications blackout.

The next day, all three mobile phone operators issued brief statements explaining that they had suspended their services pursuant to a government order and that they had no choice but to comply under the terms of their license agreements (which they did not disclose to the public). The parent companies of Egypt's main ISPs do not seem to have issued a comparable statement.

On the morning of Saturday, January 29, the government of Hosni Mubarak reversed course and allowed the three mobile phone operators to reinstate voice services, but not SMS or data services. The government then forced the three mobile carriers to send out pro-government SMSs to subscribers. These messages did not explain who had written the SMSs or who had authorized their transmission.

None of the companies initially pushed back on these SMS requests, but following consultations with the U.S. and U.K. governments, Vodafone resisted a subsequent request and the government backed down from making any further requests. Mobile data and wired internet service was restored in Egypt on February 2 and SMS services were restored on February 5. President Mubarak finally resigned on February 11, 2011.

## *LESSONS LEARNED*

***Before the crisis***

- Prior to investing in Egypt, the telcos should have conducted due diligence on the human rights-related risks posed by operating in Egypt in consultation with local and international stakeholders, including independent human rights experts.
- Given that they decided to offer services in Egypt, the telcos should have reviewed their operating licenses to ensure respect for users' access, freedom of expression, and privacy. They should also have developed robust internal review processes to evaluate and respond to any potential government request that might adversely affect users' privacy, freedom of expression, and access to telecommunications services. Telcos should have advocated unilaterally or with other actors against the government's ability to shut down mobile phone and internet services or otherwise impede free expression.

### *During the crisis*

*Response to Government Requests*

- The telcos should have presumptively rejected any oral requests from the Egyptian government officials to shut down their networks and distribute pro-government SMSs. They should have demanded instead written orders from authorized government officials that included clear statements of the legal basis for the actions requested by the government.
- Following the receipt of written orders, the telcos should have evaluated the potential to avoid or limit compliance through unilateral advocacy, and with local actors like telcos, regional bodies like the Arab League, and relevant international stakeholders.
- As promptly as possible, telcos should have conducted an internal review, pursuant to pre-existing procedures.
  - › This review should have taken place before any decision was made on how, and if, to comply with the orders. This review process should have included consultation with internal human rights experts and internal and external counsel with specific knowledge of relevant local laws, regulatory requirements, and contractual provisions.
  - › Companies should have assessed whether the order was consistent with international human rights laws and standards and the rule of law, and necessary and proportionate to achieve a clearly defined and legitimate public purpose.
  - › After finding the order unnecessary to achieve its objective, disproportionate to the threat, and lacking a clearly defined and legitimate public purpose, the telcos should have evaluated the human rights-related risks of compliance as well as the costs of resistance.
- Based on the information we are privy to, Access believes companies should not have complied with government requests to restrict their users' access to information and networks and to distribute pro-government SMSs.
- Additionally, the potential risks to the security and lives of staff should have been carefully assessed, in accordance with the companies' existing policies and procedures for responding to emergency scenarios.
- Any form of compliance necessitated by specific, credible threats to employee security should have taken place in as strict a manner and for as short a duration as possible, with minimum infringement of human rights. Any request to shut down emergency services communications should have been absolutely denied.

*Communications to Users and the Public*

- The telcos should have made a concerted and good faith effort to provide customers with advance warning of the network shutdown. The telcos should have used all means of communication at their disposal to publicize the shutdown and explain their reasons for complying with the Egyptian government's orders (such as a good faith belief that the lives of employees were specifically threatened).

- The telcos should have resisted the government's attempt to use their networks for propaganda purposes. If resistance proved futile, the telcos should have insisted that the pro-government text messages be clearly attributed to the official(s) that demanded their transmission.

### *After the crisis*

- The telcos should be commended for shutting down their mobile phone and internet networks in a manner that allowed for the rapid restoration of service, and also for providing services free of charge at the height of the political turmoil in Egypt.
- In consultation with relevant stakeholders, the telcos should now evaluate their response to the demands of the former Egyptian government and leverage the lessons learned to remedy any deficiencies in their policies and procedures for responding to government requests — both in Egypt and in other countries in which they operate.
- The telcos should ensure that users impacted by the network shutdown have access to appropriate remedies, including company grievance mechanisms by which to seek any requested explanations, redress, or service modifications. Telcos should also advocate for the availability of public grievance mechanisms and remedies.
- Given their established relationship with the government after the Egyptian uprising, the telcos should advocate for a legal or regulatory environment that disallows "kill switch" or shutdown laws and orders.

## 2. The Pakistan Telecommunication Authority's List of Forbidden Words

On November 14, 2011, the Pakistan Telecommunication Authority — Pakistan's telecoms regulator — issued an order requiring the country's mobile phone operators to block SMS messages containing any one of 1695 words or phrases it deemed "offensive" or "derogatory." Companies were given a week to implement the directive, and were also ordered to submit monthly reports on the number of messages they were blocking pursuant to the order. Notably, the directive stated that a meeting had been held on October 18th to discuss the government's censorship plans with all mobile phone operators.

The PTA's announcement was met with dismay and widespread opposition from the public, the media, civil society groups, and Pakistan's telcos. The fact that the PTA's dragnet against "offensive" and "derogatory" words and phrases had caught up such benign expressions as "deposit," "joint," and "lotion" exposed the overbreadth of the PTA's directive under both Pakistani and international law.

The telcos espoused the interests of their customers in pointing out that the PTA's directive would make it practically impossible for customers to send SMS messages on a wide variety of perfectly innocuous subjects. What is more, the telcos strenuously objected to the short timeframe they had been given to implement the government's directive, especially given the technical complexity of doing so. Opposition from this broad coalition of opponents led the PTA to issue a "clarification" on November 21 explaining that its directive had been nothing more than "preliminary advice" to mobile phone operators.

The PTA has not given up on its plan to censor SMSs containing words it deems "offensive" or "derogatory," but it has announced that it will consult with civil society representatives and mobile phone operators to develop a shorter blacklist. Several lawyers and human rights advocates have already indicated that they will challenge the constitutionality of any such measure.

## LESSONS LEARNED

- The telcos should have informed all relevant stakeholders (including home country governments, domestic opposition figures, and domestic and international human rights activists) of the PTA's censorship plans as soon as they became aware of them.
- Upon receiving the censorship order, the telcos should have presumptively rejected it. Conducting human rights evaluations of the order, the telcos should have reviewed its necessity, proportionality and supposedly legitimate public purpose. Had the directive been imposed, the telcos should have pushed back against its implementation and immediately joined together in advocacy against the censorship. This approach appears to have achieved success to date.
- The telcos should be commended for working with counsel to submit comments on the PTA's censorship plans immediately after the October meeting. In the interests of transparency, however, the telcos should have disclosed such comments to the public.
- Telcos should have policies and procedures in place to continuously evaluate whether any restrictions a government has imposed or is planning to impose on the privacy, freedom of expression, and network access of its citizens are consistent with domestic and international law.
  - › The PTA's announcement at the October 18 meeting that it was considering instituting SMS censorship should have triggered these review processes.
  - › These internal policies and procedures should include consultation with internal human rights experts and internal or external counsel with specific knowledge of relevant local laws, regulatory requirements, and contractual provisions.
  - › These policies and procedures should also include consideration of the circumstances in which a telco will take legal action in support of the rights of its customers.
- Telcos should continue to engage in unilateral and multilateral advocacy to voice their principled and practical opposition to the PTA's plans to censor SMS messages as well as other Pakistani government efforts to restrict users' access, freedom of expression, and privacy.

*Access (AccessNow.org) is an international NGO that promotes open and secure access to the internet as a means of free, full, and safe participation in society and the realization of human rights.*

*The Telco Action Plan is an initiative of Access. We look forward to receiving further input into its development.*

*Access believes that telecommunications companies should join the Global Network Initiative, upon which this Telco Action Plan draws much of its inspiration, and be subject to assessment and evaluation of the implementation of its principles and implementation guidelines.*

*Access would like to acknowledge and thank our partners FairPensions and Foley Hoag LLP for their invaluable work in updating this document.*

*For more information, please visit www.accessnow.org or e-mail info@accessnow.org.*

*Released March 2012, slightly updated from the March 7 version.*