Access Comments to Draft Telecommunications Masterplan

Submitted 7 August 2015

Access (www.accessnow.org) is an international organization that defends and extends the digital rights of users at risk around the world. We have supported the development of telecommunications in Myanmar, and submitted a comment to the public consultation on the Code of Practice for Mobile Customer Registration. We also engaged with stakeholders from governments, private sector companies, and civil society at our March 2015 conference RightsCon Southeast Asia, held in Manila, Philippines.

Access has taken a leading role in monitoring and guiding the telecommunications sector's progress in realizing its human rights responsibilities. We reached out directly to the boards of major international telecom companies in 2011, after several complied with an order to shut down Egypt's internet and spread propaganda. Soon after, we produced the *Telco Action Plan*,[1] a foundation guide to help companies better prevent and mitigate their adverse impacts through high level policy commitments, human rights due diligence, and rights-respecting responses to government requests. We consulted with several companies, including Telenor (which operates in Myanmar) on the drafting of the Telecommunication Industry Dialogue's *Guiding Principles*.[2] We have since participated in multistakeholder institutions and events, and developed guidance on such topics as corporate reporting on privacy and free expression topics, and provision of meaningful access to remedy. Governments play an essential role in safeguarding and extending rights online, and with this comment we continue encouraging Myanmar's rollout of secure, affordable, and rights-respecting telecom services.

Access congratulates the MCIT on the thoughtful and concise Draft Telecommunications Masterplan. Below we make general suggestions as well as highlight particular sections of the document that merit further consideration and development.

- *2.2 Quality*
  The Regulator will stipulate minimum quality standards for data services, including connection quality, stability and speeds … The MCIT recognizes that operators must be given sufficient freedom to focus on building out services to connect Myanmar, and to not be subjected to an onerous quality regime. The phased approach above recognizes this by delaying the introduction of enforced penalties and providing sufficient time for operators and Regulator to develop their ability to track and measure performance. (page 20)

While we recognize the need for a phased approach to service provision, the Masterplan should make a clear commitment to network neutrality in Myanmar.

[1] https://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf
[2] http://www.telecomindustrydialogue.org/about/guiding-principles

The fundamental right to access information and ideas of all kinds on the internet depends on network neutrality. Net neutrality means that all traffic on the internet is treated on an equal basis, no matter the origin, type of content or means (e.g. equipment or protocols). It comprises three principles:

- First, the end to end principle, which ensures that all points in the network should be able to connect to all other points in the network.
- Second, the best effort principle which guarantees that all providers of the internet should make their best effort to deliver traffic from point to point as expeditiously as possible.
- Last but not least, the innovation without permission principle, which states that everyone should be able to innovate without permission from anyone or any entity.

These principles can be collectively defined as network neutrality, which is fundamental to ensure that the internet remains a platform for the enjoyment of human rights and innovation. Any deviation from this principle (for instance for traffic management purposes) must be proportionate, temporary, targeted, transparent, and in accordance with relevant laws. If these criteria are not respected, users then face network discrimination and growth of the internet economy slows.

- *2.5. Security*
  With the advent of data services and the proliferation of local and international connections, Security is critical to Myanmar's telecommunications industry. The Ministry is the responsible agency to implement the Government's requirements for security protocols within the telecommunications sector, and to ensure Myanmar keeps it networks secure from threats or service disruptions. (page 22)

The MCIT and Myanmar government as a whole should commit to ensuring internet connectivity without interruption or interference. Myanmar's citizens and businesses must be able to trust the infrastructure and administration of the internet in order to grow the marketplace of ideas and fully participate in the internet economy. The internet is the enabler of a host of human rights, beyond freedom of expression and association, and is being recognized as essential to attainment of the Sustainable Development Goals. Mobile health, e-learning, and modern banking all depend on stable, secure, and efficient networks.

In this context, so-called "kill switches" or other measures whereby governments disrupt and intentionally interfere with internet service provision not only impede the positive benefits of the internet and the general trust of users, but also explicitly violate human rights standards as increasingly articulated in international law. For example, UN and regional Special Rapporteurs recently issued a Joint Declaration on Freedom of Expression and Responses to Conflict Situations finding that:

> Filtering of content on the Internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law.[3]

Frank La Rue, the previous Special Rapporteur on the freedoms of opinion and expression, likewise found that internet shutdowns pose a disproportionate interference with the right to freedom of expression.[4]

We recommend that Myanmar government declare that it will not require installation of or implement any "kill switch" or other technology to shut down communications networks, for any reason.

- *Once the policy has been created by the Union Government, the MCIT will play a key role in implementation of the national cyber security policy and in applying standards for legal interception of telecommunications networks. With external assistance from the Council of Europe and local consultation, MCIT is exploring the options for developing the appropriate protocols for legal interception which are in line with leading international practices. (page 23)*

The document states that the new cyber security policy will appear in 2016. We ask you to clarify dates for launch of the consultation in order to begin preparations. We also ask that, as a general rule, you extend any public consultation period to no less than one full month from the date of the draft or proposed rule's publication.

- *"Grey traffic," that is traffic which passes through unlicensed operators, can compromise security as traffic into the country does not pass through licensed infrastructure. Such services can be difficult to detect. International Gateway liberalization which results in lower international tariffs will likely contain grey traffic that comes into Myanmar today. Reduction of such unlicensed services will limit telecommunications network security hazards in Myanmar as traffic will pass through licensed channels which can be subject to interception. (page 23)*

The reference to interception raises questions. What is the purpose of the interception of traffic through licensed channels, as referenced in this section?

Lawful intercept policy should not be used to impede the growth of new technology. The regime for lawful intercept should be based on the 13 Principles on the Application of Human Rights to

---

[3] https://www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation

[4] http://www2.ohchr.org/English/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.PDF

Communications Surveillance[5] and the specific suggestions in the *Implementation Guide*[6] to those Principles.

- *3.3 Consumer rights*
  MCIT has requested the Regulator to ensure that consumer complaints are handled in a fair, timely and responsive manner, firstly by service providers and where necessary with the intervention of an additional dispute resolution mechanism to be established by the Regulator. The Regulator is to formalize its plans for managing this as part of its overall institutional development plan to be prepared by the end of 2015. (page 27)

This dispute resolution mechanism could be a good tool for users. We might suggest that the wording should be "access to remedy" as per international norms recognized by the UN Guiding Principles on Business and Human Rights. The Regulator should adhere to this guidance, in particular Principles 27 through 31 and the seven “effectiveness criteria.” According to Principle 31, non-judicial grievance mechanisms should be: legitimate, accessible, predictable, equitable, transparent, rights-compatible, and a source of continuous learning.

In addition, the Regulator could counsel service providers on best practices in delivering access to effective remedy. These range from simple steps, such as clearly, publicly identifying corporate officials in charge of every project and providing contact information, to engaging in multi-stakeholder entities like the Global Network Initiative. All personnel handling complaints should be trained to recognize and expedite any request implicating human rights impacts. Access has synthesized guidance on non-judicial remedy in the ICT sector in our paper, *Forgotten Pillar: The Telco Remedy Plan*.[7]

- *Matters related to data privacy are outside the purview of the sector Ministry and will be handled elsewhere in Government, as a common issue to apply across consumers in all industries and sectors. (page 27)*

To ensure the common application of the rights to privacy and data protection across sectors, telecom companies must act as responsible players when it comes to the data of their users. In that respect, Access promotes the *Telco Action Plan* and its guidance, including that all telecom companies operate under a high-level human rights policy, approved by senior leadership. At the moment, not all telecom companies operating in Myanmar have taken this essential first step. We believe the Myanmar government can play a key role in securing such commitments and encouraging implementation by telcos, thereby fostering a more rights-respecting ecosystem where user trust is safeguarded.

In addition to safeguarding individual rights, privacy and data protection frameworks also facilitate and enhance a more predictable and stable investment environment. Given the

[5] https://en.necessaryandproportionate.org/text
[6] https://www.accessnow.org/page/-/Implementation%20Guide%20International%20Principles%202015.pdf
[7] https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_0nm6ii982.pdf

government's stated intention to create an environment amenable to innovation (4.1 Competitive market, responsible business), privacy protections must be clear, accessible, and based on international law and norms.

Per international human rights norms, summarized in the 13 Principles on the Application of Human Rights to Communications Surveillance, communications surveillance should be only be permitted insofar as it:

- achieves a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society;
- is strictly and demonstrably necessary to achieve that legitimate aim;
- is in response or anticipation of a serious crime, and other less invasive investigation techniques have been exhausted;
- is only authorized by a competent judicial authority, and not the agency conducting the surveillance; and
- is monitored by independent oversight mechanisms.

Governments should release data on the number of surveillance requests approved and rejected and allow companies to do the same.

More steps to align Myanmar policy and practice with international standards are found in the Access *Implementation Guide* to the 13 Principles on the Application of Human Rights to Communications Surveillance. Additionally, appended as Attachment A is the *Lawful Interception Policy and Myanmar* document, a brief reference guide to resources and standards that apply in the area of lawful intercept and human rights.

- *Security: MCIT will set policy for information and cyber security, and will be the implementing agency within Government for such programs. This will include the implementation of the Government's requirements for legal intercept of telecommunications networks. The Ministry will need to build a specialist unit to take forward the security program, consisting of engineers, IT specialists, lawyers and professionals with surveillance and forensics expertise. (Page 32)*

MCIT should also include human rights experts and civil society so as to better ensure protection of users' rights.

Conclusion

Thank you for this opportunity to contribute to the development of this important regulatory and policy framework in Myanmar. We will continue to offer our insights and attention, in tandem with our civil society partners, as this process continues.

***

Access (www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, contact:
Peter Micek
Senior Policy Counsel
Access
peter@accessnow.org | +1-888-414-0100

ATTACHMENT A:

Lawful Interception Policy and Myanmar Reference Guide

Lawful Interception Policy and Myanmar - Reference Guide

This document is meant to provide background and guidance to stakeholders interested in influencing the formulation of State policy on lawful interception of communications in Myanmar. It contains information on the existing international and national legal frameworks governing the protection of user privacy, an overview of related human rights risks for users, and best practices for telecommunications companies operating in Myanmar. In this guide we use terminology created for the Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance. Access appreciates this opportunity to support the work our partners in Myanmar and Southeast Asia.

I. An introduction to Lawful Interception and current policy discussions in Myanmar

A. What is Lawful Interception?

a. Lawful Interception (LI) occurs where the government gains real-time access to communications information and/or content, typically without the knowledge of the user. Most countries require telecommunications companies to maintain the capacity for LI, and to allow access by law enforcement and other government agencies in cases that ostensibly implicate public safety or national security.
b. Several standard architectures exist to allow for LI. These all aim to create structures for interaction between network operators and agencies authorized to intercept communications. The interception is not limited to telephone calls, it can extend to data transferred, including Voice over Internet Protocol (VoIP), and Short Message Service (SMS). Interception can be targeted with Internet Protocol (IP) traffic of interest, type of IP traffic, location data, etcetera, identified by the authorized agency. Common examples are standards developed by the European Telecommunications Standards Institute (ETSI) and the Communications Assistance for Law Enforcement Act (CALEA) in the United States

B. What are the possible impacts of government practices or laws regarding Lawful Interception?

a. Interception of communications interferes directly with the rights to privacy and freedom of expression, and indirectly with the exercise of many other human rights. With the technological capacity and legal framework supporting interception, there is a risk that the State will misuse its power and private actors will abuse the mechanism and violate the right to privacy.

b. Overbroad surveillance and other practices affecting the privacy and personal rights of individuals can lead to a multitude of harms, including arbitrary detention and persecution, harassment, and fraud, and chill the exercise of the rights to freedom of expression and association.

c. The risk of arbitrary application of the communications intercept capability is high in situations where police forces and government agencies have previously conducted close surveillance of citizens - making the issue even more important to citizens of Myanmar given its history and the ongoing efforts to expand democracy. Strict rules and comprehensive oversight are required - in line with the human rights guidance below - and it is of special importance to ensure that individuals are afforded notice of surveillance and meaningful opportunity to challenge it before courts.

d. Without clear laws, vital information and data pertaining to everyday activity of citizens across Myanmar could be at the risk of access by others without proper oversight. This could include: their physical location when using their phones or other communication devices; the contents of their text messages, instant messaging, or email; and the details of the people they speak to or their very calls themselves

C. What is the current situation in Myanmar regarding interception of communications and the regulatory environment regarding telecom surveillance?

a. A new Telecommunications Law was passed in 2013, replacing the Telegraph Act of 1885, with extensive inputs from several stakeholders.

b. The Telecommunications Law put in place provisions regarding powers of the Myanmar Government to obtain access to telecom resources or otherwise seek to intercept communication (Article 75 - 77 of the law).

However, the regulations and standards for this were not set in place, and have yet to be framed.

D. What is the process for developing Myanmar's lawful intercept policy?

a. The Myanmar Ministry of Communications and Information Technology (MCIT) is currently working with international partners, including the World Bank, to develop the implementing regulations to the Telecommunications Law (2013). As with previously proposed rules for licensing, access and interconnection, spectrum, numbering, and competition, the MCIT is likely to invite public comment on the draft LI policy.

b. Once the MCIT receives informed feedback from diverse stakeholder groups, it should respond to the needs and concerns of its citizens with regard to the protection of user-identifying information and the privacy of communications.

II. State law and guidance on Lawful Interception

There is a growing body of guidance for States, anchored in international human rights law, for the formulation of safe and equitable telecommunications policy. The LI policy implemented by MCIT should adhere to these standards.

A. International Principles on the Application of Human Rights to Communications Surveillance ["13 Principles"]
   a. Communications surveillance should be only be permitted insofar as it: "achieve[s] a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society"; is "strictly and demonstrably necessary" to achieve that legitimate aim; is in response or anticipation of a serious crime, and other less invasive investigation techniques have been exhausted; is only authorized by a "competent judicial authority," and not the agency conducting the surveillance; and monitored by independent oversight mechanisms. Governments should release data on the number of surveillance requests approved and rejected and allow companies to do the same.

   b. The full list of these 13 Principles include
      i. Legality
      ii. Legitimate Aim
      iii. Necessity
      iv. Adequacy
      v. Proportionality
      vi. Competent Judicial Authority
      vii. Due Process

viii. User Notification
ix. Transparency
x. Public Oversight
xi. Integrity of Communication
xii. Safeguards for International Cooperation
xiii. Safeguards against Illegitimate Access and Right to Effective Remedy

B. Access has elaborated how to apply the 13 Principles in practice in our detailed *Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance*.
   a. **Based on the Implementation Guide, any Request for interception must be**:
      i. Based on publicly available, discernable law;
      ii. Applicable to only a single Target;
      iii. Narrowly tailored to minimize the impact on Protected Information;
      iv. Written and signed by a Government Agent and approved by an independent and competent Judicial Authority, who evaluates the request based on both the content and the sufficiency;
      v. Describe the Account, Device, or Repository subject to Communications Surveillance, the Necessary Information sought, any Protected Information that may be incidentally accessed, the methodology to be used, and the specific timetable for the Communications Surveillance;
      vi. Establish that the Necessary Information sought is contained in the Account, Device, or Repository identified for Communications Surveillance;
      vii. Demonstrates a sufficient nexus between the Account, Device, or Repository to be subject to Communications Surveillance and the Necessary Information sought;
      viii. Where emergency procedures are used, a formal application is filed within 24-72 hours after the initiation of the Search.

   b. **A Court Order is required for any interception**. The Court Order must be:
      i. Issued and signed by an impartial, competent, and independent Judicial Authority;
      ii. Pursuant to public and transparent proceedings;
      iii. Based on credible, lawfully acquired information;
      iv. In writing, identifying all underlying legal authorities and with the request attached;
      v. Describes the full scope of the authorisation, including the Accounts, Devices, or Repositories to be subject to Communications Surveillance, as well as the scope, timeline, and methodology for the Communications Surveillance;
      vi. Narrowed to ensure minimal incidental access to Protected Information;

vii. Limits the retention time for all Protected Information to a reasonable time, not to outlast the resolution of the Legitimate Aim of the Communications Surveillance;
viii. Includes a written opinion explaining the issues and the rationale for the decision in all cases of novel or unique factual or legal issues.

C. UN Special Rapporteur on Freedom of Opinion and Expression – Report on Surveillance of Communications
   a. "Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State";
   b. "Legal frameworks must ensure that communications surveillance measures: (a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application; (b) Are strictly and demonstrably necessary to achieve a legitimate aim; and (c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted."

D. UN Special Rapporteur on Freedom of Opinion and Expression – Report on Freedom of Expression and Opinion on the Internet
   a. States must "ensur[e] that any measure to limit the right to privacy is taken on the basis of a specific decision by a State authority expressly empowered by law to do so, and must respect the principles of necessity and proportionality."

E. UN Special Rapporteur on Freedom of Opinion and Expression – Report on the Use of Encryption and Anonymity in Digital Communications
   a. "Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective."

F. Budapest Convention on Cybercrime
   a. States should implement conditions and safeguards protecting human rights, including "judicial and other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure."

III. Relevant Myanmar legal provisions

A. Telecommunications Law, Arts. 75-77
   a. "To obtain any information or communications that may adversely affect the security of the State, the rule of law and order, the Union Government may direct the relevant organizations as necessary without infringing upon the original rights of the citizens.
   b. The Ministry or the department/organization assigned by it may, for defense and security matters of the State or for the public interest, if necessary, may enter into the premises of the licensed telecommunication services provider and inspect, supervise and request the licensee to submit records regarding the services.
   c. The Ministry may, when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to suspend the telecommunications service provider business, prohibit a specific type of communication, to block and hold, to retrieve necessary information and communications, to temporarily control and use the telecommunications service provider businesses and telecommunications equipment."

IV. Policy guidance for telecommunications companies

While the State is responsible to drafting and applying LI law and policy, telecommunications companies must develop consistent and transparent policies for responding to State LI requests.

A. Access Telco Action Plan
   a. 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].

B. Access Telco Remedy Plan
   a. Investigate and cease or alter activities that contribute to adverse human rights impacts in an effective, timely manner.
   b. Interview executives and staff overseeing and conducting those rights-infringing activities, and review relevant policies. Clarify whether staff deviated from policy or the policy itself failed. To minimize risks of repetition, revise policies, retrain staff, and communicate policy changes to personnel, business partners, and the public.

c. Preserve evidence wherever possible and publish when appropriate, particularly when obstacles make providing access to effective remedy impossible in the near-term. In cases where the state instigated the telco's rights-infringing activities, evidence can inform a victim's search for effective remedy, especially where states deny their role in unlawful surveillance, censorship, or network interference.

C. Access Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance
   a. Providers must only supply protected information in response to a Request for search, supported by a valid court order. Where it appears that a request for search does not comply with the 13 Principles and/or international human rights law obligations, providers should demand further explanation and, where appropriate, challenge the legality of the request.

D. Institute for Human Rights and Business Digital Dangers Project
   a. Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems Institute for Human Rights and Business
   b. "Technical strategies form only some of the mitigation steps that a company should undertake to prevent misuse of its technologies. Also critical is training for network operators in correct use of equipment and in ensuring that customers effectively implement technical and security strategies."
   c. "Regulators need to clarify the capabilities and the uses of technology that comprise lawful interception and also the limits of lawful surveillance."

E. Telecommunications Industry Dialogue Guiding Principles
   a. Many telecom companies operating members of this group - including Telenor which operates in Myanmar - and have committed to its Guiding Principles.
   b. These principles include
      i. Policy commitment
      ii. Raising awareness and training
      iii. Impact assessment and due diligence
      iv. Sharing knowledge Process (to handle and anticipate government requests)
      v. External reporting
      vi. Mitigating risks of governmental demands
      vii. Informing policy and regulations on freedom of expression and privacy
      viii. Employee safety and liberty Grievance mechanisms
   c. The guiding principles have been translated for Myanmar and made available by the group.

F. GSM Association (GSMA) guidance on government access

a. “Any interference with the right to privacy of telecommunications customers must be in accordance with the law;
b. The interception of communications for law enforcement or security purposes should take place only under a clear legal framework and using the proper process and authorisation specified by that framework;
c. There should be a legal process available to telecommunications providers to challenge requests which they believe to be outside the scope of the relevant law(s);
d. The framework should be transparent, proportionate, justified and compatible with human rights principles, including obligations under applicable international human rights conventions, such as the International Convention on Civil and Political Rights;
e. Governments should provide appropriate limitations of liability or indemnify telecommunications providers against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of communications and data; and
f. The costs of complying with all laws covering the interception of communications, and the retention and disclosure of data should be borne by governments. Such costs and the basis for their calculation should be agreed in advance.”

***

Access defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For More Information
Contact: Peter Micek
Senior Policy Counsel, Access
1-888-414-0100 x709
peter@accessnow.org
Twitter: @lawyerpants

Visit: accessnow.org