



هيئة تنظيم الاتصالات  
Telecommunications Regulatory Authority

## Consultation Report

Responses received in relation to the  
consultation document on a draft regulation  
regarding Lawful Access

24 December 2009

**Purpose:** To report on the responses received to the consultation document and determine the final form of the draft regulation's articles

## 1 Introduction

- 1.1 In February of 2009 the Telecommunications Regulatory Authority (“TRA”) published a consultation document concerning a draft regulation requiring licensees to provide technical resources to achieve the requirements of national security (the “Draft Regulation”) (reference TOD/ICT/0209/003). This document summarizes the responses received in relation to the Regulation and provides TRA’s views and final position on the issues raised by the respondents.
- 1.2 TRA received responses from (listed alphabetically):
  - 1.2.1 Ahmed Bin Hindi (Bahrain Communications Users Association – Under Formation – Special Interest Group)
  - 1.2.2 Ahmed Zainal (Consumer)
  - 1.2.3 Amna Murtaza (Consumer)
  - 1.2.4 Arab Banking Corporation B.S.C. (Consumer/Interested Party)
  - 1.2.5 Consumer Advisory Group (Special Interest Group)
  - 1.2.6 ETI Connect (Lawful Intercept Consultancy Firm)
  - 1.2.7 Farida Ismail (Consumer)
  - 1.2.8 Fatima Bader Al Thakher (Consumer)
  - 1.2.9 Hafedh Ali (Submitted on behalf of the Political Office of the National Democratic Action Society “Wa’ad”)
  - 1.2.10 Hamed Mohamed Abulfatih (Consumer)
  - 1.2.11 Jalal Fairouz (Member of Parliament)
  - 1.2.12 Jameel Alalawi, Dr. (Consumer)
  - 1.2.13 Kulacom (Licensed Operator)
  - 1.2.14 Life Telecom (Licensed Operator)
  - 1.2.15 Lightspeed Communications (Licensed Operator)
  - 1.2.16 Mena Telecom (Licensed Operator)
  - 1.2.17 Nuetel (Licensed Operator)
  - 1.2.18 Waleed (Consumer)
  - 1.2.19 Yuri Volkov, PhD Information Law (Interested Party)
  - 1.2.20 Zain Bahrain (Licensed Operator)
- 1.3 TRA additionally received several confidential responses. Having reviewed all confidential responses, TRA agrees to uphold confidentiality, and as such, those responses will not be disclosed. They will be taken into account and addressed below as far as possible without breaching confidentiality restrictions.
- 1.4 The structure of this report generally follows the layout of the draft Regulation, addressing responses received to each section/provision in order. General comments that are not directed at a specific section of the Regulation will be addressed first.

## CONSULTATION REPORT

- 1.5 Comments and suggestions made by interested parties that do not fall in the above categories (i.e. general or article-specific) will be addressed last.

## 2 General Comments

- 2.1 General comments were made by several interested parties (i.e. comments that do not directly address one or more articles of the proposed Regulation) – these can be summarized as either for or against the Regulation

### ***General Comments against the Regulation***

- 2.2 The parties against the Regulation considered that:
- 2.2.1 There will be a violation of constitutional rights as a direct result of the Regulation
  - 2.2.2 TRA may be infringing the privacy of individuals within the Kingdom of Bahrain
  - 2.2.3 The Government would be eavesdropping on personal communications of citizens and residents
  - 2.2.4 Individuals working within Licensed Operators may divulge confidential information of consumers
  - 2.2.5 The Regulation is purely motivated by political and intelligence reasons
  - 2.2.6 The rights of individuals must be respected within the confines of the Constitution
  - 2.2.7 Having joined the International Covenant on Economic, Social and Cultural Rights, Bahrain may not issue this Regulation
  - 2.2.8 TRA is trying to increase its remit by issuing this Regulation, and is not concerned with the wellbeing of residents of Bahrain

### ***General Comments in support of the Regulation***

- 2.3 The parties supporting the Regulation considered that:
- 2.3.1 It is in the national interest to mandate such a Regulation
  - 2.3.2 The general safety of the Kingdom will be improved as a direct result of the Regulation

### ***TRA's general position on, and clarifications to, the comments made***

- 2.4 TRA thanks all the interested parties for their responses to the Regulation.
- 2.5 It is critical to note that the constitutional rights of individuals, as they relate to the privacy of communications, are guaranteed and protected in a number of different laws, including the Constitution of the Kingdom of Bahrain, the Telecommunications Law, the Criminal Procedures Law, and the Law on Protecting Society from Terrorism.

## CONSULTATION REPORT

- 2.6 Article 26 of the Constitution of the Kingdom of Bahrain states that “The freedom of postal, telegraphic, telephonic and electronic communication is safeguarded and its confidentiality is guaranteed. Communications shall not be censored or their confidentiality breached except in exigencies specified by law and in accordance with procedures and under guarantees prescribed by law”.
- 2.7 Article 30(a) of the Constitution of the Kingdom of Bahrain states that “Peace is the objective of the State. The safety of the nation is part of the safety of the Arab homeland as a whole, and its defence is a sacred duty of every citizen.”
- 2.8 It is therefore clear that the right to freedom of communications must be balanced against the duty to maintain the safety and integrity of the Kingdom of Bahrain for all its citizens.
- 2.9 The provisions of article 78 of the Telecommunications Law, under which the Draft Regulation is prepared, places a responsibility upon Licensed Operators to provide, at their own cost, all their Telecommunications Equipment, systems and programs relating to their Telecommunications Networks which allow security organs of the Kingdom of Bahrain access to their networks for fulfilling the requirements of national security. The security organs are still subject to the requirements of the law of the Kingdom of Bahrain, and the Constitution. As such, before a body can “tap” or otherwise disclose the secrecy of a communication or data relating to the contents of any message, its sender or receiver, article 75(2) of the Telecommunications Law requires permission from the Public Prosecutor’s Office or an order issued by an appropriate court. Breaching this requirement for permission shall be punished by a criminal fine of up to BD 10,000.
- 2.10 It is therefore incorrect to suggest that all citizens will be monitored and there will no longer be any privacy in communications. This is neither practical, nor achievable in the technical sense. As can be seen above, it is also not envisaged by the Constitution of the Kingdom of Bahrain nor the Kingdom’s laws. There are clear prohibitions against and punishments for illegally tapping into or disclosing the secrecy of communications.
- 2.11 As stated at paragraph 2.9 above article 78 of the Telecommunications Law requires TRA to issue regulations and resolutions to enable access for purposes of national security. With the growing number of Licensees within the Kingdom of Bahrain, a regulation is required to implement the technical requirements of national security in a uniform manner across all Licensees, and provide visibility to telecommunications users as to the method by which their information will be stored, retrieved, and destroyed.

## CONSULTATION REPORT

- 2.12 As there is common confusion amongst respondents in the difference between Call Content and Access Related Information, a simple analysis may be useful. In the context of postal mail (normal letters), the written letter itself is considered Call Content (which is neither stored nor accessed by Licensees), and the envelope of the letter is Access Related Information (sender, addressee, timestamps, etc.).
- 2.13 TRA has closely examined the International Covenant on Economic, Social and Cultural Rights for its relevance to the Regulation and found no relevant provisions that address privacy of communications. The aforementioned covenant will therefore not be considered in TRA's final position. TRA notes that article 19 of the Universal Declaration of Human Rights states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". TRA considers that article 26 of the Constitution of the Kingdom of Bahrain is consistent with this declaration, and therefore that the draft Regulation is also consistent with it.

### 3 Comments to the Articles of the Regulation

#### 3.1 Article 3 (Definitions)

##### 3.1.1 *Access Capability Plan (ACP) – Comments Received*

- 3.1.1.1 Not all products and services are planned and launched within a 6-month cycle; some take considerably less, others may take longer
- 3.1.1.2 TRA should consider removing the reporting requirement of the ACP and place the risk of compliance on Licensees. Licensees would then retrospectively report on products and services launched and their compliance with the regulation
- 3.1.1.3 Licensees should launch products first and then consider providing the technical requirements to support the Regulation's requirements
- 3.1.1.4 The 6-month cycle places an administrative burden on smaller operators that is translated into additional financial requirements
- 3.1.1.5 The ACP should be produced only if there are changes in technology; for example, GSM and 3G have existed for a number of years and have not changed

## CONSULTATION REPORT

### 3.1.2 *Access Capability Plan (ACP) – TRA’s Position*

- 3.1.2.1 The primary objective of the ACP is to ensure that operators have taken into account the requirements of the Regulation before rolling out *new* products and services, or *significantly changing* existing products and services.
- 3.1.2.2 The emphasis is upon the capability of a Licensee to support the requirements of national security – whether by using existing facilities and equipment or by making new investments in such assets.
- 3.1.2.3 If a new service to be introduced by a Licensee is significantly different (for purposes of Lawful Access, Data Retention, etc.) in terms of its technical description, then the Licensee must produce an ACP and have the same service subject to approval. The objective is to ensure that all Lawful Access functions, Data Retention functions, and other functions, are not interrupted, circumvented, or otherwise rendered ineffective.
- 3.1.2.4 By being significantly different, a service is fundamentally dissimilar to other services currently being provided by a given Licensee (e.g. a Licensee that is primarily offering international voice calls via prepaid cards intends to provide Internet services using fixed lines), or is being provided in a fundamentally different way (e.g. an ISP that is providing access to the Internet via USB-based HSPA devices is going to provide Internet access using fixed lines through Digital Subscriber Lines Access Multiplexers).
- 3.1.2.5 In light of the comments received, TRA considers that the primary consideration related to the ACP is the potential limitation to product development, innovation, and time-to-market. On balance, TRA considers that removing the 6-month cycle of the ACP and replacing it with an alternative method of reporting is required.
- 3.1.2.6 As such, the ACP requirements (and definition) will be changed so that a Licensee will produce an ACP whenever necessary, but always before a product or service is rolled-out. Approval time for ACP’s will be shortened to 14 days only.
- 3.1.2.7 In order to encourage innovation in telecommunications service development and deployment, and in line with Article 78 of the Law, special care will be granted towards new services that may not readily have a Lawful Access solution currently available in the global market. In such instances, TRA will review (along with security organs) the level of risk that may be inherent in each instance and will approve ACP’s accordingly

### 3.1.3 *Access Implementation Plan (AIP) – Comments Received*

## CONSULTATION REPORT

- 3.1.3.1 Coordination should be carried out only between operators and TRA.
- 3.1.3.2 TRA is best suited to evaluate the requirements of all the involved stakeholders (consumers, operators, and security agencies), and as such, TRA should be involved in all aspects of the AIP
- 3.1.4 *Access Implementation Plan (AIP) – TRA’s Position*
  - 3.1.4.1 TRA’s initially proposed role was that of a coordinator – passing AIP’s to and from security agencies. This would have entrusted TRA with only acting as a central point of contact.
  - 3.1.4.2 Having considered the concerns above, TRA will process and review all AIP’s based on a previously agreed minimum set of requirements (as agreed with concerned security organs).
- 3.1.5 *Access Related Information (ARI) – Comments Received*
  - 3.1.5.1 The definition of ARI reads “... Call Content ... can only be accessed or retained through Lawful Access procedures set forth below”
  - 3.1.5.2 Website addresses should not be considered ARI since the Licensee is providing access to the Internet and is generally not concerned with websites visited by subscribers.
  - 3.1.5.3 The volume of ARI to be recorded is significant.
- 3.1.6 *Access Related Information (ARI) – TRA’s Position*
  - 3.1.6.1 TRA acknowledges that merely stating that Call Content can be *accessed* or *retained* is inconsistent with the definition of Call Content and the overall objectives of the Regulation, and may be misconstrued as indirectly allowing access to Call Content.
  - 3.1.6.2 TRA reaffirms that Call Content may not be accessed or retained under the auspices of the Regulation. Any operator accessing or retaining Call Content is in violation of the Constitution, the Telecommunications Law, and other applicable laws.
  - 3.1.6.3 Call Content is accessed only by security organs for purposes of fulfilling the requirements of national security, after having followed due process

## CONSULTATION REPORT

- 3.1.6.4 ARI of website access and ISP services is vital for purposes of investigating crime, and must be accessible by security organs. Therefore ARI is to be retained, but may not be accessed by Licensees except for billing purposes.
- 3.1.6.5 Recent advances in technology enable Licensees to procure significant amounts of storage capacity at relatively inexpensive prices (when examining average US \$ cost per Terabyte of storage<sup>1</sup>). Nevertheless, the requirement to retain information for a period of up to 3 years will utilize a significant amount of electronic storage space.
- 3.1.6.6 TRA additionally considers that stating a fixed term, as opposed to the originally proposed 1-3 years period, is appropriate in this instance. A uniform fixed term will make it easier for consumers to understand how long their data is stored with any Licensee.
- 3.1.6.7 The period to hold ARI will be changed to a fixed term of 12 months only. After such a time, Licensees will be required to destroy expired ARI (exceptions are listed within the Regulation).

### 3.1.7 *Lawful Access – Comments Received*

- 3.1.7.1 The definition of Lawful Access reads “*provision of access to the traffic...*”
- 3.1.7.2 The concept of “traffic” is undefined, and it is only used in the definition of Lawful Access. This could arguably lead to the understanding that access to “traffic” would encompass access to both ARI and Call Content.
- 3.1.7.3 The resources, equipment, systems and programs relate to the Licensee’s licensed network, not another public or private network or public or private equipment which connects to a given operator’s network, and as such, the obligations only relate to a given operator’s licensed services.
- 3.1.7.4 Further, it is the security organs who fulfill national security requirements, not the Licensee – who provides the support and access (i.e. operators should only bear the costs associated with their own networks, systems, equipment, etc.)
- 3.1.7.5 The requirements under the Law only relate to Lawful Access, not data retention or CLI requirements

### 3.1.8 *Lawful Access – TRA’s Position*

---

<sup>1</sup> See *Computer Economics* and *Monash University* for more information.

## CONSULTATION REPORT

- 3.1.8.1 TRA accepts the argument that the term “traffic” is undefined and may lead to ambiguity in the interpretation of the concept of Lawful Access
- 3.1.8.2 However, it is important to differentiate between the concepts of Lawful Access and Data Retention. Lawful Access is concerned with access to communications data (i.e. Call Content) for example for the purposes of tracking suspects using telecommunications equipment and facilities, while Data Retention is concerned with storing key pieces of information for purposes of supporting post-crime investigation procedures
- 3.1.8.3 As such, Lawful Access describes the access of duly authorized security organs to Call Content, and is not related to Data Retention
- 3.1.8.4 The definition of Lawful Access will therefore be updated to replace the term “traffic” with the term “Call Content” so that the definition will read *“provision of access to the Call Content sent via...”*
- 3.1.8.5 All instances of the term “traffic” will be removed as much as possible from the Regulation and replaced with more descriptive, well-defined, terms
- 3.1.8.6 Article 78 of the Law<sup>2</sup> is concerned with ensuring Licensees provide the necessary technical resources (using the term loosely to signify all technical resources) to fulfill the requirements of national security
- 3.1.8.7 The fulfillment of national security requirements is achieved via providing access (using the above mentioned technical resources) to a Licensee’s network. The mere readiness or capability to provide access does not fulfill the requirements of national security as no access can be made at this point.
- 3.1.8.8 The same Article states that technical resources deployed by Licensees must allow security organs access to their networks for purposes of Lawful Access. Without a fully integrated Lawful Access architecture, security organs cannot access a Licensee’s network.
- 3.1.8.9 As the article refers to “security organs” the article requires support to multiple security organs (not only one).
- 3.1.8.10 TRA is therefore of the view that Licensees must provide, at their own expense, all the necessary Lawful Access technical resources and assets as required by the Law.

---

<sup>2</sup> The original Arabic version of the Telecommunications Law is being used without reliance upon the English translation

## CONSULTATION REPORT

- 3.1.8.11 Regarding the matter of Data Retention and CLI being irrelevant to Article 78, security organs must have access to sufficient information to fulfill the requirements of national security. A death threat or a bomb threat made by a caller with no CLI hampers the efforts of security organs<sup>3</sup>. By the same token, it is necessary to retain a reasonable amount of ARI should such data be required as evidence in a court of law.
- 3.1.8.12 As the retention of data and the delivery of CLI may be required for the purposes of national security of the Kingdom of Bahrain, TRA considers that the inclusion of these concepts in the Regulation is directly within the remit of article 78 and will therefore remain.<sup>4</sup>.

### 3.1.9 *Call – Comments Received*

- 3.1.9.1 Based on the definition of a “Call”, any attempt to make a Call will generate a certain amount of data, irrespective of the success or otherwise of the attempt. This in turn means that any Call attempt will generate ARI that has to be retained.
- 3.1.9.2 An attempted Call may be entirely successful (connected and answered, after which Call Content is transmitted), partially successful (connected but not answered), or entirely unsuccessful (not connected).
- 3.1.9.3 There seems to be no need to retain ARI for entirely unsuccessful Calls

### 3.1.10 *Call – TRA’s Position*

- 3.1.10.1 TRA agrees that ARI resulting from entirely unsuccessful Calls should not be retained.
- 3.1.10.2 However, TRA is of the view that the definition of a Call in the Regulation (“communications conveying voice or data”) is reflective of entirely successful and partially successful calls, as a communication that does not convey voice or data does not qualify for the definition (entirely unsuccessful Calls do not convey neither voice nor data)
- 3.1.10.3 For the avoidance of doubt, Article 9 of the Regulation will highlight the necessity to retain ARI only for entirely successful and partially successful

---

<sup>3</sup> Regulation 2 of 2008 regarding the requirement to register prepaid mobile subscriber information was based on Article 78 of the Law. It was drafted based on a need that is derived from national security requirements with the general objective of supporting the safety and wellbeing of citizens and residents of the Kingdom of Bahrain.

<sup>4</sup> Insofar as Licensed Operators are concerned (i.e. data retention as mandated by TRA shall not apply to any organization not holding a telecommunications license).

## CONSULTATION REPORT

Calls, and will note that ARI resulting from entirely unsuccessful Call attempts is not required.

### **3.2 Article 4 (Scope)**

#### *3.2.1 Article 4 – Comments Received*

3.2.1.1 No comments were received.

#### *3.2.2 Article 4 – TRA’s Position*

3.2.2.1 During the consultation, TRA proposed that the scope of the Regulation shall apply to all Licensees.

3.2.2.2 However, there are Licensees that do not own or operate any telecommunications networks, equipment, facilities, or other such assets. Such Licensees typically provide value-added services, or rely upon the technical assets of other Licensees (the “Facilitating Licensee”) to carry out their services.

3.2.2.3 In such cases, the Licensee in question must still produce the necessary plans required within the Regulation, detailing how the Facilitating Licensee will support their compliance with the Regulation.

3.2.2.4 The Facilitating Licensee is at a liberty to charge a fair and reasonable fee for carrying out the necessary service(s) to ensure Article 78 of the Law applies to Licensees listed in 3.2.2.2 above.

### **3.3 Article 5 (Organizations Entitled and Authorized to Lawful Access under this Regulation)**

#### *3.3.1 Article 5 – Comments Received*

3.3.1.1 Arrangements for the implementation of the Regulation should seek the most cost effective and efficient way of providing access and responding to information requests.

3.3.1.2 TRA should consider there being one point of contact for submission of implementation plans and that if one security organ approves a plan, then this is deemed to be acceptable to the other.

## CONSULTATION REPORT

- 3.3.1.3 Security organs should cooperate between themselves and agree on the necessary arrangement to share the same access facilities (communication links and monitoring systems)<sup>5</sup>.
- 3.3.1.4 A Licensee should provide Lawful Access to one party and not all parties entitled and authorized. The one party that is provided with Lawful Access should in turn enable other security organs to have Lawful Access.
- 3.3.1.5 Ultimately the cost of providing Lawful Access will be borne by consumers of telecommunications services.

### 3.3.2 Article 5 – TRA’s Position

- 3.3.2.1 With respect to the matter of determining which security organs are entitled and authorized to Lawful Access, TRA does not consider that this is relevant to the preparation and enactment of the Regulation.
- 3.3.2.2 Instead of defining the security organs within Bahrain that may be entitled and authorized for Lawful Access, article 5 of the Draft Regulation will be removed, and a new definition for “Security Organs” will be added. The new definition will read as follows: “Security Organs: *every entity that is concerned with any matter related to national or international security in accordance with the applicable laws and regulations of the Kingdom of Bahrain*”.
- 3.3.2.3 The process of determining which security organs shall be entitled and authorized for receiving Lawful Access, as per the definition of Security Organs within the final Regulation, shall be determined by consulting with the Directorate of Legal Affairs (“DLA”).
- 3.3.2.4 TRA will remain the single point of contact between Licensees and security organs on all matters pertaining to the AIP, ACP, central contacts database, and other relevant tasks up until full implementation of the AIP/ACP is completed. Once the Licensee has complied with the Regulation, TRA will not be involved in operational matters.
- 3.3.2.5 Article 78 of the Law specifically states that security organs (plural term) shall be afforded with Lawful Access. The article does not limit the number of security organs that are entitled and authorized to Lawful Access.
- 3.3.2.6 TRA considers that the obligation is upon Licensees to make available all technical resources which allow access to their networks by security organs

---

<sup>5</sup> The primary consideration here being redundant costs

## CONSULTATION REPORT

for fulfilling the requirements of national security. Article 78 clearly states that Licensees shall bear all expenses associated with access as contemplated by Article 78 of the Law, and TRA is of the view that the cost of providing the technical resources in accordance with Article 78 must be considered a cost of business by Licensees.

### **3.4 Article 6 (Implementation of Lawful Access)**

#### *3.4.1 Article 6 – Comments Received*

- 3.4.1.1 Failure to respond to a reasonable submission<sup>6</sup> should not lead to automatic rejection. Within 60 days of the submission of an AIP, TRA must accept, with written conditions, or reject all or in part while giving reasons. Failure to respond within the timescale would be deemed written acceptance of the AIP (the same does not apply to the ACP)
- 3.4.1.2 Article 6 may conflict with Article 11 (Transitional Provisions) that Lawful Access has to be provided within a maximum of 6 months from the effective date of the Regulation – delay (deemed rejection) at the plan submission stage will hinder a Licensee in committing to the 6 months deadline
- 3.4.1.3 The prohibition of marketing or activating a telecommunications service before the provision of Lawful Access should be extended to offering or providing such a service.
- 3.4.1.4 The effect of the Regulation on public services and universal service services must be clarified (e.g. access to emergency services and provision of basic telephony..)
- 3.4.1.5 Article 6.5 of the Draft Regulation should be expanded to include existing operators
- 3.4.1.6 Article 6.5 of the Draft Regulation is unclear about whether or not the prohibition of activating and marketing services shall take effect during the period of reviewing AIP submissions.
- 3.4.1.7 The ACP being produced every six months will lead to financial burdens on smaller operators.
- 3.4.1.8 The period of 2 months to review an AIP is too long, and it is unclear whether TRA will allow existing Licensees to market and activate their services during such a period.

---

<sup>6</sup> The term “reasonable submission” was not defined by the respondent

## CONSULTATION REPORT

- 3.4.1.9 The ACP should not be required at a set point in time (every 6 months), and the introduction of new services should be preceded by an ACP at any point in time. Further, the period to review an ACP should be reduced from 60 days to 30 days.
- 3.4.1.10 The term “telecommunications service” in article 6.5 of the Draft Regulation should be changed to “telecommunications technology”. The respondent argues that SMS, MMS, voice calls and video calls are telecommunications technology, while conference calls and call forwarding are telecommunications services

### 3.4.2 Article 6 – TRA’s Position

- 3.4.2.1 TRA accepts the argument that if it does not respond within a period of 60 days to an AIP submission than this should be considered acceptance of the AIP. The Regulation will be amended accordingly, however, the amended article will include provisions that allow TRA to extend the revision period should it deem such an extension necessary (again, with providing reasons). The extension to the AIP review period can only be extended once.
- 3.4.2.2 TRA does not consider that Article 6 of the Draft Regulation conflicts with Article 11 in light of TRA’s updated position. But in any case, the final Regulation will be updated so that Licensees shall implement the requirements of the Regulation within a period of 6 months from the time of AIP approval.
- 3.4.2.3 The ban listed in Article 6.5 of the Draft Regulation will be extended to restrict Licensees from “offering” or “providing” a telecommunications service until an AIP is approved<sup>7</sup>
- 3.4.2.4 TRA maintains that Licensees, at the effective date of the Regulation that do not comply with the provisions of the Regulation after all deadlines under Article 11 (as amended) have passed, shall cease from offering *any* telecommunications service that does not conform to the Regulation. In effect, the Licensee switches off relevant facilities, equipment, and resources until Lawful Access can be implemented.
- 3.4.2.5 Article 6.5 of the Draft Regulation does not apply to existing Licensees, so the prohibition of marketing or activating services without the implementation

---

<sup>7</sup> This article is intended for newly licensed operators only. Operators extant at the effective date of the Regulation are addressed using Article 11 (Transitional Provisions), which takes into account that Licensees may be actively offering their services at the effective date of the Regulation

## CONSULTATION REPORT

of Lawful Access does not apply. Existing operators who do not implement Lawful Access in accordance with Article 11 will be in breach of the Regulation and will face strict enforcement action.

3.4.2.6 The matters of the ACP and AIP have already been sufficiently addressed above under Definitions, so therefore the comments received in this regard are no longer applicable.

3.4.2.7 TRA is of the view that the examples made to describe telecommunications *technology* are all in fact examples of a telecommunications *service*. The base technology is what lies underneath these services, such as GSM, TDM, SS7, etc. In any event the underlying technology that supports the service will be required to be reviewed during the review of any AIP for the service. For these reasons the reference to “telecommunications services” will remain as is.

### 3.5 Article 7 (Lawful Access Procedures)

#### 3.5.1 Article 7 – Comments Received

3.5.1.1 It should be made clear that Licensees and security organs will conduct the mutual identity verification exercise on each occasion that Lawful Access is requested by a security organ.

3.5.1.2 The way the employee authorization process is proposed may result in employees receiving a one-off authorization signed by the most senior member of staff that would allow the same employee to always be involved in Lawful Access until such an authorization is revoked.

3.5.1.3 Such a blanket delegation of authority could pose its own security risks. Ideally, each time Lawful Access is requested, specific written authorization signed by 2 duly authorized signatories from the Licensee and the security organ (respectively) should be required. This should be reflected in the AIP.

3.5.1.4 Lawful Access procedures should be determined by TRA through a separate public consultation process to ensure a high level of transparency.

3.5.1.5 The process of notifying Licensees of authorized individuals (in case of blanket authorizations) should include TRA as a central point of contact (i.e. security organs notify TRA, and TRA in turn notifies the concerned Licensee – and vice versa).

#### 3.5.2 Article 7 – TRA’s Position

## CONSULTATION REPORT

- 3.5.2.1 The security risk that may arise from blanket authorizations is difficult to manage. This is due to the fact that more often than not the same members of staff within a given Licensee will always be responsible for Lawful Access operations, and the same is also the case with security organs.
- 3.5.2.2 This is a question of security versus usability; in principle, TRA agrees that mutual identity checks should be performed each time Lawful Access is requested, however, it may be impractical to request dual-signatory authorization for each Lawful Access request.
- 3.5.2.3 On balance, TRA will reinforce the need to conduct the mutual identity checks for each instance that contact is initiated between entities, and will indicate that Licensees should perform a number of checks throughout the year to ensure that authorizations are still valid.
- 3.5.2.4 TRA will further elaborate on Lawful Access procedures, however, TRA does not consider that a separate public consultation process is warranted to determine such procedures.
- 3.5.2.5 TRA perceives no added-value in it potentially being involved in passing authorizations between Licensees and security organs. The only instance in which TRA foresees that it should intervene is in the initial contact stage – beyond which TRA will have no role to play in employee authorizations.

### **3.6 Article 8 (Financing of Lawful Access)**

#### *3.6.1 Article 8 – Comments Received*

- 3.6.1.1 Licensees should not bear the costs of networks or equipment that are not part of a given Licensee's networks or equipment (i.e. Licensees should not pay for Lawful Access assets that are used by security organs).
- 3.6.1.2 The financing of Lawful Access should be subject to a reasonableness requirement so as not to divert resources from service delivery and provisioning and the life cycle of technical developments (that innovations generally become cheaper over time if procurement of the latest technology is staged in a phased manner).
- 3.6.1.3 TRA and the government of Bahrain should finance all Lawful Access assets regardless of asset location, and such financing should be based on plans produced by Licensees.
- 3.6.1.4 Financing Lawful Access assets shall differ between small operators and dominant operators in the market to ensure the gap between these two

## CONSULTATION REPORT

types of operators is continuously diminishing. Accordingly, it is recommended that only dominant operators should bear the costs of Lawful Access.

3.6.1.5 TRA should implement a cap on each Licensee's expenditure on technical resources as this Article places a massive financial burden on small and newly established Licensees.

3.6.1.6 As no operator in Bahrain currently owns sufficient connectivity infrastructure to establish direct communication links with security organs, Licensees will have to resort to using Batelco's infrastructure network, which will increase costs for all other Licensees, and reduce Batelco's costs. As the overall objective of the Regulation is the protection of the general public, TRA should allow Licensees to use Batelco's infrastructure network, for purposes of connecting Licensees to security organs<sup>8</sup>, at no cost.

### 3.6.2 Article 8 – TRA's Position

3.6.2.1 As described above under the definition of Lawful Access, and for these same reasons, TRA is in no position to exempt operators from any financing obligation in part or in whole that is related to Article 78 of the Law

3.6.2.2 As listed under the definition of ACP above, TRA will consider authorizing the deployment of new services that may not have a Lawful Access solution readily available – after careful consideration of any inherent risks that may be present.

3.6.2.3 The statement about TRA and the Government of Bahrain paying for Lawful Access fails to consider that TRA cannot amend the Telecommunications Law. Therefore the requirement for Licensees to bear their own costs and expenses in complying with article 78 must be adhered to. The Regulation may specify how these costs are incurred.

3.6.2.4 The issue of treating operators who have or who have not been declared to be dominant has no bearing on a Licensee's responsibility and obligations towards the Law. All Licensees shall equally comply with the Law regardless of company size or market share.

3.6.2.5 TRA sees no practical application to the matter of placing a cap on the expenditures made by Licensees towards achieving compliance with the articles of the Law. Licensees shall be obliged to make any and all

---

<sup>8</sup> The respondent additionally recommended using redundant communication links to minimize outages

## CONSULTATION REPORT

investments as required by the Law, their Licenses, and the resolutions and regulations issued pursuant to the Law by TRA from time to time.

- 3.6.2.6 It is the responsibility of Licensees to ensure that security organs are connected to their networks pursuant to Article 78 of the Law, and the articles of the Regulation. Batelco, just as much as any other operator, will incur costs in this provision. The argument made in 3.6.1.6 above is unfair to Batelco – if Batelco was to provide all such connections free of charge, then it becomes unreasonably more expensive for Batelco than all other Licensees.
- 3.6.2.7 TRA considers that the argument presented regarding free connections is not sufficiently justified and is not in line with Article 78 of the Law, and will therefore stand by its original position.
- 3.6.2.8 TRA recognizes that the investments that must be made by Licensees to comply with this Regulation may be significant and challenging to secure by some Licensees. This matter is additionally aggravated for Licensees extant at the date of publication of the Regulation by the fact that such investments must be secured during a Licensee’s operational phase (as opposed to trying to secure investments at inception).
- 3.6.2.9 TRA will therefore establish a fund to finance the purchase of necessary technical resources on behalf of Licensees, and will finance such purchases over a fixed term. All existing Licensees at the time of publication may apply to receive such financial support from TRA, and TRA will consider applications on a case-by-case basis. TRA will establish a set of guidelines to govern the proposed fund.
- 3.6.2.10 This fund will not be available to operators that are licensed after the final Regulation’s publication date.

### **3.7 Article 9 (Retention of Access Related Information)**

#### *3.7.1 Article 9 – Comments Received*

- 3.7.1.1 ARI should be retained for a fixed period (as opposed to the proposed range of years). Suggested periods were 6 months, 1 year, and 2 years.
- 3.7.1.2 The final Regulation must stress that the Licensee is prohibited from both accessing and retaining Call Content.
- 3.7.1.3 The responsibility of ARI storage should primarily fall with the security organs since only they have the lawful authority to access information. They would be free to search for targeted data themselves.

## CONSULTATION REPORT

- 3.7.1.4 Some Licensees stated that their current systems may not be able to support a maximum response period of 24 hours to retrieve stored ARI.
- 3.7.1.5 There is no European Union (EU) requirement to retain location based data (in the form of Longitude and Latitude information), and none of the 25 EU countries have to comply with such a requirement. The requirement should be amended to per-cell locations.
- 3.7.1.6 Only completed calls shall have retainable ARI (because only completed calls convey voice or data – based on the definition of a Call).
- 3.7.1.7 Branch exchange numbers cannot be identified for all calls in a traditional PABX (the Licensee will identify the PABX as a single line).
- 3.7.1.8 Instead of providing the time at the end of a call it is suggested to only provide the call duration.
- 3.7.1.9 Receiver IMEI number can be provided if the receiver is a customer of the same network provider “On-Net”.
- 3.7.1.10 There are limitations to what ARI can be retained (e.g. the caller IMSI number may not be available, some ISP’s are not storing which IP addresses are used by their subscribers, the number of an SMS message recipient is not stored, the Receiver IMEI number may not be available, certain ISP’s can only store a few weeks of access history, the requirements of instant messaging are not entirely achievable and MAC address of DSL subscribers is not available).
- 3.7.1.11 ISP’s have no control over any email service that is not operated by the ISP’s themselves (including, without limitation, web based email and private email servers).
- 3.7.1.12 The content of an email is directly linked to the ARI, and it is not possible to separate the two from each other, which may lead to a breach of the Regulation.

### 3.7.2 *Article 9 – TRA’s Position*

- 3.7.2.1 As stated above, TRA considers that a fixed term of 1 year is sufficient for purposes of storing ARI. ARI that expires must be destroyed by Licensees (subject to the exceptions made within the Regulation).
- 3.7.2.2 Article 9.2 of the Regulation will be updated to emphasize that Licensees are strictly prohibited from accessing Call Content and ARI.

## CONSULTATION REPORT

- 3.7.2.3 Licensees shall be responsible for storing ARI that is generated by their subscribers, or generally generated in relation to their own telecommunications services. The Regulation will not place the burden of storing ARI with security organs.
- 3.7.2.4 Near real-time access to ARI is currently available in the market; Licensees shall ensure they are capable of providing requested ARI within the stated maximum period.
- 3.7.2.5 Whilst reference to the EU can be useful in terms of guidance, its laws are not binding upon TRA or the Kingdom of Bahrain. Nevertheless, while referring to the EU directive on data retention it is evident that all EU member states have to retain location based data in one form or another. At least one EU country records such data in the form of longitude and latitude to within a few yards of the target<sup>9</sup>. For purposes of the requirements of the Regulation, TRA is of the view that current technological developments allow for such a requirement to be fulfilled relatively easily<sup>10</sup>.
- 3.7.2.6 With additional reference to sections 3.1.10.2 and 3.1.10.3 above, TRA considers that partially successful Calls fulfill the definition of a Call in that data, in the form of a ring tone, for example, is delivered to the subscriber. Furthermore, for certain types of security threats, nothing more than a ring tone is required to initiate the threat. TRA therefore stands by its position stated in articles 3.1.10.2 and 3.1.10.3 above.
- 3.7.2.7 Branch exchange numbers will be removed from Article 9 (Direct-Out-Dial numbers will not be exempt).
- 3.7.2.8 Stating only the duration of a call adds the burden of having to calculate the time a call ended and is error-prone. Further the exact time a call is made and ended can be vital information in certain criminal investigations. This requirement shall remain as is.
- 3.7.2.9 The list of ARI to be retained will be reviewed before final publication of the Regulation; however, ARI elements that are beyond a Licensee's capability to retain due to current equipment/systems limitations will be left unchanged.

---

<sup>9</sup> See <http://security.homeoffice.gov.uk/ripa/communications-data/retaining-data/>, <http://www.retentia.com/dataretention.htm>, [http://en.wikipedia.org/wiki/Anti-Terrorism,\\_Crime\\_and\\_Security\\_Act\\_2001#Part\\_11](http://en.wikipedia.org/wiki/Anti-Terrorism,_Crime_and_Security_Act_2001#Part_11), and [http://en.wikipedia.org/wiki/Telecommunications\\_data\\_retention](http://en.wikipedia.org/wiki/Telecommunications_data_retention) for more information

<sup>10</sup> Some location solutions do not even require any hardware upgrades (using software-only). See [http://en.wikipedia.org/wiki/Location-based\\_service](http://en.wikipedia.org/wiki/Location-based_service) for general information on LBS.

## CONSULTATION REPORT

It is the responsibility of the Licensee to ensure compliance with technically feasible requirements.

- 3.7.2.10 As far as email ARI is concerned, the Regulation will be updated to clarify that ISP's shall be responsible for retaining ARI that pertains to ISP-provided email only, to the exclusion of other types of email (web-based, user-hosted, etc.)
- 3.7.2.11 Email header information is separate from the email body (the Call Content), and can be retained without difficulty.

### **3.8 Article 10 (CLI)**

#### *3.8.1 Article 10 – Comments Received*

- 3.8.1.1 The definition of CLI needs to be refined to require operator-CLI only (i.e. CLI sent by the operator) as opposed to CLI provided to consumers as a service. The obligation, therefore, will be for Licensees to always transmit CLI, but not necessarily provide it to consumers for free.
- 3.8.1.2 It may be unlawful to require operators to block traffic that does not include CLI.

#### *3.8.2 Article 10 – TRA's Position*

- 3.8.2.1 The definition of CLI will be updated as recommended in 3.8.1.1.
- 3.8.2.2 Having consulted on the matter, TRA is now of the view that it should not mandate the blocking of a Call that does not have CLI information. The Regulation will be updated accordingly.

### **3.9 Article 11 (Transitional Provisions)**

#### *3.9.1 Article 11 – Comments Received*

- 3.9.1.1 Licensees, at the effective date of the Regulation, should be provided with a period of 3 months to prepare an AIP and should be provided with a period of 1 year to comply with the Regulation

#### *3.9.2 Article 11 – TRA's Position*

- 3.9.2.1 The AIP primarily comprises of the list of services and technical assets currently available/deployed by a Licensee, and a proposed set of solutions in support of Lawful Access, Data Retention, and Location Based Services. TRA is of the view that preparing the AIP should not take more than 2 months.

## CONSULTATION REPORT

With regards to the period of time to comply with the Regulation, TRA considers the above mentioned 6 months period (from the date of approving the AIP) is sufficient.