Trinidad and Tobago Computer Society

Comments on the Interception of Communications Bill, 2010

Section	Comment/Suggested Amendment
5	"Intercept" should be redrafted for the last line to include: *knowledge of the person making or the intended recipient of the communication*; "Telecommunication" should be redrafted- (i) to include *satellite and microwave communication,* (ii) as *(b) in any form other than those specified in paragraph (a) which can be put into intelligible form with or without the use of a key*, and (iii) for a definition for or mention of electronic data to be included in this section, perhaps under (a)(iv), (and not its inclusion only in the definition for "protected communication")
6(2)(a)-(f)	Clear guidelines must be given in the regulations to companies regarding- (i) recording of customer service calls (for quality assurance), as well as record of keystrokes on private network computers etc. (ii) what constitutes reasonable grounds in S.6(2)(b) *"reasonable grounds for believing that the person… consents to interception"* Suggest redrafts of S.6(2): *(d) "the communication is not a private communication on a public telecommunications network"* The need for further definition as to private or public telecommunications network is required. *(e) the communication whether a privately or publicly stored communication is acquired in accordance with any other law;* (f) "*network that is not a public telecommunications network"* should be replaced by *"private telecommunications network"*
7	The overall wording of the clause implies that possession of software such as, any network detection tool (e.g. nmap) which is installed/used by any network administrators is now illegal; another case could be when installing Voice over IP (VoIP) systems which have facilities to record conversations for delivery via email. These instances must be clearly reviewed and dealt with. Suggest redraft to link the person referred to in S.7(2)(b) to the person being granted the warrant under S.8(1) such as: *(b) any other person named in the warrant under S.8(1) in possession of such a device of component for the purpose of national security.* This is important to ensure that this person is known by the Minister under S.8(3)(b)
13	Clear guidelines must be given in the regulations to companies regarding this section particularly, what constitutes "prompt assistance" under S.13(1). This is especially important as there is a fine of $1,000,000 for contravention
14(b)	There must be a clear cut-off period for the retention of copies of the communication and should not be stored indefinitely
15(1)	States essentially at line 3 - *if protected communication is "likely to" come into possession of an authorised officer… the officer may apply to the Judge for an order...* Though guidelines and the criteria for the Judge to assess is given under S.15(4), this assessment will be speculative and vague for information that does not yet exist. Suggest that "*is likely to do so"* in S.15(1) be deleted

16	We need to clarify generally under S.16 that where the receiver of protected communication is the one being monitored it would be a tip-off to request a key from him Need for clear and standardised guidelines must be given in the regulations to companies regarding guidelines on the storage, access, length of retention or terms for destruction of the data to ensure that important data is not destroyed under 16(3)(a) Also under S.16(3) the person whom a disclosure order is addressed should have the opportunity to utilise any keys he may hold (in the presence or with the assistance of the authorised officer) to determine if the communication can be rendered in an intelligible form; rather than being mandated to hand over all or any keys he holds in his possession (which may not be able to successfully put the protected communication into intelligible form) Under S.16(7) it must be defined what is meant that the person who "*without reasonable excuse*" fails to comply. The burden of proof is beyond reasonable doubt.
17(b)	There must be a clear cut-off period for the retention of keys and should not be stored indefinitely
18	Why is no warrant from the Judge required for the Disclosure of Communications Data? Certainly this should be a requirement.

Other Comments:

1. The Bill should be enacted with the corollary of legislation such as the Data Protection Bill (which will help define, support and enhance this Bill), the Electronic Transactions Bill as well a Bill/regulations governing data retention (If there aren't any accompanying data retention, data audit and policy logging laws then nothing prevents entities from deleting any incriminating data before being served with a warrant). This bundle of legislation requires a reasonable period for multi-stakeholder comment and should be aligned with regional ICT legislation (thankfully the Data Protection and Electronic Transactions Bills have been before Parliament for some time our comments on these Bills can be found at
   www.ttcsweb.org/articles/computer-laws/index.htm#dataprotection;
   www.ttcsweb.org/articles/computer-laws/TTCS_data_protection_comments.txt;
   www.ttcsweb.org/articles/computer-laws/TTCS_electronic_transactions_comments.txt.
   It is not good enough for us to determine the success/failure of this bill by an Annual Report presented by the Minister of National Security.

2. Needs for proactive provisioning of separation of privileges by the authorised officers and a continuous 3rd-party. This 3rd-party will report directly to the Minister and audit the information collected by these agencies to ensure that they are only monitoring what they are authorised to and nothing else.

3. No guidelines on the storage, access, length of retention or terms for destruction of the Data obtained by under the Bill. The data obtained should be treated with appropriately, if the data is not properly stored, managed and destroyed, unintentional disclosure may and most probably will occur.

Dated 23 November 2010