@BACT
ARTHIT SURIYAWONGKUL
THAI NETIZEN NETWORK

# LAWS THAT WOULD ALLOW INTRUSIVE SURVEILLANCE IN THAILAND

# SEC 18 PARA 1 – COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)

- **Section 18.** With the enforcement of Section 19 and for the benefit of an investigation, if there is reasonable cause to believe that there is the perpetration of an offense under this Act, the competent official shall have any of the following powers necessary for the acquisition of evidence to prove the wrongdoing and to identify the perpetrators:

- (1) .... (8)

# SEC 18 PARA 1 – COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)

- (4) **copy** computer data, computer traffic data from a computer system, in which there is a reasonable cause to believe that offenses under this Act have been committed if that computer is not yet in the possession of the competent official;

- (6) **inspect or access** a computer system, computer data, computer traffic data or computer data storage equipment belonging to any person that is evidence of, or may be used as evidence related to, the commission of an offense or used in identifying a person who has committed an offense, and instruct that person to send the relevant computer data to all necessary extent as well;

- (7) **decode** any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a competent official in such decoding;

# SEC 19 PARA 1 – COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)

- **Section 19.** The power of authority of the competent official under Section 18 (4), (5), (6), (7) and (8), is given when that competent official files a petition to a Court with jurisdiction for a writ to allow the competent official to take action. However, the petition must identify a reasonable ground to believe that the offender is committing or going to commit an offense under the Act as well as the reason of requesting the authority, including the characteristics of the alleged offense, a description of the equipment used to commit the alleged offensive action and details of the offender, as much as this can be identified. The Court should adjudicate urgently such aforementioned petition.

# SEC 25 PARA 1 – SPECIAL INVESTIGATION ACT B.E. 2547 (2004)

**Section 25.** In cases where there is a reasonable ground to believe that any document or information sent by post, telegram, telephone, facsimile, computer, communication device or equipment or any information technology media has been or may be used to commit a Special Case offence, the Special Case Inquiry Official approved by the Director-General in writing may submit an ex parte application to the Chief Judge of the Criminal Court asking for his/her order to permit the Special Case Inquiry Official to obtain such information.

# SEC 25 PARA 2 – SPECIAL INVESTIGATION ACT B.E. 2547 (2004)

When granting permission under paragraph one, the Chief Judge of the Criminal Court shall consider the effect on individual rights or any other right in conjunction with the following reasons and necessities:

(1) there is a reasonable ground to believe that an offence of a Special Case is or will be committed;

(2) there is a reasonable ground to believe that access to the information will result in getting the information of a Special Case offence; and

(3) there is no more appropriate or efficient method.

## COMPARING PROCESS TO GET ACCESS TO INFORMATION

| | Computer Crime Act<br>Section 18+19 | Special Investigation Act<br>Section 25 |
|---|---|---|
| Requester | CCA Officer | DSI Officer with approval from Dept Chief |
| Court | Any judge in a jurisdiction | Chief of Criminal Court |
| Things Court need to Consider | - | Privacy rights, Efficient way to get n info needed?, Last resort measure?, etc. |
| Time limits | - | 90 days, court may put additional conditions |
| After approval | After measure has been use, should report back to Court - within 48 hours | After measure has been use, should report back to Court |