Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

by Taiwan Association for Human Rights

Contact1: E-Ling Chiu, eeling@tahr.org.tw
Contact2: Ming-Syuan Ho, hmsyuan@tahr.org.tw

A. Information concerning the domestic regulatory frameworks that may be applicable to the development, marketing, export, deployment, and/or facilitation of surveillance technologies by private companies, such as:

1. Laws, administrative regulations, judicial decisions, or other policies and measures that impose regulations on the export, import or use of surveillance technology;

About Export and Import

In Taiwan, there are laws and administrative regulations that regulate the export and import the surveillance technology. ***The Article 13 of Foreign Trade Act*** (the content see appendix 1) is exactly the main law to regulate the export and import of **strategic high-tech commodities (SHTC)**. It provided three conditions to decide whether SHTC could be import or export.

The procedure of export or import of SHTC is regulated by ***Regulation Governing Export and Import of Strategic High-Tech Commodities***, which is a administrative regulation.

The main definition and scope of SHTC are defined in the "**Export Control List for Dual Use Items and Technology and Common Military List**" （ briefly as **"List"** ）, which is a document include ten categories of SHTC. **Other types or categories of SHTC** may be referred to some international documents like UN documents or defined by sales destination of the commodities. For example, the sensitive commodities list for North Korea and Iran are also be included in the scope of SHTC.

The computer (category 4), and telecommunication apparatus & information security apparatus (category 5) are most worthwhile to be noticed in the **"List"**, especially in its description in part 5a001f and part 5a001j of category 5.

In the part 5a001f, it clearly said that one kind of the SHTC is the telecommunication apparatus to intercept or monitor the information (like IMSI, TIMSI, or IMEI) sent by mobile telecommunication device.

In the part 5a001j, it also include the apparatus that could execute the function of Internet Protocols in national level or telecom companies' level, these kinds of apparatus should include "all" below functions: analyze in application layer(with regard of OSI 7 layers), intercept the metadata and

content data, search the data intercepted, search data based on personal identifiable information, and draw the network between different group of people.

About the deployment and use

The *Foreign Trade Act* and related regulations do not regulate the private company to deploy or use of surveillance technology

However, the telecommunication company have the obligation to provide the assistance for communication surveillance, and have the obligation to setup and maintain the communication surveillance act according to the ***Article 14 of The Communication Security and Surveillance Act*** **(CSSA).**

2. Remedies available in the event of illicit export or use of private surveillance technology;

According to *the* ***Article 13 of Foreign Trade Act***, the company should get the permission for exporting or importing all SHTC in principle. If the company did not get the permission, the government may detain, confiscate, or return the shipment of the SHTC.

According to *the* ***Article 27 of Foreign Trade Act***, if company violate the related export or import regulation (like Article 13), there would be a punishment with imprisonment for not more than 5 years, detention, or a fine not more than NTD 1,500,000 (approximately USD 500,000)

And according to *the* ***Article 2 of CSSA***, the communication surveillance could only be implemented based on national security reason or maintaining social order and should get the interception warrant from court, therefore, if the illicit communication surveillance was conducted by private company or individuals and, therefore, accused, the company or individual may be imprisoned at most 3 years according to the ***Article 315-1 of Criminal Law*****.**

3. Whether the laws, regulations, or policies identified are consistent with State obligations under Article 19 of the International Covenant on Civil and Political Rights, Article 19 of the Universal Declaration of Human Rights, and other relevant human rights standards.

No comment here.

B. Information concerning the use of such surveillance technologies:

1. Details of emblematic cases of State use of private surveillance technology against individuals or civil society organizations.

3. The extent to which private surveillance companies offer services to States and other actors to deploy their technologies in specific circumstances, and the extent to which companies are aware of the end-use of the technologies they market.

Confirmed information about government buy surveillance technology.

There are no solid evidence that Taiwan government use private surveillance technology “against” individual or civil society organization, since Taiwan government will always claim that they buy the private surveillance technology only for combating or preventing serious crimes, not against civil society.

But anyway, Taiwan Government did buy some surveillance technology from private companies. The communication surveillance system or cyber forensic system used by police units or Investigatory Bureau under Ministry of Justice are mainly developed and provided by two private companies: Decision Group Inc.（定興科技）or Gorilla Technology（大猩猩科技）. These two companies provide different kinds of surveillance technology to government (especially to the law enforcement departments).

Below are the information on these two companies’ website, It should be noticed that Decision Group Inc. obviously disclose more information than Gorilla Technology, hence we could get more concrete image about what Decision Group Inc do.

For the Decision Group Inc., the main product of this company is "E-Detective". According to E-Detective its own introduce, this apparatus would be set in the middle of data transfer procedure, pretend to be the original user to connect to different Internet service provider, then it would sniffer all IP packets and try to decode them, which works like a typical man-in-the-middle attack.

Gorilla Technology did not have much detailed product information in their website. But based on the information on the website, they do develop many “Smart” systems, including license plate recognition system, face recognition system etc,. And according to the information searched on Government e-Procurement System, they did provide above Smart systems to some law-enforcement departments, and also help Criminal Investigation Bureau, which is under central government, to setup the communication surveillance system that can wiretap or gather 4G LTE signal.

We do not know whether these two companies "import" their technology from other countries. However, we know that they all have many foreign customers, so there’s huge possibility for them to do some exports.

Decision Group Inc. publicly list more than 35 countries as their customers, and some of them have bad human rights records, like China, Myanmar, Egypt. In another page, Decision Group Inc. proudly show that their systems has been adopted by more than 54 countries' governments' law enforcement units. Besides that, Decision Group Inc. also have some connections with Morocco national security unit in November 2011 due to the civil society of Morocco raise more and more democratic social movement in 2011, therefore Decision Group Inc. try to help Morocco government

to monitor those social movements. The Morocco's movement and surveillance story was also been reported by Privacy International.

About Gorilla Technology, actually we almost do not have any export or import information about this company, what we only know is that this company has nine offices in the worldwide, that is the only reason why we think this company also export their surveillance product to other countries.

Possible information about government buy surveillance technology.

Besides Decision Group Inc. and Gorilla Technology, Taiwan government might have other records about importing surveillance technologies.

1. Based on the documents leaked by Wikileaks in 2015, Taiwan government once tried to buy the remote control system developed by Hacking Teams in 2013, but did not sign the contract at last.

2. Based on the research conducted by Citizen Lab and Surveillance Industry Index Database published by Privacy International, there's a Finfisher's server in Taiwan. But we do not know whether it is deployed by government or not.

3. Based on the research conducted by Citizen Lab and Surveillance Industry Index Database published by Privacy International, there's one or more Blue Coat device which has been setted in Taiwan's public internet. But we do not know which Telecommunication corporation set it/them.

2. Company policies to ensure that the development and sale of surveillance technologies meets human rights standards, particularly those articulated in the UN Guiding Principles on Business and Human Rights.

4. Company standards or policies to monitor the use of their technology after it is sold to governments

For the above two companies, basically we do not find any policy related to their developments and sales of surveillance technologies on the websites.

Decision Group Inc. stress several times in their pages for what they assist is lawful communication surveillance, but we do not find any information about how they make sure their product would only be used legally, or how they assess the human rights risk of the use of their products.

And there's much fewer related information or policy that could be found in Gorilla Technology's website. The only thing we could find is that this company's CEO ever publicly said that right to privacy is the biggest problem for the development of smart cities.