Multi-functional Smart Lampposts: Technical Advisory Ad Hoc Committee 1st Meeting

12 August 2019

Meeting Agenda

Date: 12th August 2019 (Monday)

Time: 4:30 – 6:30 p.m.

Venue: Conference Room, 15/F Wanchai Tower

Agenda:

1. Membership and Terms of Reference
2. High-level Work Plan
3. Background of the Multi-functional Smart Lampposts Pilot Scheme
4. Personal Privacy and Information Security Measures
5. Security Assessments and Reviews conducted by independent third parties
6. Any Other Business

Membership and Terms of Reference

Membership

Convener

Mr Victor LAM, Government Chief Information Officer, OGCIO

Members *(list by order of surname)*

Mr Vincent CHAN, Partner, Ernst & Young Advisory Services Limited

Dr K P CHOW, Associate Professor, Department of Computer Science, The University of Hong Kong

Mr Francis FONG, Honorary President, Hong Kong Information Technology Federation

Mr Stephen HO, Honorary Chairman, Communications Association of Hong Kong (CAHK)

Ir Prof Joseph NG, Professor and Director of the Research Centre for Ubiquitous Computing, Department of Computer Science, Hong Kong Baptist University

Mr Ronald PONG, Chairman, IT Governance Committee, Smart City Consortium

Dr Lawrence POON, General Manager, Hong Kong Productivity Council

Dr K F TSANG, Associate Professor, Department of Electronic Engineering, City University of Hong Kong

Mr Stephen Kai-yi WONG, Privacy Commissioner for Personal Data

Mr Wilson WONG, Chief Executive Officer, Hong Kong Internet Registration Corporation Limited

OGCIO Representatives

Mr Tony WONG, Assistant Government Chief Information Officer (Industry Development), OGCIO

Mr Jason PUN, Assistant Government Chief Information Officer (Cyber Security & Digital Identity), OGCIO

Secretary

Senior Systems Manager (Smart City) 2, OGCIO

Terms of Reference

- To examine personal privacy protection and related information security technology issues relating to the operation of multi-functional smart lampposts, and recommend measures to address concerns and any additional safeguards required, in individual smart lamppost applications; and
- To advise on the publicity and engagement strategy to facilitate public understanding over the equipment installed on smart lampposts and their functionalities in various applications as well as the potential uses, so as to communicate to the public in an effective and transparent manner to engender greater community support for the smart lampposts initiative.

High-level Work Plan

High-level Work Plan

Meeting	Purpose
1st (12 Aug 2019)	• Declaration of interests • Brief Members on the Terms of Reference (TOR) and modus operandi of the Committee • Seek Members' agreement on the proposed work plan and meeting schedules • Brief Members on the smart lampposts pilot scheme and seek their views and advice on the personal privacy protection and related information security technology issues relating to the operation of multi-functional smart lampposts
2nd (10 Sep 2019)	• Brief Members on the originally planned and potential applications to be implemented on the smart lampposts • Seek Members' views and advice on the personal privacy protection and related information security technology issues of individual smart lamppost applications
3rd (8 Oct 2019)	• Examine and recommend technologies and measures to address personal privacy protection concerns and any additional safeguards required in individual smart lamppost applications
4th (12 Nov 2019)	• Present the draft findings and recommendations to Members • Seek Members' views and advice on the publicity and engagement strategy to facilitate public understanding on the applications and potential uses of smart lampposts so as to engender greater community support
5th (10 Dec 2019)	• Seek Members' endorsement on the final report (if necessary, the report would be further revised for endorsement at a later meeting or by circulation)

Background of the Multi-functional Smart Lampposts Pilot Scheme

Background of the Multi-functional Smart Lampposts Pilot Scheme

The Multi-functional Smart Lampposts pilot scheme is a three-year programme to install some 400 smart lampposts by phases in four districts with higher pedestrian and traffic flow, namely Central / Admiralty, Causeway Bay / Wan Chai, Tsim Sha Tsui and Kwun Tong / Kai Tak Development Area with a view to promoting smart city development in Hong Kong and supporting 5G mobile network implementation.

Smart devices including traffic detectors, panoramic cameras, meteorological sensors and air quality sensors are proposed to be installed to collect three types of real-time city data, including meteorological data, air quality data and traffic snapshot images with a view to enhancing city and traffic management.

Schedule of the Multi-functional Smart Lampposts Pilot Scheme

Three-year programme： 2019-20 to 2021-22

In June 2019

50 smart lampposts already rolled out:

- Sheung Yuet Road (20)
- Shing Kai Road (20)
- Kwun Tong Town Centre (Batch A) (10)

By phases in three years

Discussed in Kowloon City District Council:

- Kai Tak Cruise Terminal (21)

Discussed in Kwun Tong District Council:

- Kwun Tong Town Centre (Batch B) (10)
- Hoi Yuen Road
- Hong Ning Road
- Lai Yip Street
- Tai Yip Street
- Tsun Yip Street

Pending discussion in Yau Tsim Mong District Council:

- Canton Road
- Kowloon Park Drive
- Nathan Road
- Salisbury Road
- Near Ladies' Market
- Temple Street Night Market

Wan Chai District and Central & Western District (not yet consulted)

Past Consultations

✓ Legislative Council Panel on Information Technology and Broadcasting (12 March 2018)
- Obtained support from LegCo.

✓ Tsuen Wan District Council Traffic and Transport Committee by invitation (3 September 2018)
- The committee requested OGCIO to consider including Tsuen Wan district into the subsequent phase of the pilot scheme.

✓ Kwun Tong District Council (8 January 2019)
- Members requested the data collected from smart lampposts to be used in city management, tackling city problems, and assisting in traffic offences prosecution as well as emphasising that the data collected from smart lampposts should be openly disseminated to the general public.
- The meeting generally supported the installation at the proposed road segments.

✓ Kowloon City District Council (24 January 2019)
- Some members expressed their concern on possible public health regarding radiation emission; the necessity of privacy protection; subsequent maintenance arrangement and the availability of the collected data to the general public.
- The meeting generally supported the installation at the proposed road segments.

✓ Yau Tsim Mong District Council Meeting by invitation (24 January 2019)
- Members generally requested to speed up the installation and extend the coverage in YTM district.

✓ Legislative Council Panel on Information Technology and Broadcasting (16 April 2019)
- Members noted the progress of the project implementation.

Background of Smart Devices and Functions on Smart Lampposts

HyD:

- ✓ **LED lighting –** to adopt energy saving equipment and smart management for carbon emission reduction

OGCIO:

- ✓ **Wi-Fi access point and related network equipment** – to install free Wi-Fi service on smart lamppost at suitable locations

TD:

- ✓ **Bluetooth detector** – to detect journey time and average vehicular speed for sharing traffic information with the public

HKO:

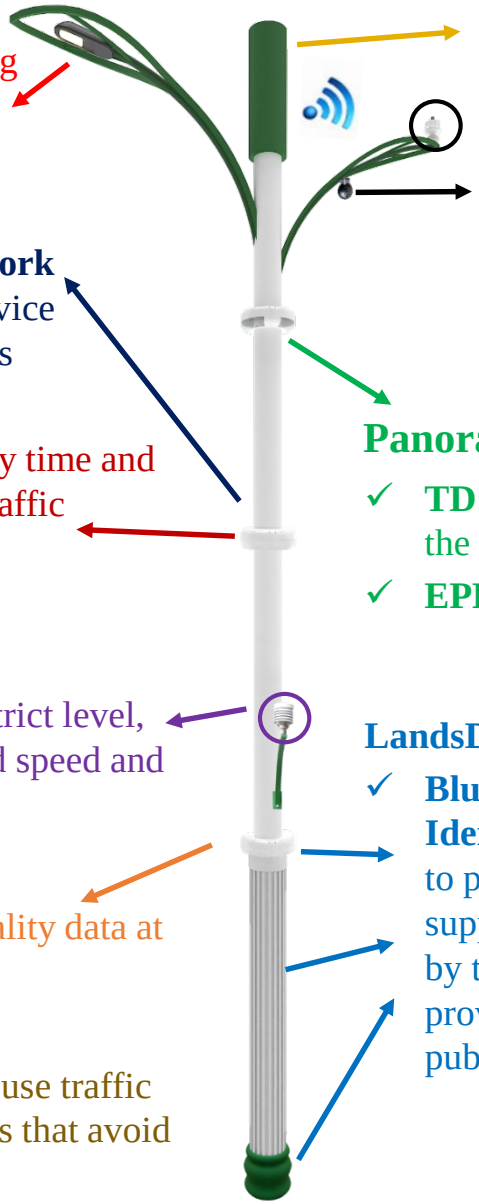
- ✓ **Meteorological sensors** – to collect meteorological and related data at district level, including temperature, humidity, wind speed and direction, rainfall, UV index, etc.

EPD:

- ✓ **Air quality sensor** – to collect air quality data at district level

TC:

To advise the tourist trade/agents to make use traffic messages or alerts to help them plan routes that avoid congested areas



4G / 5G – to facilitate mobile network operators to install base stations

TD:

- ✓ **Thermal detector & camera** – to collect real-time traffic data, including vehicular speed, vehicle types and traffic flow, and to monitor traffic conditions

Panoramic Camera

- ✓ **TD:** to collect real-time traffic data for sharing to the public as well as traffic monitoring
- ✓ **EPD**: to collect illegal dumping data

LandsD : Positioning Devices

- ✓ **Bluetooth Beacon, Radio Frequency Identification (RFID) tag and Geo-QR Code** – to provide accurate positioning services to support the development of related applications by the Government and the industry, such as providing information of public facilities to the public and visitors

The Latest Development

To address the recent public concern on privacy protection of the smart lamppost and some of its applications,

- ✓ we explained the details of the devices and functions on smart lampposts, in particular privacy protection through:
  - a technical briefing and an on-site visit for the media on 16 July 2019
  - clarification on functions of smart lampposts made on 18 July 2019
  - an animation shared via social media on 26 July 2019
- ✓ we also introduced some immediate measures, including:
  - not to activate three applications which may touch on personal privacy
  - Publish locations, devices and functions installed on every smart lamppost on our website and as open data for public reference

Security Protection and Threat Detection

Security Threats	Protection	Detection
Sabotage on Devices	Installed at 3m Height or above	System Logs and Event Management
Thieve / Device Spoofing	- Donut Casting - Protective Cover - Intelligent Door Locks - Mac Address Whitelist	
Physical Damage	- Made by High Grade GR 65 Steel	Site Inspections
Spray Paint on / Shade Camera	- Installed at the Highest Donut - Donut Casting	Real-time detection on camera occlusion
Eavesdropping	- Data Encryption - Anti-Malware Facilities - Private Network over Metro-Ethernet - Mobile Private Network over IPSec VPN	System Logs and Event Management
Spoofing/Tampering	- Access control - Mutual authentication with digital cert	
System vulnerability	- Patch Management	
Denial-of-service (DoS) and distributed denial-of-service (DDoS)	- Network segmentation - Firewalls - Content Delivery Network - Anti-DDoS Protection	
Malware /viruses	- Anti-Malware Facilities	

Personal Privacy and Information Security Measures

Privacy Impact Assessment

Privacy Impact Assessment

- No immediate issue of non-compliance under the six Data Protection Principles for the assessment of the backend system.
- No privacy issue / observation was identified in the PIA report.

Comments from Privacy Commissioner for Personal Data

1) Data user for each type of data captured by the smart lampposts should be stated clearly in the PIA report

   Action/Response: Information is recorded in relevant document.

2) Collected data, such as video/image involved personal information should be reviewed periodically to assess any privacy risks that may arise from time to time

   Action/Response: The policy to conduct PIA is set as a biennial exercise or whenever there is any newly launched application.

3) Surveillance cameras may unintentionally capture human face of an individual, appropriate level of resolution should be adopted and the possibility of converting low resolution images back to high resolution images has to be included in the PIA

   Action/Response: Resolution of traffic snapshot image is lowered to 320 x 240 and periodic PIA will be conducted to review the latest technology.

Privacy Impact Assessment

4) Data retention should not be kept longer than necessary for the fulfillment of the purpose in compliance with Data Protection Principle 2 (2) in Schedule 1 to the PDPO

   Action/Response: Data collected are not to be stored in the lampposts. Collected data are transmitted directly to backend system of users.

5) Regular security review should be conducted to make sure the encryption method being used is effective and assess if the data could be de-encrypted in the light of the technological development

   Action/Response: The policy to conduct relevant security review is set as a biennial exercise or whenever there is newly launched application.

6) Conspicuous notice should be displayed near the smart lampposts to notify the public about the installation of camera in the smart lamppost and how the data collected would be used

   Action/Response: Notices or banners put up at prominent locations to notify the public has been adopted for smart lampposts with camera.

Personal Privacy Protection Measures

For applications on smart lamppost:

- Conduct Privacy Impact Assessment & Privacy Compliance Audit
- Consult Privacy Commissioner for Personal Data
- Collected data would only be sent to the relevant departments, and after transmission, the data would be deleted and would not be stored in the smart lampposts
- No facial recognition function
- Fully complied with Personal Data (Privacy) Ordinance by following the guidelines below -
  - Cameras are set to face and take pictures of public areas only
  - Notices or banners are put up at prominent locations to notify the public
  - All images taken are solely for specific purposes
  - Data collected are not to be stored in the lampposts
  - Various local stakeholders and district councils are thoroughly consulted prior to the installation

Security Assessments and Reviews conducted by independent third parties

Information Security Assessments on Smart Lamppost Conducted by Independent Consultants (May – June 2019)

- Through multiple independent security assessments/tests:
  - Review security measures and identify security risks
  - Recommend areas of improvement and additional safeguards to strengthen security protection
- Three separate assessments/tests conducted:
  - Security risk assessment & audit on the hardware and software components
  - Penetration tests on wireless services
  - Holistic security assessment on the integrated system and processes

Security Risk Assessment & Audit on H/W and S/W Components

Scope

- General control review, e.g. access control, physical security, etc.
- Vulnerability scan at network, hosts and servers
- Penetration tests for IT support systems (e.g. device management and status tracking, data processing hub, etc.)

Findings and Recommendations

- Necessary security measures already in place with proper safeguards
- No high risk items identified
- Some low risk items identified with recommended safeguards, e.g.
  - ✓Improve ventilation to prevent overheating
  - ✓Update the latest software and patch version on certain devices
  - ✓Perform hardening of certain network equipment

Follow-up Action

- Most of the recommendations had been completed before system launch
- The remaining recommendations (for very low risk areas) will be completed before September 2019

Penetration Tests on Wireless Services

Scope

- On-site penetration tests for wireless components (Bluetooth, Wi-Fi, RFID):
  - ✓Passive Attack, e.g. eavesdropping
  - ✓Active Attack, e.g. denial of service attack

Findings and Recommendations

- No major issues identified
- Bluetooth intelligent lock assessed to be secure
- Some areas of improvement recommended, e.g.
  - ✓Strengthen authentication for Bluetooth beacon (to prevent replay attack)
  - ✓Use more secure encryption for transmitting device health-check data via Wi-Fi
  - ✓Enhance control procedure to detect/prevent rogue RFID tags

Follow-up Action

- All except one very low risk recommendation were completed
- The remaining one will be completed before December 2019

Holistic Security Assessment on Integrated System and Processes

Scope

- Review of end-to-end security architecture and design:
  - ✓ From end-point/IoT devices on lampposts, IT support systems and network infrastructure, to the interfaces with backend application systems
- Review of overall security management: Policy, Organisation and Processes

Findings and Recommendations

- No major security issues identified; network protection measures already in place
- Pilot system launch can proceed
- Some areas for long-term improvement recommended, e.g.
  - ✓ Develop checklist of requirements for reference in future procurement of IoT devices
  - ✓ Evolve network traffic protection capabilities on the smart lampposts to limit degradation of services resulting from malfunctioning devices
  - ✓ Evolve individual logging tools to a centralised monitoring architecture (e.g. SIEM)

Follow-up Action

- Long-term improvement measures will be taken if smart lampposts are to be widely deployed

AOB