Rationale for starting Study Period on "Guidelines for Privacy in Internet of Things (IoT)”

The Internet of Things describes a world in which objects or devices (referred to as ‘things’) are connected to other ‘devices’ and ‘people’ over internet - not only to share information but more importantly to cause and respond to physical changes within and outside the object. In the recent years we are witnessing rapid development of IoT solutions & products – particularly in the area of device-to-people IoT segment, and the lowering of costs driven by the scale, and business process innovation is increasing its reach across all sections of society – both in the developed and developing parts of the world.

While it is intended to greatly benefit consumers and improve quality of life for society at large, it also introduces new type of privacy threats and challenges such as the following:

1. Sensors triggered remotely through internet and often without manual intervention;
2. Misuse of personal data due to ease of data flow and lack of transparency & control;
3. Occurrence of unwanted action - Cause physical harm, loss or theft of property. E.g., a hacker can tamper with a sensor attached to a gadget such as car garage door, activate it and intrude into victim’s house;
4. A wanted action not occurring - Safety concern due to a physical action triggered remotely by a genuine owner not getting executed, which can lead to an accident. E.g, one switches off ones’ kitchen oven from smartphone, but it doesn’t get switched off, possibly due to sensor not working or due to its getting connected to neighbors oven;
5. When more than one individual is associated with a device, whose consent need to be taken for processing data?;
6. How do we establish identity of a device, and how is it changed when owner changes?;
7. Authentication risk, since device is often not in physical proximity to individual; and
8. Difficulty in establishing accountability due to multiple data controllers and processors unlike in traditional data processing transactions.

In view of the above, and given that existing ISO standards do not have provisions on IoT related threat vectors on privacy, for this reason, a new study period is being proposed as in attached draft ToR.

Several organizations are working in IoT architecture and some of them also on IoT security, but very little work has been done on privacy although the threats are real now. Following are some of the references :

* ISO/IEC JTC 1/WG 10 on IoT
* AIOTI , WG3
* Article 29 WP study on IoT
* CSA
* ITU-T SG 17, SG20, ITU-T JCA-IoT

Proposed Terms of Reference for a Study Period on "Guidelines for Privacy in Internet of Things (IoT)”

ISO/IEC JTC 1/SC 27/WG 5

Taking into account the recommendations of SWG on IoT and projects in ISO/IEC JTC 1/SC 27 including the following:

* ISO/IEC 29100:
* ISO/IEC 29101;
* ISO/IEC 29134;
* ISO/IEC 29151;
* ISO/IEC 27018;
* ISO/IEC 30141.

## ****Establish****

a Study Period on a guideline for "Guidelines for Privacy in Internet of Things (IoT)” in April 2016 and

## Task the rapporteurs of the Study Period

1. assess the viability of producing guidelines for Privacy in IoT within WG5;
2. to potentially provide (a) New Work Item Proposal(s) and/or input material for existing relevant projects as a recommendation to the Working Groups 5 depending on the outcome of this assessment.

A call for contributions will be circulated after the Tampa Meeting and the National Bodies are requested to provide their contributions by July 1, 2016. The National Body contributions received in response to this call for contributions will be discussed at the ISO/IEC JTC 1/SC 27 Working Group 5 Meeting in October 2016.