IOTWeek

Dublin — June 20-23, 2022

Security & Privacy Threats

Antonio Skarmeta
David Goodman
Francesco Capparelli
Ruben Roex

GLOBAL VISION:
IoT TODAY AND BEYOND

IOTForum

END-USER'S (AND END -TARGET'S) ENGAGEMENT

Several measures have been identified in an approach that relates end-user's engagement to multiple factors.

The main factor concerns data protection and security, considered as conditions that increase trustworthiness in the usage of IoT.

The **challenge** is to develop technologies that are **inherently privacy-preserving** and can offer the basis for empowering the end-user (and more in general, the end-target) to **understand** and **be informed** of (and, where appropriate, control over) the use of their personal data.

END - TARGETS

We have to consider not only end – user but also data subjects, whose data are being collected and processed trough IoT even if not in an interactive usage.

END - USERS
=
PEOPLE THAT HAVE AN INTERACTIVE USAGE
+
OTHER DATA SUBJECTS POTENTIALLY INVOLVED

a) The most important reasons why we should engage end–users (and other data subjects) is to ***develop a democratic process*** in both the governance and business areas.

A project can include users/data subjects ***as actors*** or ***as factors***.

Most of IoT solutions are moving towards factorization of people:
people **as an object** that interacts with other sensors, condition which could potentially **contrast with general principles of the European Union law**.

b) Another reason to engage end-users is to ***educate and train them***.
Through training and education users' awareness increases and their skills in using IoT can **improve, building a self-sustaining mechanism**.

THIS HAS TO BE CONVEYED THROUGH DATA PROTECTION AND CYBERSECURITY

In order to ensure greater protection for individuals - not only data-subjects - the legislator requires that economic operators using IoT devices **think about privacy** as a general preventive measure, rather than an instrument to use after damage has been caused.

The goal is to ensure an "**individual-centric**" approach, aimed at preventing violations of individual fundamental rights (e.g. to self-determination in managing their data).

To properly engage end-users and other data subjects a necessary condition is **to increase their trust**. Only when trust and confidence are satisfied, end-users and other data subjects can be open to accept such technology.

To increase their trust some elements must be taken into account.

DATA PROTECTION → TO **ENGAGE END - USERS**

Engagement's Measures

Feedback

One of the most important things to increase end–user's trust and assess their engagement is to give them **constant feedback**. In fact, **giving credit to users** on what is happening whit their data, whit theirs input, **increases their perception of security,** making them feel subjects that are involved in the process, rather than objects from which information is harvested.
The relationship between the IoT technology and the users must not be unilateral: the information must not arrive only from the users to the device, for the latter to process it; the information must also be sent from the IoT device to the end-users so that they are constantly updated on the use made of their data.

Engagement's Measures

Feedback (Co-creation)

The end-users should be involved in the **risk assessment process** to address properly the **risks** that **users can perceive**.

The end-user should be involved in **co-creation of metrics and threats catalogues** in order to perform DPIA and Risk Assessment.

Engagement's Measures

Crowd - privacy

Enabling end-users in order to organize **self-defense measures** from cyber/privacy to **exchange information/awareness** threats on line and in IoT environments can increase end-user engagement.

Crowdsourcing mechanisms aims to identify, monitor and assess privacy-related risks and can increase trust and therefore engagement.

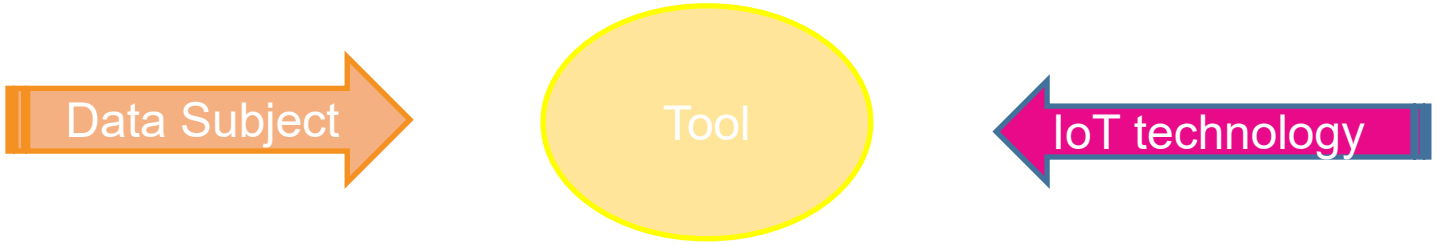
End-users would feel more comfortable **having a way to comment and alert other users on privacy-related risks**.

Engagement's Measures

Crowd - privacy (TOOLS)

Another measure to engage end-user are tools.
Tools intends to **simplify the relationship** between **IoT technology** and **data subject**: it has to be user-friendly and freely available; it has to enable them to understand, whenever they want (right of access), which kind of data are involved and the logic that rules the processing (right to receive the information/right of access), showing it continuously and promptly, each time.

A tool, for example, can be matched with a smartphone app and by using the app an end-user can discover if there are new devices or sensors around him and decide to deactivate them.



Engagement's Measures

Choices & Consent
(CONTROL PANEL)

AN EXAMPLE OF DATA PROTECTION AS A MEASURE TO ENGAGE END USERS

***EX ANTE* / OPT- IN**

In order to increase engagement and trust the end-users have to be in the condition to **choose freely if** they want to be **involved** in the data processing carried out by the IoT environment
Nonetheless, the end-users should be able to **choose freely what kind of personal** data they **share** with the IoT environment before interacting with it.

***EX POST* / OPT- OUT**

The end-users have to be able to **control their data after the process** in order to eventually exercise their rights.

For this purpose a control panel
should be installed to achieve the aforementioned goals.

Conclusions

Data Protection and Cybersecurity are the way to achieve trust and end-user engagement

IOTWeek

Dublin — June 20-23, 2022

Thank you!

Find more:

UNIVERSIDAD DE MURCIA

Cyber Security for Europe

iotweek.org