



# CSP FORUM

## Privacy and Innovation in the Internet of Things – Report

Co-located with the Internet of Things Week (London, June 16-19)

CSP Forum ([www.cspforum.eu](http://www.cspforum.eu))  
Funded by SecCord CSA ([www.seccord.eu](http://www.seccord.eu))  
Unit H4, European commission, DG CONNECT  
Consortium Partners: WIT, UNITN, HP, SAP ATOS

## Table of contents

---

Executive Summary .....	3
1. Introduction.....	4
2. Agenda.....	5
3. Outcomes .....	5
1. Industrial session.....	<b>Error! Bookmark not defined.</b>
2. Research session .....	<b>Error! Bookmark not defined.</b>
3. Panel and wrap-up session.....	<b>Error! Bookmark not defined.</b>

---

## Table of figures

---

Figure 1- Agenda.....	<b>Error! Bookmark not defined.</b>
Figure 2- Mapping research contribution to raised industrial challenges	<b>Error! Bookmark not defined.</b>

## Executive Summary

---

The constant increasing of mobile devices in our daily life is a great enabler for the Internet of Things (IoT). End of 2013, the number of mobile devices (smartphone, tablet, smart anything) has exceeded the world population. But as IoT attracts more and more the interest of industrials, privacy and security concerns, such as access control, data protection, or resilience to attacks, are increasing as well.

The CSP Forum event “*Privacy in the Internet of Things*”, organized on June 17th 2014 in London as part of the annual IoT week (<http://www.iot-week.eu/>), presented novel outcomes from current ongoing security and trust research projects in the IoT domain, as well as discussed how privacy and data protection can co-evolve with IoT applications.

## 1. Introduction

The constant increasing of mobile devices in our daily life is a great enabler for the Internet of Things (IoT). End of 2013, the number of mobile devices (smartphone, tablet, smart anything) has exceeded the world population. But as IoT attracts more and more the interest of industrials, privacy and security concerns, such as access control, data protection, or resilience to attacks, are increasing as well.

CSP Forum identifies Privacy has a significant topic for its cluster activity, and Privacy in IoT shows major research challenges. CSP Forum wanted to bridge security and trust research community with IoT practitioners, and this is why it organized the Privacy in the Internet of Things workshop in the context of the annual IoT week (<http://www.iot-week.eu/>). The IoT week is a major, yearly, event on the Internet of Things, which gathers researchers, industries, and practitioners discussing current technologies as well as future challenges, including their societal impact. This year, the IoT week also benefitted by the integration in the London Technology Week (<http://londontechnologyweek.co.uk>), that contributed to extend the reach of the IoT event.

The Privacy in the Internet of Things workshop combined short presentations and a panel, and introduced research results from current ongoing security and trust research projects (not only EU FP7, but also UK national-funded initiatives) in the IoT domain, as well as discussed how privacy and data protection can co-evolve with IoT applications. The IoT week event featured also two workshops organized by the EU-funded projects CUMULUS and TRESCCA. All in all, this CSP Forum event reach-out to a key industrial area and disseminated there novel privacy and data protection research outcomes to a wide community, including UK national stakeholders.

## 2. Agenda

Table 1 presents the agenda of the CSP Forum on Privacy in the Internet of Things (also available here: [http://www.iot-week.eu/privacy\\_innovation\\_iot.html](http://www.iot-week.eu/privacy_innovation_iot.html))

Table 1: agenda

Contribution	Speaker	Projects
Innovation and Personal Data	Dr Galwas	UK Catapult centre
IPACSO: Towards developing an innovation framework for ICT innovators in the Privacy and Cyber Security Markets.	Jamie Power (WIT)	IPACSO
Privacy for mobile devices	Jonas Jensen (Alexandra Institute)	ABC4trust
Enhancing data control: from cloud to mobile... and back	Laurent Gomez (SAP)	CocoCloud
Panel	Moderated by Laurent Gomez (SAP)	

## 3. Outcomes

The privacy-focused national UK project/initiative Catapult centre discussed personal data protection. Novel methods and technologies to enhance the control and the security of personal data in in mobile devices and sensor networks developed within the ABC4trust (<https://abc4trust.eu/>) and Cococloud (<http://www.coco-cloud.eu/>) research projects were presented. The EU funded project IPACSO also contributed by providing an insight of an innovative model framework for privacy and cybersecurity, detailing its relevance to the IoT area. A panel with open floor discussion concluded the event. More details are provided hereafter.

- Innovation Challenges where IoTs and Personal Data meet.*

Dr Galwas from UK Catapult centre, introduced the innovation challenges where IoT technologies are used to collect/consume Personal Data. The worlds of Personal Data and Internet of Things (IoT) are colliding to create a plethora of opportunity. But, there are growing concerns as personal and business interests are balanced against a framework of broadening regulations. Social and cultural aspects, as “Winning people’s hearts and minds” is as important as the security measures that pervade the space, and innovation is key on both fronts. In this context, ‘Privacy by design’ is emerging as a key mind-set: technologies and solutions must embrace our ‘wish to share’ with the ‘need to identify’. The underlying security mechanisms typically cross-cut multiple solution components, yet the IoT is populated by a massively diverse set of products, each contributing to the ever-growing pool of increasingly real-time data.
- IPACSO: Towards developing an innovation framework for ICT innovators in the Privacy and Cyber Security Markets.*

Jamie Power presented the project IPACSO (<http://ipacso.eu>), an EC FP7 Coordination and Support Action, focused on the assessment and exploitation of market opportunities across Privacy Cyber Security industry domains. IPACSO developed a knowledge and decision-support framework for identifying, assessing and exploiting market opportunities across the PACS (Privacy and Cyber Security) industry domain. To this aim, the project identified existing market drivers, inhibitors, environmental influencers, different applicable innovation models from other industries. The IPACSO framework supports different stakeholders (security innovators in industry and academia) in the PACS space to identify, assess and exploit new ideas (and emerging research outcomes) using innovation and market assessment best practices. IPACSO also reaches out to PE markets (Private Equity) and supports organizations (existing innovation support companies, brokers, etc.) to facilitate the process for development.
- Privacy for mobile devices.*

Dr Jonas Jensen, from Alexandra Institute Security Lab in Denmark, presented the recent results of ABC4Trust, <https://abc4trust.eu>. ABC4Trust aims at providing a Privacy preserving attribute based credential allowing user to authenticate while revealing minimal information on their identity. So far, credentials such as digitally signed pieces of personal information or other information used to authenticate or identify implies the user disclosing her personal data. In fact, users often reveal a large amount of personal data, even though the application needs much less information, for instance only the confirmation that the holder is a teenager or is eligible for social benefits. Privacy-preserving Attribute-based-credentials (Privacy ABC's) solve this by allowing a user to reveal just the minimal information required by the application, without giving away full identity information. The ABC4Trust project has created a common framework for existing privacy ABC technologies and has tested it in pilot projects, showing that it is feasible to use these technologies in real world applications.

- Enhancing data control: from cloud to mobile... and back

Dr. Laurent Gomez presented a recent European funded project CoCoCloud (<http://www.coco-cloud.eu/>) related to the secure data sharing. CoCoCloud aims at providing a cloud based framework for the enforcement of data sharing agreements both on the cloud and on mobile. Data sharing agreements are defined based on regulations (EU or national) and data subject privacy preferences. In order to demonstrate the feasibility our CoCoCloud approach, three uses cases are developed in the scope of the project: healthcare, public administration and corporate data sharing. The technology has been demonstrating in a healthcare scenario, related the patient information sharing between patient and physicians in a hospital. The healthcare scenario, supported by Quiron Hospital from Valencia in Spain, shows the patient information sharing between patient and physicians. A public administration scenario aims at securing citizens information sharing between citizens themselves, but also with different public administrations. This scenario is supported by AgID, the Italian Digital Agency. A third use case, related to internal information sharing between the cloud and mobile devices within a private organization, is supported by SAP.

## 4. Conclusions

Privacy and Innovation in the Internet of Things forum gave us the opportunity to further understand, develop, and discuss the privacy challenges related to the Internet of Things. With an increasing interest from industrial, IoT calls for solutions in order to preserve individual's (e.g. customers, citizens) privacy. In this context, projects such as ABC4Trust and CoCoCloud, demonstrated how recent results from research may be used to support innovation in IoT while addressing privacy in Europe.