The Future of the Internet of Things in Europe

Brussels, 26 November 2015

Conference Report

Contents

1. Introduction

Almost all technology and market forecasts agree that by 2020, for every PC, phone or tablet connected to the internet there will be five to ten other types of devices sold with native internet connectivity. This sets the stage for the Internet of Things (IoT) as a global system connecting people, data and tens of billions of physical or virtual 'things' using interoperable communication protocols. The success of the IoT is predicated on the parallel and complementary development of cloud technologies, semantic and big data technologies, and future networks such as 5G. This emerging ecosystem enables a deeper meshing of the world of machines into the digital world that can transform global industry yet again.

The conference on the Future of the Internet of Things in Europe was organised by the Digital Enlightenment Forum (DEF), Huawei Europe and the Parliament Magazine in cooperation with the Alliance for Internet of Things Innovation (AIOTI). The meeting brought together policy makers, technology experts and industry representatives in view of making concrete recommendations on how to meet specific challenges inherent in emerging policy, technology and application issues. It included breakout sessions in each of these areas, as well as keynotes on the IoT ecosystem and trust and societal impact. Around eighty people attended in Brussels, while more than one hundred and twenty followed streamed sessions via the internet.

Presentations from the meeting and a full recording of the event are available from the Digital Enlightenment Forum website.[1]

2. The IoT Opportunity and the European Approach

Opening the meeting, **Prof. George Metakides, President of DEF**, noted that a complex ecosystem is emerging through the convergence of cloud computing, fifth generation mobile (5G), and IoT. This new ecosystem is full of promise but also brings threats and risks. While IoT evangelists wax lyrical about the benefits, our enthusiasm for IoT needs to be tempered by a cogent policy in the context of a global single market strategy. We have to put "people in the middle" rather than treat them as a subset of "things", Prof. Metakides argued, ensuring interoperability but also security and trust in the new digital world that is emerging. Hence, the workshop focused not just on technology and services but also on issues such as trust, security and standards.

Mario Campolargo, Director at DG-CONNECT, European Commission, provided an overview of the EU's approach to and expectations of the Internet of Things.

It is clear, explained Mr Campolargo, that today we live in a hyper-connected society. Billions of devices are already connected to the internet and many more will be connected by 2020. These new technologies bring completely new approaches in business models. The issue is no longer about technology but about the impacts on business processes and innovation; about new services that were not available before; and about new innovation ecosystems where startups can grow quickly into businesses with global reach. In short, the Internet of Things is at the heart of the EU's thinking of what future markets will be. Echoing Prof. Metakides, Mr Campolargo emphasized that the central question should be: "Where does the human sit in this?".

The European Commission has recently issued its Work Programme 2016-17 for Research & Innovation in Information & Communication Technologies (WP2016-17) as part of Horizon 2020. IoT features prominently in the proposed actions; it is effectively the first time that IoT has been addressed as a cross-cutting issue in the EU's ICT research. By treating IoT as a cross-cutting issue, the

---

[1] See https://digitalenlightenment.org/event/future-internet-things-europe

Commission is aiming towards a more holistic approach that combines technological development, in areas such as cyber-physical systems, data, and communications, with societal challenges. 5G, in particular, offers opportunities to make applications and services more accessible and easier to manage, but still poses major research challenges.

For Europe to lead in IoT, we need a level playing field across sectors, not just strength within specific verticals. Vertical sectors such as environment, transport and health all have interlinked requirements and the distinctions between them will gradually disappear. New services and business models will emerge as a result of this data fusion.

At the centre of the European strategy is a series of Large-Scale Pilots (LSPs) that aim to integrate the whole value chain in specific application areas. The Commission intends to invest around €100m in LSPs across a broad range of applications such as smart agriculture, smart cities, connected cars, and wearables (approximately €20m per project). The LSPs will trial not just technology but also new business models and address issues such as interoperability and security. International partners such as Korea, Brazil and Japan will also be involved. DG-CONNECT strongly connects with other DGs, such as Agriculture, so as guarantee a strong user perspective. The LSPs are intended to have a catalysing effect on the IoT market and cooperation with stakeholders such as the AIOTI will be key to their success.

Turning to policy, Mr Campolargo noted that the Single Market is essential to IoT. The new services and applications depend, to a large extent, on the free flow and common interpretation of data. Car number plates are one example: services such as traffic charging and connected cars will depend on barrier-free access to data across Europe and beyond. This presents fundamental challenges to our understanding of issues such as trust and security Europe wide; yet if the services are not trusted by citizens then they will not flourish. Data non-ownership – data that is ours but is of use for society – is another important issue. The Commission expects to issue a reflection on these new policy challenges – in the form of an official Communication – during 2016.

Summing up, Mr Campolargo observed that Europe needs to have a pro-IoT attitude. Through a combination of research, catalysing value chains through the LSPs, and forward-thinking policies, Europe can lead in global IoT markets.

3. The Emergence of the IoT Ecosystem

Karabet Krikorian, Head of WEU IoT & Industry 4.0 Solution Innovation, Huawei, presented an overview of technology developments from Huawei's perspective. The company is active across a broad range of markets, from transportation, manufacturing and oil & gas, to smart energy and telcos, serving both enterprises and consumers. Its open platform, based on interoperability between verticals, offers customers flexibility so that they can launch and control new solutions as they wish.

Huawei's Smart Home strategy, for example, follows a horizontal approach, combining home monitoring, home security, home entertainment, home automation, and home health within a single IoT platform. Similarly for the Connected Car, where Huawei is working across the automobile value chain. Other examples include: predictive maintenance of cement trucks to ensure the quality of cement delivered to construction sites; and use of advanced IoT-based solutions in the logistics industry to improve response and delivery times.

Huawei sees partnering as essential to the success of IoT: "Without partners we will not get anywhere", Mr Krikorian concluded.

The Alliance for IoT Innovation

AIOTI was launched by the European Commission in March 2015 to create a vibrant IoT ecosystem in Europe, and aims notably at breaking silos between leading vertical IoT application areas.

AIOTI will be an important tool for supporting the policy and dialogue within the Internet of Things (IoT) ecosystem and with the European Commission.

AIOTI builds on the work of the IoT European Research Cluster (IERC) and expands activities towards innovation within and across industries. This also offers an opportunity to discuss legal obstacles to further IoT take up, and to forge consensus. The Alliance will also help the Commission prepare future IoT research and innovation, standardization and policy.

AIOTI has established a series of twelve Working Groups to investigate innovation-related issues and to make recommendations. The Working Groups have recently published their first reports, which were referenced frequently within the Conference presentations and discussions.
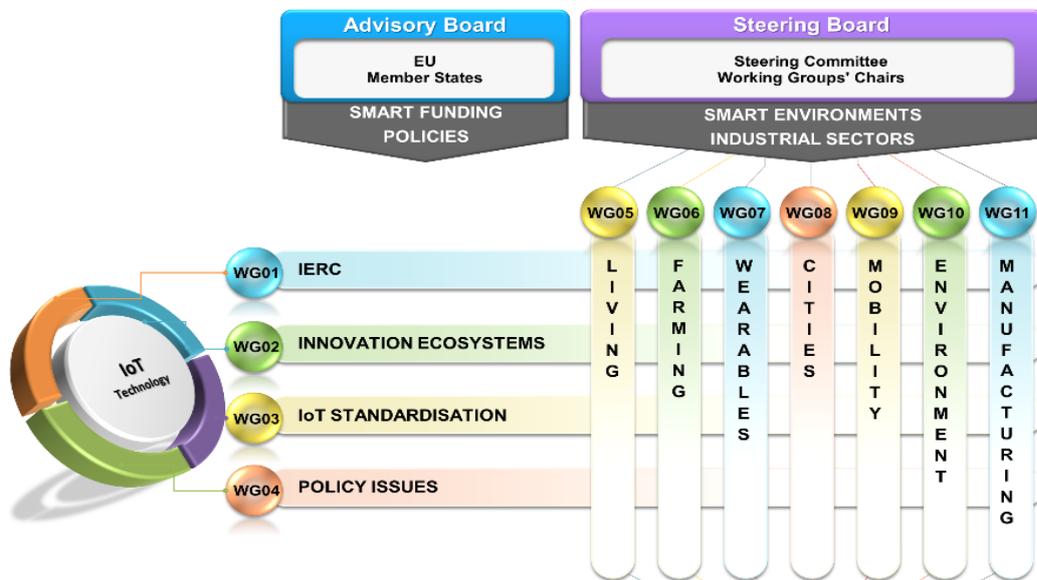
For further information see: www.aioti.eu

Wim de Waele, CEO of Eggsplore, an investment company based in Belgium, and founder of the business incubator iMinds, focused on IoT as a driver towards an ecosystem economy. The rate of mass adoption of new technologies is unprecedented, Mr de Waele explained. According to Business Insider, the number of IoT devices installed worldwide will increase fivefold, from around 5 billion in 2015 to around 25 billion in 2020. However, the financial sector is lagging behind in the adoption of applications such as mobile banking.

Today, the convergence of data science, distributed trust and everything connected brings a world of hyper-scalability. Distributed trust, where central authorities no longer manage transactions (as in Block Chain) has the potential to transform various domains in the same way that peer-to-peer (P2P) has done in content. A block chain-type app for identity verification, for example, would be highly disruptive.

Putting these trends together, it is clear that we are evolving rapidly towards a platform economy. The hyper-scalability this offers has major implications for businesses. Dominant players are seeking to build offers that bring together partners (for example, a bank, an equipment supplier and a network operator) to deliver new solutions, such as API banking. Sectors are converging.

The insurance industry is an example of a sector that is being disrupted by IoT. Companies such as Scanadu (www.scanadu.com) are developing a new generation of mobile consumer medical devices that empower people to monitor and better understand their own health. Although founded in Belgium, the company perceived the health insurance market in Europe to be over-regulated and so moved to California in order to raise investment and trial its products.

In conclusion, Mr de Waele recommended that we work towards a user-driven, citizen-centric internet, for example by focusing on personalising the customer experience; and we ensure that the proposed Large-Scale Pilots address regulatory and policy issues, not just technology.

4. IoT Policy

Chair: Thibaut Kleiner DG-CONNECT, European Commission

Introducing the session, Mr Kleiner noted that this is a key moment in the policy debate. IoT is a complex area, touching on many important policy domains. It is also central to the Digital Single Market (DSM) initiative. The Commission is planning a consultation on policy for IoT, addressing issues such as trust, security and regulation. Is there, or should there be, an IoT policy as such, something that is distinct from other areas of ICT? The consultation will seek to delineate which aspects are generic within the DSM and which are specific to the IoT arena as far as policy is concerned. This aspect has received relatively little attention over recent years, so there is a need to consult with industry and other stakeholders to see what is needed. The Session was a first opportunity for stakeholders to input to this debate.

Discussion in this area is being informed substantially by the work of AIOTI Working Groups. **Robert MacDougal of Vodafone and Chair of the AIOTI Policy Working Group** formally introduced the AIOTI and its work. Founded in March 2015, the Alliance for IoT Innovation comprises more than 300 members, primarily industry representatives, who are working together on innovation issues (see box above).

Working Group 04 – Policy has focused on identification of existing or potential market barriers that prevent the take-up of IoT in the context of the Digital Single Market, as well as from an Internal Market perspective. Its first report makes horizontal policy recommendations across four main areas: privacy, security, liability and net neutrality.

In relation to privacy, the Working Group strongly advocates the adoption of privacy-by-design best practice by AIOTI members, as well as the creation of an 'AIOTI Privacy Knowledge Base', and European Commission sponsorship of an accredited privacy engineering programme. On security, the WG stresses that systems are only as strong as their weakest link. In systems comprised of diverse stakeholders and technology, there is a need to embed security in both technologies and standards. On issues of liability and net neutrality, the WG proposes that the emphasis should, in the main, be on the development of policy solutions.

Cornelia Kutterer, Policy Director, Microsoft EMEA, argued that IoT represents an inflection point. The convergence of cheap hardware, pervasive connectivity, accessible development environments, escalating user benefits, and new innovative scenarios brings opportunities for all. Today, "Every company is a data company", as device connectivity and management together with analytics bring new operational insights, which in turn open up new insights for the business.

Key policy areas include:

1) Privacy, security and data access: the GDPR presents major challenges and companies will need to think through how to comply. We should be wary of recommendations that may be too prescriptive, such as codes of conduct.

2) Contractual and IP issues: including data ownership (a new concept under the DSM), multi-party pools, trade secrets, and liability. New areas of law will evolve in these spaces and the legal community should be involved.

3) Market regulation and connectivity: including net neutrality/platform neutrality – important issues relating to how future ICT markets will be regulated. Whether we have more or less competition in this space will determine the sort of partnerships that are (or are not) formed.

4) Ethics and societal issues: such as behavioural experimentation, predictive analysis, discrimination and individualisation of risks. If we wish to move on with IoT adoption, then we have to bring citizens with us.

Underpinning all these is standards as a horizontal issue.

Sébastien Ziegler, Director, Mandat International and President, IoT Forum looked at trends and convergences in the IoT landscape. With more and more IoT available, direct interaction with end-users brings new sets of questions and the need for a more holistic approach. Pervasive testbeds are being deployed, allowing citizens to explore, test, validate and improve on new applications and services. The traditional view of the research cycle is changing from top-down to more bottom-up, bridging the gap between researchers and end-users.

The General Data Protection Regulation (GDPR), due to enter into force by April 2016, represents a major departure in the EU's approach to regulation. It increases the legal obligations for companies and end-users, has global scope (i.e. will affect companies in US and Asia if they process European data), and introduces legal and financial risks for those who do not comply. Projects such as Privacy Flag (www.privacyflag.eu) and IoT Privacy & GDPR Certification (www.europrivacy.org) are assessing the risks and investigating solutions.

A "silent revolution" is taking place within the internet. The remaining free address blocks under Internet Protocol version 4 (IPv4) are being exhausted. This is forcing a migration towards the Internet protocol version 6 (IPv6) whose adoption is increasing very quickly. IPv6 provides an addressing scheme able to cope with the scalability requirements of the IoT. Most emerging IoT standards are now converging towards IPv6 and projects such as UDG (www.devicegateway.com) have demonstrated the integration of over 40 IoT standards together with IPv6, which can therefore be seen as an essential tool for IoT integration.

Finally, Mr Ziegler suggested some recommendations for the EU research programmes, namely: to focus on an IoT cross-domain approach; to make IPv6 a requirement for future IoT calls; to focus European 5G research on IoT requirements; and to promote international cooperation and global presence (through forums such as ITU, ISO and IoT Forum).

In discussion, the question arose as to whether the EU's regulatory framework will make it more difficult for companies to comply. Mr MacDougall said that companies would accept horizontal frameworks as they evolve and that an emphasis on approaches such as privacy-by-design would avoid the need for discrete action. Ms Kutterer saw multi-party data pools as very challenging. How can a subject ask for their data to be deleted and ensure compliance, and how will processes be adapted within companies and across value chains? We have to be very forward looking, she concluded. Mr Kleiner added that IoT takes us into new territory: a world with billions of devices reinforces the need for privacy-by-design but also for guidance to companies on how to implement the rules in a way that guarantees legal certainty. The new framework is intended to bring harmonisation across Europe.

In response to a question regarding the GDPR, Mr Ziegler noted that the Regulation will not target IoT specifically but relates to all personal data. While the GDPR imposes high requirements, it will also pave the way to innovative solutions, including for end-users and citizens. Companies mastering these requirements will benefit from a competitive advantage.

Asked whether spectrum represents a limiting factor, Mr MacDougall responded that potentially it did for certain applications, such as the connected car. This will be considered in the next phase of WG04's work on policy.

5. IoT Standards

Chair: Yun Chao Hu, Director Standardisation and Partnership Strategies, Huawei

The situation regarding standardisation is highly complex, Mr Hu observed. AIOTI's Working Group 03 on Standardisation had identified more than 50 organisations involved in developing and issuing standards in relation to IoT. The Working Group had provided a useful mapping of these initiatives, as well as those involved in high-level reference architectures and semantic interoperability. Open source is changing the standards world rapidly but there are still enormous interoperability issues to resolve, as well as opportunities for new business models and engagement issues.

Jacopo Cassina, CEO of Holonix and a member of the AIOTI Working Group 03 provided further detail on the Group's work on standards. The work of WG03 is seen as a reference for the AIOTI Working Groups in order to address the interoperability issues and to recommend the use of standard-based solutions for the deployment of IoT solutions. The Group has consulted with SDOs[2] and Alliances about collaborations and interworking as a means to reduce fragmentation. AOITI brings a dramatic acceleration of the pace of those discussions.

Semantic interoperability across the various application domains is a major issue for IoT. Key challenges include: ontologies that formalize the meaning of domain data and information models; ontology merging, matching and alignment strategies across domains; semantic discovery of services, devices, things and their capabilities; and semantic metadata.

Going forward, the Group aims to leverage its results in existing IoT standardisation efforts; use as inputs on standardisation to the LSPs; and provide guidelines for prospective future projects.

Harm Jan Arendshorst, Head of IoT Product Development at Verizon, addressed the need for IoT product standards. The ecosystem of competing standards and associated trust issues identified by the AIOTI WG03 represents a major challenge. Yet accessible and well-defined standards are essential for consumer confidence and unleashing their innovation potential.

Verizon's approach has been to create a tightly interconnected ecosystem that helps its customers on that journey. Its IoT platform, called ThingSpace, was created for developers and customers to accelerate IoT adoption. ThingSpace comprises three components: Develop, a developer community with easy access to Verizon APIs; Manage, a portal covering all self-serve IoT platforms; and Market, providing access to IoT services, solutions and applications developed by Verizon and its partners.

Ulrich Seldeslachts of LSEC, a European network of security professionals, research and industry, provided an industrial perspective on IoT in practice, based on working with SMEs in the Flanders region, Belgium. Manufacturing SMEs today are very far from working with anything that could be

---

[2] Standards development organisations

called 'standards'. We first have to convince them what IoT could mean for their businesses and then bring them along and find converging views.

For example, Thyssen, the elevator manufacturer, is fundamentally changing its business model from installing and maintaining elevators and lifts, to preventive maintenance of lifts and elevators. It is able to provide this service over the internet thanks to the many sensors and actuators embedded within its products. Another example is the American confectionery manufacturer Mars Inc., which now has certain factories operated by third parties under service level agreements. In short, we are seeing the emergence of Manufacturing as a Service (MaaS).

Turning to standardisation, Mr Seldeslachts noted that standards can offer powerful incentives for companies to interconnect. In markets such as IoT, they can drive innovation, while too many competing standards can lead to standards wars, where dominant players generally have the advantage. He then expanded in greater detail on the definition and advantage of open standards and recent developments in this area.

One participant expressed surprise at the number of standards organisations involved in this arena. Panel members responded that this reflects the innovation potential of IoT but agreed the situation was not necessarily conducive to an innovation culture. Consolidation is inevitable but at present it is not clear which standards will win through. AIOTI could be the linking pin here and play a major role in helping the various initiatives to find common ground.

What role is there for government involvement here apart from promoting cooperation, another participant asked? Mr Cassina cautioned against too much government involvement: we are in an ideation phase and regulation could shut down opportunities too quickly. However, Mr Seldeslachts disagreed, arguing that regulations were likely to emerge in relation to critical infrastructures.

Should implications for bandwidth also be considered? Individual IoT devices require very little bandwidth but, of course, mass deployment means that bandwidth issues cannot be ignored. In transport, for example, there are issues around vehicle-to-vehicle systems, where current networks struggle to handle inter-car communications.

How does Europe balance privacy and security? Mr Arendshorst noted that different settings and use cases demanded different approaches. Mr Seldeslachts thought privacy-by-design an important response, though clearly this is not required at all levels.

6. Trust and Societal Impact

Frédéric Donck, Director of the European Regional Bureau of the Internet Society (ISOC), presented the ISOC perspective on the Internet of Things. He professed amazement at how the internet, which was conceived more than 25 years ago, has been able to adapt to the IoT and all of the other developments that we see today. The internet's success is due primarily to its unique development model. This is based on: shared global ownership with no central control; open technical standards; collaborative engagement models; freely-accessible processes for technology and policy deployment; and transparent and collaborative governance.

The ISOC sees five key issues in relation to future internet development. The first is security: do we as users have a full view of what we mean by security? In our world there is not, and cannot be, any such thing as 'absolute security'. In a fully connected world we need a better appreciation of the risks and trade-offs, including the ecosystem risks (i.e. the risks from others' devices through being part of a network). IoT poses some unique security challenges. Most devices do not have embedded security layers but have lifetimes longer than most computers. Also, devices generally do not report their

(over)performance or non-functioning. In essence, a device <u>on</u> the internet is a device <u>part</u> of the internet and hence we have to look to more collaborative approaches to security. Other key issues highlighted were privacy, interoperability and standards, regulation, and development.

Summing up, Mr Donck observed that IoT brings many challenges and opportunities and hence collaboration across a wide range of stakeholders is essential.

Jacqui Taylor, Founder and CEO of FlyingBinary, UK, spoke about putting the citizen at the heart of IoT. FlyingBinary is a supplier to G-Cloud, a ground-breaking initiative by the UK Government to bring the efficiency, scale and cost benefits of cloud computing to the public sector. Using a pre-approved OEJU framework, the procurement overhead associated with traditional ICT purchasing is minimised. The company is one of hundreds of suppliers accredited to provide public, private, hybrid and community cloud offerings through the UK Digital Marketplace. These cloud services are helping to break down silos across government by leveraging the data without the need to create expensive bespoke solutions.

Smart Cities will be a key use case for IoT. In the UK, the British Standards Institute (BSI) has launched a family of standards for Smart Cities. These establish a good practice framework for city leaders to develop, agree and deliver smart city strategies that can help transform their city's ability to meet its future challenges and deliver its future aspirations. The BSI Smart City standards distil current good practices into a set of consistent and repeatable patterns that city leaders can use to help develop and deliver their own smart city strategies. Rather than a one-size-fits-all model, it focuses on the enabling processes by which the innovative use of technology and data, together with organisational change, can help deliver diverse visions for future UK cities in more efficient, effective and sustainable ways. Developments such as these will help the UK to move beyond smart cities to 'resilient and sustainable cities', focusing on issues such as citizen participation: how can citizens actively co-create?

We also need more citizen-centric health services. In the UK, NHS Citizen is a national programme to give the public a say on healthcare matters and influence the National Health Service's decision making. Issues raised by members of the public are selected for discussion by senior NHS leaders and citizens at the NHS Citizen Assembly meetings twice a year.

Specific and innovative efforts are needed to engage both with those citizens who are still not online (18% in the UK) and with Generation Z, the under-25s who have largely disengaged from certain online platforms. FlyingBinary's work in the UK, for example, has succeeded in establishing a dialogue on health issues with young men via PlayStation4, their 'trusted zone' online environment.

Citizens, concluded Ms Taylor, will drive the value of their data as part of this connected IOT agenda.

7. IoT Applications

Chair: Prof. Atta Badii, Intelligent Systems Research Laboratory, University of Reading

Tamme van der Wal, of AeroVision BV in the Netherlands, was unable to attend the meeting but his presentation of the ICT 2015 conference was made available to participants. His presentation asked the question: How can IoT improve farming? The response was in a number of important ways. Firstly, IoT applications can provide real-time virtualisations of agri-industry value chains. Secondly, they operationalise and standardise connectivity within this most traditional sector. Thirdly, they create intelligence through: data quality assessments, data refinery, and data analytics (predictive systems). Finally, IoT can help integrate best practices and make them available to help farmers to reach their targets.

Markus Dillinger, Director for Industry Communication Applications, Huawei European Research Centre, provided an overview of 5G issues affecting IoT. Connectivity is the key for value-added IoT applications. Complex sensors are processing data in real-time according to algorithms. Data fusion from distributed multi-sensor sources complements the real-world representation, and increased network capacity is demanded for fully-fledged IoT development. In short, increased capabilities in IoT-based systems create demands that can only be addressed by 5G connectivity.

Huawei is pursuing these developments as part of the Car-2-Car Communication Consortium, a European-funded research project. It aims to develop an automation platform supported by 5G which will be implemented in test vehicles.

Hans Schaffers of Saxion University of Applied Sciences, Netherlands and Aalto School of Business, Finland focused on creating societal value with IoT for smarter cities. AIOTI's Working Group 08 has proposed a smart city technology strategy, which is presented in the Group's recent report.

The report aims to prepare the ground for large-scale IoT pilots for smart cities ("Reference zones in EU Cities") and states the intention to create a city-centric ecosystem based on state-of-the art technologies. Although the report mentions the need for combined top-down and bottom-up approaches, Prof. Schaffers thought the work to be too technology centric. "How will this connect with decentralized innovation models and social & collaborative innovation", he asked? "How to marry IoT technology strategy and CAPS (Collective Awareness Platforms) thinking?"

Recent work by US researcher Anthony Townsend provides some insights into how IoT can address the challenges faced by cities and regions.[3] Such challenges include: enhancing inner city attractiveness; strengthening the innovation ecosystem; maintaining security and safety; efficient use of resources and infrastructures; and strengthening a bottom-up grassroots culture. We have to recognise that cities are complex social ecosystems and that change comes from both bottom-up and top-down. Therefore, we have to allow innovation ecosystems (what Townsend refers to as 'Civic Laboratories') to emerge as breeding grounds for innovation in smart cities. In Europe, the Open and Agile Smart Cities (OASC) initiative is an example of an activity that is aiming to create an open smart city market based on the needs of cities and communities.[4]

Summing up, Prof. Schaffers said that we need different ways of thinking about piloting and 'engineering', for example by incorporating the living labs concept and socio-technical systems engineering. In addition, cities need to share technologies, software, and expertise in setting up and managing (common and complementary) pilots.

Patrick Kennedy, of the European Factories of the Future Research Association (EFFRA), presented a manufacturing perspective on IoT. IoT is a multi-sector issue that relates to all of the 'Factories of the Future 2020' partnership (FoF) and its research and innovation priorities. Preparations for IoT are underway via FoF projects and it is expected to be an increasing feature in future FoF calls.

EFFRA is an active member of AIOTI's Working Group 11 on Manufacturing, which provides an opportunity to explore how smart manufacturing meets horizontals and also for the manufacturing community to exchange knowledge and approaches with others. The EFFRA Innovation Portal provides a one-stop resource for FoF-related projects, results and demonstrators, including IoT developments (see www.effra.eu/portal).

---

[3] *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia*, Anthony M. Townsend, Norton & Company, 2013.
[4] In technological terms, OASC combines: the FIWARE (EU-funded) cloud platform; CitySDK data model; and CKAN as open data platform

Thomas Kallstenius, CTO of iMinds and Co-Chair of the AIOTI Working Group 07 - Wearables, described his personal experiences with mobile medical devices. Having used a simple phone-based app to track his sleep patterns, he found unexpected correlations between sleep and heart rate during the course of the night. A doctor was unable to explain these variations and suggested a referral to a specialist. Nevertheless it appears that these patterns were not uncommon for most people, but rather unknown in the medical profession.

The experience points to a number of important lessons. Firstly, who owns this data and how can the user's privacy be protected? Secondly, all stakeholders – including professionals such as doctors – need to be involved and understand modern data sets. Are we prepared for this in the context of the LSPs? Thirdly, wearables such as this are not categorised as 'medical devices' because they are not clinically certified. Although they produce useful and viable results, polls show that clinical validation would significantly increase their market potential; however, such accreditation is extremely costly. We need business models that enable device manufacturers to bridge the 'second valley of death' for non-accredited medical devices.

In discussion, the panel was asked how data owners within vertical industries could be encouraged to share with others. What incentives should be offered? Mr Kallstenius agreed that the issue is very complex. Ownership of data is often not transparent and in many cases the simple tick-box approach to consent does not offer sufficient safeguards. Consent has to be given with full knowledge and be revocable.

Is FIWARE intrinsically better than other platforms or just financially attractive, one participant asked? Should the public sector (EU and Member States) be involved in this field at all? Panel members noted that FIWARE has been jointly funded by the EU and the private sector and that early take-up will help create a network effect. IoT applications are often complex socio-technical systems requiring multi-stakeholder engagement. EU funding allows people to collaborate across borders, which often is not allowed under national funding rules. There are a huge range of initiatives across Europe, such as the OASC which now has over 60 cities working together.

The final word went to an online participant, who commented that: "It is necessary to achieve risk reduction and leverage large scales within the EU and globally. Those scales will be achieved by corporations exclusively if nation states fail to work together."

8. Conclusions

The Conference explored a wide range of issues relating to the emergence and future prospects for IoT in Europe and stimulated much debate, both within the formal sessions and during the networking breaks.

The Conference's key messages were the following:

1) **The hyper-connected society facilitated by IoT presents major opportunities for Europe.** The convergence of data science, distributed trust and ubiquitous connectivity is bringing a world of hyper-scalability that will transform Europe's economy and society. Traditional business models are being disrupted. Boundaries between sectors are breaking down. Citizens are becoming innovators and holding traditional authorities to account. Europe has to embrace this new hyper-connected world in a way that puts the human at the centre.

2) **Europe must have a pro-IoT attitude**. The Internet of Things poses many challenges and threatens established ways of thinking and doing. We should focus on the positive rather than putting barriers in our way. The newly-formed Alliance for IoT Innovation is already making a

valuable contribution here, providing a focal point for stakeholder efforts in building a vibrant and innovative IoT ecosystem.

3) **The Large-Scale Pilots should address more than just technology**. The LSPs represent an important development in the EU's approach to IoT, addressing it for the first time as a cross-cutting issue to be tackled in a holistic way. The Conference emphasized the need to ensure that the pilots were driven by users; that they address business models as well as interoperability, security and privacy; and that they be testbeds for regulatory and policy issues as well as technology. The Conference also recommended that European 5G research be focused on IoT requirements and that IPv6 be made a requirement of IoT calls.

4) **Trust, security and privacy demand innovative approaches:** Issues such as trust, security and privacy present major challenges to the adoption of IoT which must be tackled for businesses and end-users to have confidence in new services and business models. These issues should be resolved through a combination of education, collaborative approaches, and efforts to embed security and privacy through technology and standards.

5) **Positioning Europe for the ecosystem economy**: The transition to an ecosystem economy demands innovative and forward-thinking approaches to policy and regulation. These should range from support for open platforms, such as FIWARE; to ensuring a level playing field for high-tech start-ups with disruptive innovations (for example in mobile consumer medical devices).

6) **International cooperation and global presence**. Europe has the opportunity to lead in business and societal applications of IoT. To do so it should exchange best practices with international partners and adopt a strong presence in international forums, including efforts to simplify the highly complex standardisation landscape.