Report from Dagstuhl Seminar 17412

Internet of People

Edited by

Elizabeth M. Belding[1], Jörg Ott[2], Andrea Passarella[3], and Peter Reichl[4]

1 **University of California – Santa Barbara, US,** ebelding@cs.ucsb.edu
2 **TU München, DE,** jo@in.tum.de
3 **CNR – Pisa, IT,** a.passarella@iit.cnr.it
4 **Universität Wien, AT,** peter.reichl@univie.ac.at

Abstract

This report provides a summary of the organization, program, and outcome of the Dagstuhl Seminar titled "Internet of People". We first provide the main motivations for organising the seminar. Then, we briefly describe the organisation goals of the seminar, and summarise the rationale for the set of researchers involved. We then report on the activities carried out during the sessions, consisting of talks and group works. Specifically, we provide the abstracts of the talks and extended reports on the output of the groups work. Finally, we draw the main conclusions of the seminar.

Seminar October 8 – 11 , 2017 – http://www.dagstuhl.de/17412
1998 ACM Subject Classification C.2.1 Network Architecture and Design, H.1.2 User/Machine Systems, H.3 Information Storage and Retrieval, J.4 Social and Behavioral Sciences
Keywords and phrases Internet design; Next Generation Internet; human-centric Internet; social-aware Internet
Digital Object Identifier 10.4230/DagRep.7.10.42

1 Executive Summary

Elizabeth M. Belding
Jörg Ott
Andrea Passarella
Peter Reichl

The key objective of the seminar was to bring together a diverse group of researchers and practitioners to reflect on technological and social issues related to the emerging concept of Internet of People (IoP). The group of attendees was composed of 28 people with diverse expertise on the various areas of Internet, coming from Europe, US, Asia and Australia.

The group worked for two and a half days, and the work was organised on (i) seed talks, (ii) snippet talks on selected research topics related to IoP, and (iii) parallel group work. The group sessions were particularly productive, and attendees worked on many topics. Specifically, they covered the following topics: (i) IoP definition, (ii) IoP use cases, (iii) IoP and people; (iv) Privacy, security and trust; (v) IoP architecture, and (vi) transition towards IoP. Over the last day, the group again split in three sub-groups, to focus on conclusions and follow-up activities. Specifically, the three groups produced (i) guidelines for IoP toolkits, (ii) a possible IoP research agenda, and (iii) an IoP manifesto.

Internet of People, *Dagstuhl Reports*, Vol. 7, Issue 10, pp. 42–68
Editors: Elizabeth M. Belding, Jörg Ott, Andrea Passarella, and Peter Reichl

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

We managed to bring together a quite balanced group of 32 people with expertise in the design and implementation of wireless ad hoc networks of various types, human-computer interaction, community informatics, urban interaction design, ethnography, media studies, arts and design.

The main take-home message from the seminar is that IoP is an emerging research topic with a lot of potential. It spans many aspects, including but not limited to the set of topics identified for the group work. Each of the group works provided concrete guidelines on the selected topics, possibly providing focused research agenda for the future.

Most of all, we are very happy that attendees greatly enjoyed the seminar, including those attending for the first time a Dagstuhl event (about one third). We do believe that the seminar laid the grounds for future fruitful collaborations, and helped a lot in shaping the key ideas of the emerging research topic of IoP.

2 Table of Contents

3 Background and motivation

The diffusion of personal (mobile) devices and pervasive communication technologies is expected to exponentially increase in the next few years (for example, Cisco foresees an eightfold increase of mobile data traffic between 2016 and 2020, with a compound annual growth rate (CAGR) of 53% [1]). This is pushing more and more the Cyber-Physical Convergence vision, discussed, among others, in [2]. According to this vision, the physical world of the users and the cyber world of Internet applications and services are more and more integrated and converging. Data generated in the physical world (e.g., by sensors embedded in personal users' devices and physical infrastructures) flows to the cyber world, where it is elaborated and exchanged. On the other hand, interactions in the cyber world result in actions in the physical world (e.g., because users modify their behaviour based on information received through Internet applications, or because physical infrastructures are configured through actuators).

One of the key effects of this convergence is that humans are more and more at the centre of the technical systems they use. Humans and the cyber systems through which they communicate become actors of a complex socio-technical ecosystem, and designing effective communication systems needs to take into consideration human behaviours as a structural paradigm, rather than as an afterthought. Moreover, in this view humans are not anymore passive objects of Internet technologies, but they play an active role in the design and even operation in the network, to the point of becoming one of the components of the complex Internet socio-technical system – crowdsourcing being a very primitive example of this new perspective. In [3], this paradigm change is named the "Anti-Copernican Revolution", as it puts (back) the human at the centre of the stage in the design and evaluation of Internet communication systems.

According to this communication ecosystem view, we see future research on Internet-based communication systems as a truly inter-disciplinary field, shaped by at least five main interacting dimensions and linking the technological perspective closely to the social, economic and cognitive sciences (describing the behaviour of humans) for designing the communication and data exchange mechanisms of future communication systems.

1. **ICT** provides the basic enabling solutions for communication to occur. However, the algorithms and protocols for communication and data exchange are not driven exclusively by the need to optimise network resource usage (as in the design of legacy Internet systems). In the converged cyber-physical environment, user devices become proxies of their users in the cyber world: They communicate, exchange and manage data by "emulating" the way their human users would do if interacting with each other in the physical world.
2. **Social sciences** model the way users establish social relationships, how they trust each other, and how they are prepared to share resources with each other. Communication systems exploiting these models ("social-aware networking protocols") have proved to be very efficient in supporting communication in human-centred mobile networks [4, 5].
3. **Cognitive psychology** describes, among others, how human beings perceive and interact with data, how they assess relevance of information, how they exchange it when interacting, and how they extract knowledge out of it. Data-centric communication systems for mobile networks have already been proposed, where these models are exploited to efficiently guide information diffusion among users [6].
4. **Micro-economics** is modelling how humans negotiate the use of infrastructure and content resources, trade and share them. This is also fundamental knowledge to predict

how they can interact with each other through communication systems, how they are prepared to share material and intellectual resources in a complex socio-technical system, and to embed such knowledge in the systems' design and operation.

5. Finally, very useful models have been derived in the area of **complex network analysis**, describing, for example, human social relationships with compact graph descriptions, amenable to characterise human behavioural properties and exploit them in the design of networking solutions.

We stress the fact that the proposed human-centric approach to the design of Internet communication systems is not yet another bio-inspired networking design wave. Because of the fact that user devices act as proxies of their users, embedding efficient models of human behaviour in the core design of communication systems is a natural way to make devices behave as their human users would do if faced with the same choices and decisions. Moreover, this approach is not confined to designing human-centred applications. The inter-disciplinary approach impacts all conventional layers of the communication stack above the enabling communication technologies, and brings advantage at all layers, as shown by the mentioned examples.

This approach can be the basis for a seamless communication ecosystem for Cyber-Physical Convergence, where communication entities can be humans, their personal devices, as well as other "machines" communicating in the cyber world. Specifically, we can foresee at least three classes of communication paradigms:

1. **The "Human proxy" paradigm.** This is based primarily on communications between devices, whereby user personal devices communicate with each other acting as proxies of their human users.
2. **The "Crowdsourcing" paradigm.** This is based both on device-to-device as well as on device-to-human and human-to-human interactions. The human user is seen as another entity of the communication ecosystem, and its behaviour can be modelled and predicted (clearly, up to a certain extent), and the resources it brings exploited to optimise the operations of the system (think, for example, of crowdsourcing systems, where humans are used to solve complex problems in a synergic way together with computers).
3. **The "User experience" paradigm [7].** This is based on interactions between users and devices, and the behaviour of the devices is designed taking into consideration the reactions of the human users to the service offered by the communication system, and the resulting quality of the users' experience.

In this view, another cornerstone for the design of Cyber-Physical Converging communication systems is Quality of Experience. Quality of Experience models interactions between humans and ICT services through a human-centric approach, by taking into consideration human expectations on the quality to be obtained, and reactions to varying level of quality. QoE models can thus be fruitfully integrated in the communication systems design, for example to anticipate the effect of devices behaviour on the human users, or to understand how users could react and behave when exposed to certain tasks to be carried out in collaboration with devices.

For further information about the concept of "Internet of People", we also refer to [8, 9].

4 Organization

The main goal in organsing the seminar was to bring together a diverse set of people with expertise relevant for the Internet of People concept. Specifically, we wanted to involve researchers with complementary backgrounds in the various areas that touch upon IoP, such as:

- Internet architectures
- Mobile networking
- Self-organising networking
- Internet standardisation
- Quality of Experience
- Community Networks and Engagement
- Internet for Development
- Internet Application and Service design
- Internet Governance

This was required, as one of the goals of the seminar was to elaborate the main IoP concept, and exploit the seminar as a seminal event to spread knowledge about this new research area. Therefore, we needed to involve relevant researchers in the various communities possibly interested in the IoP concept. In addition, geographical diversity was also sought, trying to bring to the seminar a good mix of people from Europe, US, Asia and Australia.

The initial set of invitees was shaped based on these guidelines. Also thanks to the reputation of the Dagstuhl seminars, we have been very happy to receive a significantly positive feedback from the invitees. Although some could not attend due to clashing commitments, many of the invitee were able to join. Specifically (besides Europe), we had a significant participation from the US, two researchers from Asia, and one from Australia. It is worth mentioning that we also invited the Next-Generation Unit of the European Commission to join the seminar, as we thought that IoP is very much aligned with the spirit of this new H2020 initiative. We have been very happy to receive a very positive feedback from the Unit, confirmed by the participation of its Acting Head.

All in all, 28 researchers attended the seminar. About one third were newcomers in Dagstuhl. It is worth mentioning that, in the survey after the seminar, all respondents stated that they would come back to another Dagstuhl seminar in the future.

5 The seminar

5.1 Breaking the ice: Initial session

As usual, we started the seminar with a round table introduction of all participants, who had been informed beforehand to prepare a 2-slide presentation stating who they are, what are their main research activities, and what they expected from the seminar. The initial round table was a very nice way to break ice and starting to getting to know each other better. While a good share of attendees were already known to each other, some of them were not. We anticipate that they have been productively engaged into the seminar activities, nevertheless.

After the initial roundtable, the organisers delivered a short presentation, stating their view on IoP before the beginning of the seminar, which motivated them to organise it. Specifically, the presentation started by noticing a few facts relate to the current evolution of

the Internet. The first one is the emergence of cyber-physical convergence, whereby there is a tighter and tighter correlation and interplay between what happens in the physical and in the cyber world. The second fact is the expansion of the Internet primarily at the edges, much more than in the core, due to the pervasive diffusion of mobile and IoT devices, i.e., devices with a tight link with human users. The third fact is that in this trend, users' devices become more and more proxies of their human users in the cyber world. These facts potentially have a disruptive impact on the Internet as we now it today, such that it may not be possible anymore to think at the Internet according to "business as usual" innovations, but we might be in need of radical rethinking of all the main Internet primitives. In this view, we need to rethink those primitives taking a human-centric approach, i.e., considering the human behaviour as one of the key design concepts of the new Internet. This human-centric perspective is the key concept behing IoP. Finally, the presentation also made the point that Internet research is not only on the ecosystem around the Internet, as the latter is not an immutable technology given for granted now and for all. Rather, IoP calls for radical new research also in the Internet technologies, which are the key technological underpinning of any technological and societal impact related to the Internet.

The initial presentation already stimulated very lively debate and discussions. Among the many others, Max Ott provided quite a strong feedback about the fact that we need to consider the impact of 5G technologies, which are bound to provide a lot of bandwidth and capacity at the edge. Rather, we need to look at the information side of the network, and consider IoP mostly as a information-centric network. While there was not unanimous consensus on the fact that 5G might solve all networking issues in the mid- long-term, all attendees agreed that IoP would be primarily an information-centric network, and this is a correct perspective to use to look at it. Moreover Jörg Ott proposed a more top-down approach, whereby we should (i) think to the services first, which are human-centric, and (ii) then go down and think to the network that one needs, and whether this is local or global.

All in all this initial session proved to be extremely helpful in breaking the ice, start putting onto the table many key concepts related to IoP, and start identifying possibly complementary and sometimes contradicting views.

5.2 Seed Talk 1: Good City Life

Daniele Quercia, Elizabeth M. Belding, Jörg Ott, Andrea Passarella, and Peter Reichl

We invited Daniele Quercia, from Nokia Bells Labs Cambridge, UK, for the first seek talk. Daniele presented the project "Good City Life", as follows.

The corporate smart-city rhetoric is about efficiency, predictability, and security. "You'll get to work on time; no queue when you go shopping, and you are safe because of CCTV cameras around you". Well, all these things make a city acceptable, but they don't make a city great. We are launching goodcitylife.org – a global group of like-minded people who are passionate about building technologies whose focus is not necessarily to create a smart city but to give a good life to city dwellers. The future of the city is, first and foremost, about people, and those people are increasingly networked. We will see how a creative use of network-generated data can tackle hitherto unanswered research questions. Can we rethink

existing mapping tools [happy-maps[1]]? Is it possible to capture smellscapes of entire cities and celebrate good odors [smelly-maps[2]]? And soundscapes [chatty-maps[3]]?

Daniele's presentation was very well received, and stimulated also controversial discussions. Among the many points raised, it was questioned the fact that, in general, "better" areas of the cities become more expensive, and therefore making a city "nicer" might lead to excluding vast portions of the population from it. However, there is a middle point to be met between the right to live in a nice environment, and the price of it. More related to Internet design concepts, and to IoP topics, the Good City Life concepts can provide very useful input to design human-centric IoP services and applications, possibly at a global scale. It would be possible to design services to foster interaction between people through urban elements, ultimately exploiting IoP to make services that make people happier.

5.3 Seed Talk 2: IoP – People Centric Designs

Paul Houghton, Elizabeth M. Belding, Jörg Ott, Andrea Passarella, and Peter Reichl

The second seed talk was given by Paul Houghton, from Futurice, Finland. Paul conveyed his experience on human centric services and application designs. Paul took the angle of human-centric IoT (which is a part of IoP), advocating the need to start from a user-centric perspective. He made the case of lego-type IoT (inside IoP), whereby IoT components can be miniaturised and form-factored into lego bricks, that one could mount and compose appropriately. This would also put into the picture gaming-inspired IoT designs. The ultimate goal, would be support extremely cheap IoT systems that any user can build on their own, out of very basic technologies affordable to anyone. An example of a prototype developed along this line is the 3D parametric LEGO-compatible model in OpenSCAD[4], to generate arbitrary size blocks such as electroncs enclosures and mounting panels. First print the calibration blocks, then use those turning parameters to fabricate with a perfect fit using different plastics.

Moreover, Paul also covered an industrial-oriented perspective, envisioning a sort of IoP design kit. He made the point that people want new techonlogies, but most of the time they don't know how to use them. Therefore, we need designing for IoP workshops, i.e., interactive, collaborative tools. The details of such a kit implicitly sets the boundaries and mindset, for better and for worse. The IoT Service Kit is a prototype along these lines presented by Paul during the talk. It is a board game that brings domain experts out of their silos to co-create user-centric IoT experiences and achieve mutual understanding. Clashes and miscommunication between differing perspectives and disciplines can disrupt the workflow. The playful nature of the Kit brings down walls and naturally incites communication. On the other hand, Paul also highlighted that industry adoption needs simple, usable concepts they can map to ideas they already know.

[1] http://www.ted.com/talks/daniele_quercia_happy_maps
[2] http://goodcitylife.org/smellymaps/index.html
[3] http://goodcitylife.org/chattymaps/index.html
[4] https://github.com/paulirotta/parametric_lego

5.4 Panel: IoP around the world

Peter Fatelnig, Pan Hui, Max Ott, Ellen Zegura

After the seed talks, we organised a panel, initially conceived to provide views about IoP-related efforts around the world. For this reasons, we invited in the panel one representative from each continent involved in the attendance. This perspective was taken in the initial presentation from Ellen, who reminded some lessons learned in disruptive Internet designs funded in the US through, e.g., the NSF FIND programme. Moreover, Peter presented the main points of the coming Next Generation Internet H2020 calls, and how they are framed in the more general Internet of People concepts.

Then, the discussion then drifted towards arguments that were already been touched upon during the previous presentations, and expanded the discussion on these points quite a bit. One point that was discussed was the problem of large monopolies, and the typical tendency to for "winner takes it all" phenomena, which happened for Internet in the 70s/80s and now is happening for Facebook. Another important aspect that has been discussed was related to privacy and trust, as a possible perspective to migrate towards a more decentralised, IoP-like paradigm. However, some evidences contradict the typical importance given to these aspects, such as the fact that people uses services like Facebook even if they don't trust them. Again, the information-centric perspective was brought to the table, as one possible incarnation of IoP. An information-centric IoP would be more decentralised than the Internet, in the sense that everyone would "owns" part of the data that make up the network. Therefore, decentralisation would be key for data-centric services, for doing data computation in a privacy-preserving way.

5.5 Group work: IoP definition

Andrea Passarella

After the panel, we split into three separate groups. Before the meeting, we identified some possible topics for discussion, which have been refined before splitting into the groups. The three groups turned out to be homogeneously subscribed, so there was no need to reshuffling or reorganising them. The outcome of all groups were reported at the beginning of the second day of the seminar.

The first group worked on the IoP definition, and came out with a set of features for IoP. The first feature is that IoP would be a network of active Digital Twins. Specifically, there would be one entity per person, representing their identity, also defining the person's profile. Such a digital twin would ideally collect all information about the respective person, which is currently scattered and sometimes inconsistenly stored across current Internet services. The digital twin would control access to personal data by external services, thus acting on behalf of "its person", even when s/he is not active in the Internet.

The second IoP feature is that IoP would be a network where the "IP node" is a person. Thus, personal devices would only be incarnations of the person at a lower layer. Devices would communicate seamlessly, exploiting the most appropriate communication means at

any given point in time, including global vs local communication, as appropriate. It was found that this could embody even legal frameworks at the "personal IP" layer.

The third IoP feature discussed was that IoP would be a network including human-centric primitives, primarily at the edge. In such a network, personal devices would work with each other based on their users' behaviour, data sharing/management/access being the main focus, according to an information-centric perspective. These novel primitives would be unleashed by more "programmer-friendly" standardised support for local communication. Finally, it was discussed that IoP primitives would complement (and not replace) conventional Internet primitives.

A fourth key feature was considered to be that IoP would be a network bringing value to people, not to Things (or to Big Things). In this sense, there is a huge difference between IoP and IoT, as (i) IoP would be using IoT as a means for people-centric interaction, and (ii) M2M communication per se would be of little value, if not in the context of people interactions. Another key aspect is the relation between IoP and "Big Things", i.e., the fact that data about people behaviour is most of the time of benefit only to the big players in the IoT domain. IoP could provide technical (and non-technical) mechanisms to bring (more?) control by people over their data.

IoP was also seen as an open network for human-centric innovation, thus going back to the roots along which Internet was conceived. IoP is seen as an open ecosystem hosting innovative, unforeseen services, vs. the perception of the Internet as a centralised monopoly in the hands of a few (i.e., Internet = Google + Facebook).

Last, but not least, IoP is seen sas an "organically growing", people-centric Internet, exploiting the analogy of global vs local farming productions (e.g., Monsanto vs organic farming). Along similar lines, IoP would address different needs, between one-size-fits-all managed network and a network that organically grows from personal devices, aggregating and controlling them according to the purpose for their users. This clearly calls for novel ways of decentralised management, governance and control.

5.6 Group work: IoP use cases

Ellen Zegura

The group began with an example provided by Max about a company selling hearing aids that wants to be able to collect data from the devices to improve the product, however the data is considered medical data and cannot cross national boundaries. This is an instance of private data that in aggregate might benefit users of this product (and the company). It is an instance of a clash between Internet boundaries and national policy boundaries. We discussed a re-design where the computations move to the data rather than the data moving to the computation. Will this solve the problem? What if all the data needs to be together? We discussed providing users with greater control over allowing access to their data. We discussed the education challenge that users don't understand their data, and service providers (e.g., Apple) become data gatekeepers.

We discussed the limitations of the Internet in crisis situations, such as those produced by natural and human-caused disasters. We discussed the challenge of enabling collective groups of people to accomplish something immediately and locally, such as citizen volunteers

for search and rescue. Current practice is to cobble together digital and non-digital tools in ad hoc and organic ways. We briefly discussed the idea of a human sensor system that would be created and sustained over a long period of time and that could be queried to take the pulse of a community or to track reactions or attitudes over time or to provide large-scale crowd sourced information (e.g., is help needed where you are).

We spent a long time talking about whether and how Facebook is an Internet of People. We discussed why people like Facebook and what they use it for beyond the obvious of staying connected while apart. Examples of uses included humor, cleverness, a pool to tap for commiseration (e.g., Elizabeth's travel woes!), a trusted subgroup to get advice from (e.g., Dagstuhl travel advice), a window into the views of people you don't normally interact with (e.g., political differences in friends of friends). We discussed the risks and value of on-line forums that allow one to shape the presentation of self (see Goffman book), with possible relevance to the digital twin idea. A risk of on-line representation is that social norms will not always carry over. We discussed whether the fact that Facebook is a company making money and gathering data means it cannot be an Internet of People. We forsee a potential tipping point for Facebook as they face pressure to filter certain content, to be more transparent with ads (e.g., Russia buying ads influencing US election).

We talked about the value of fairly immediate feedback from a local crowd, e.g., to learn how to improve a presentation, but also how that feedback is very personal and should not go to the cloud. This capability – private but rapid insight into what people are thinking for personal use– was mentioned as valuable, even vital, for self-development, evolution, and learning. We talked about a tool for gathering feedback from people based on micro-narratives and self-signification, forming a type of self-ethnography. Maybe this is useful for getting anonymous but useful feedback? Tools like this can be used to measure and track culture change.

Our last IoP use case (or perhaps it was an example of an IoP) was community networks. Leonardo shared the scope, history and uses of a number of community networks in Europe and elsewhere. Community networks arise for multiple reasons – in some cases there is nothing else, in others there is a desire to operate without ISP constraints, some favor the philosophical reasons connected to freedom. Many (most?) community networks rely on a sufficient number of tech geeks who have the experience and inclination to manage the nodes. That makes it challenging in communities that lack this expertise. Sometimes community networks serve to create and demonstrate demand that then attracts a commercial ISP to the area and results in the end of the community network. Community-based networks can generate social and cultural capital.

5.7 Group work: IoP and People

Kirsi Louhelainen

The third group discussed about the interplay between IoP and people. What follows is a set of bullet points highlighting the key aspects of the discussion. The discussion was organised around three main themes, (i) a roundtable on establishing an initial perspective on IoP; (ii) reflection on some basic issues, and (iii) discussion aspects.

1. Roundtable: establishing an initial perspective on IoP The key aspects discussed are as follows:
   - IoP as long-term counterperspective to IoT. Internet is for communication between humans, not between things. Sort of philosophical perspective.
   - Internet built by people for people/community networking/democratizing control
   - Embedding social aspects into technology and vice versa.
   - Improve collaboration: enhancing how people work + enable them to form social groups. AI usage for enhancing collaboration.
   - Content is cheap, but you need reputation and trust (not easily duplicated, costly). Tactile Internet (low latency Internet, touch will be transmitted to other person).
   - Milgram-Experiment -> social networks? Networks set up by people, plus trust. Internet of social networks. Services for people. Alexa is not in IoP. Social networking/connections between people.
   - Low latency/AR could be a use case. 2 types of data: information (public interest) vs private information (you want control). IoP pushes both of this to the extreme: 2 silos (public information with low entrance threshold), tied to private information. Allows new digital market place: opening up and generating energy for new service creation. More value in giving up certain control options and instead increase user numbers.
2. Basic issues
   - How do people use the Internet?
   - Social aspects of the Internet
   - People setting up the Internet themselves – (what does setting up mean?)
   - Individuals vs groups vs communities
3. Discussion aspects
   - Is it a local or a global thing? What is the smallest constraint space for sharing public and private information? Storing data, anonymization, history of data.
   - Digital memory: we should not save everything for all time. Audit logs + need to store some information (how many people use service) plus personalized log
   - Mechanisms that allow people to control what happenswith them.
   - Personalization
   - Handling multiple people w.r.t. their needs through some sort of bartering (with automatic convergence)
   - Making users an equally important staktholder as the other stakeholders (“workers’ union” type)
   - Charter of Internet rights (e.g. privacy....). Might include the right not to use the Internet!. See IoT manifesto (https://www.iotmanifesto.com/)
   - Fundamental categories: Base rules – physical properties – Internet rights
   - Example: AI checking whether persons are real? One possible IoP principle: NO BOTS. Alternative: autonomous agents who behave like humans = proxies (and share one ecosystem)
   - Tagging suspicious data / means for transparency
   - Is IoP more about traditional Internet sites or about new sites?
   - FAT – fairness/accountability/transparency: use case specific? Limited to contexts?

5.8 The second day

The second day started with a presentation of the three group works of the first day. This was again an opportunity for ample discussion and reasoning about the IoP concepts and topics, with significant participation from all attendees. Afterwards, we organised the day allocating "snippet" presentations by attendees, and a final session with additional group work. As for the previous day, the topics were roughly identified before the seminar, and have then be refined before splitting up. Also in this case, the composition of the groups followed quite naturally attendees interests, and no significant reshuffling was needed. It is worth noticing that the groups composition was quite different from that of day one.

In the following we provide abstracts of the snippet talks, and summary reports from the group work.

5.9 Snippet talk: Finally Closing Up: QoE in IoP

Markus Fiedler and Tobias Hossfeld

So far, Quality of Experience (QoE; "the degree of delight or annoyance") is perceived by users far above the very Internet core layers, aka TCP/IP. The differences in foci have led to a range of unsuccessful QoE modelling and management approaches, and there is still a clear divergence of viewpoints and agendas for QoE and Internet researchers and practitioners, respectively. However, given that the Internet of People (IoP) resides at the top of the communication stack, it comes naturally close to where QoE resides. Thus, there is hope that QoE will be much closer related to IoP principles, provisioning, services, and management, than it has been the case for Internet so far. Thus, any provisioning and control will be much more efficient, creating delight for and reducing annoyance of users, in the best sense of QoE. So we may hope for better user-friendliness (with its many facets) of IoP compared to classic Internet, i.e. for "power to the users" / "power to the people".

In particular, we discuss what is missing in the QoE world like taking into account social interactions between people or the consideration of data and IoT services. For such services, the Quality of Information (e.g. accuracy, timelineness) may be more relevant and contribute to the overall QoE. A major aspect in IoP is privacy which is often mentioned as QoE context factor, but not explicitly addressed in QoE models. Those aspects need to be taken into account in an IoP-aware design in addition to a QoE-aware design. While the primary goal of QoE may be the make the people happy, the question arises at which costs. Machine learning approaches may need to know a lot of private information e.g. user's context, location, preferences to optimize QoE. In IoP, people should be made aware of privacy in an easy way. Internet services and apps should empower the user, i.e., allow the user to decide. This may include the degree of neutrality of recommendation mechanisms or which kind of data to be collected. In summary, IoP requires to allow the implementation of "ethics".

5.10 Snippet talk: IoP for the 99%

Nicki Dell

My goal would be to broaden the conversation to the ~80% of the world's population that lives in the so-called "developing regions". Most of the biggest technological advances have primarily benefitted people who live in western societies. It is crucial that we expand this view. Doing so requires us to think about how to (re)design the Internet and computing experiences to account for cultural, social, linguistic, and socio-economic diversity. People have vastly different value systems and desires. We need designs that support this diversity – combining new technical innovations with human and social aspects of design. A multi-disciplinary approach is essential! HCI, design, networking, law, security, privacy and more. We also need to push beyond the prevalent model of designing for individuals and consider how to design for different groups – families, villages, communities, cities, and so on. How do the design principles change when we expand our view? How do the technical primitives change? How can we come together to design better systems that accommodate people's values, meet their needs, and simultaneously make the world a better place.

5.11 Snippet talk: IoP and Community Networks

Leonardo Maccari

Community networks (CNs) are large-scale wireless mesh networks made of tens, hundreds, or even thousands of nodes that are blooming in many world regions. CNs are organized through a bottom-up, decentralized and participatory process by communities of people, thus they challenge the current for-profit, market-based Internet access model of commercial Internet Service Providers. Today, we know that at a certain scale CNs help to overcome the digital divide where the market fails, however, the degree of innovation of a CN is not only embodied in the number of bits per second it can carry. It resides in the kind of P2P applications that it can enable and that can challenge the current centralized computing model. It resides also in how many people from the currently marginalized groups can get access via the CN. Finally it resides in the extent to which the network can be governed as commons, and not only as a for-profit initiative. Commons-based governance makes it possible to have transparency, participation and to democratize the key decisions on the way networks work.

A CN is an archetypal example of the Internet of People, in which literally every network node is one person. The netCommons project deals with CNs and researches on the way they can scale, be sustainable, offer applications, and interact with society at a broader level.

5.12 Snippet talk: The organic Internet or The Internet of (the) People

Panayotis Antoniadis

The popular Internet platforms that mediate today our everyday communications become more and more efficient in managing vast amounts of information, rendering their users more and more addicted and dependent on them. Alternative, more organic, options like community networks, http://netcommons.eu, and DIY networking, see http://mazizone.eu/, do exist and they can empower citizens to build their own local networks from the bottom-up.

If we wish to facilitate the creation of an "Internet of People" where People are not just extensions of Things, we need to design for diversity, participation, local ownership and governance, and in this sense David Clark's "design for tussle" needs to be redefined in light of the eventual concentration of power over the Internet infrastructure and services, in the hands of very few global corporations. Some of these ideas are included in an upcoming book chapter (submitted draft attached) which will appear in November 2017: http://www.palgrave.com/de/book/9783319665917

5.13 Snippet talk: IoP and Agile wireless network architectures and protocols

Mariya Zheleva

Internet access in rural areas, displaced persons scenarios and cases of political oppression are just a few examples that have demonstrated at scale that the Internet today is far from open, inclusive and equal to all. Emerging agile wireless networks and protocols have the potential to resolve some of these growing limitations and establish the IoP, as defined during this Dagstuhl seminar. Such architectures and protocols will bring innovation both at the network and the client side and will enable local entrepreneurship to foster organic growth and cultivate the diversity of the future Internet.

5.14 Group work: IoP architecture

Andrea Passarella

The group tried to "think architecturally", i.e., to identify key architectural concepts for IoP. The outcome was a set of concepts, summarised as follows.

Firstly, the group discussed about what is an IoP "end-point", particularly, if the IoP node would be a (group of) person(s), or its digital twin. We agreed that we need identity-based routing, which in turns, calls for trust management. But, most likely, we found that data-centric routing should be natively supported as well. A second concept is the fact that

we need flexible scoping in routing/data access. Specifically, we don't necessarily need that every-thing, every-one, every-data is accessible globally. So, mechanisms to dynamically define the "visibility" scope of IoP entities are required (moving from local to global visibility). Moreover, there is a need for large-scale measurement studies about locality of data access. We then discussed what should be inside IoP headers. One possibility would be to have "manage-me-like-that" embedded information (e.g., for geo-fencing packets). This might also be a way to support "human-value-centric" forwarding. We also discussed whether this would be essentially similar to active networking.

A significant part of the discussion was related to whether we need a "narrow-waist", and what this would be, in the case. The group agreed that a natural narrow-waist would be the social graph(s) of the IoP users. In this case, the abstractions of nodes would be Persons, Communities, "Legal entities" behind "things". This would be probably a multi-dimensional (or a hyper-) graph, to accommodate for the different roles each person takes at different points in time. But then, how do we account for trust? In a completely centralised manner? But then, we would need a globally trusted entity, which might be quite questionable. Or, should trust be a completely distributed and subjective way, i.e., one of the properties of a link on the social graph? Another related concept is how do we cope with dynamism, such as, e.g., stable social relationships vs "ephemeral" social relations. In this context, we should take into account that the social graph would subjective, and each node would have its own view of it. Scalability issues were also discussed, i.e., whether we should consider one gigantic flat graph vs a hierarchical graph, at the hierarchical levels of persons; communities; groups of communities, ... Finally, we discussed what would be the relationship with the current Internet stack. Most likely, we would use the current stack when appropriate (e.g., for global communication). But the, an issue is how to integrate IoP with "conventional" traffic engineering approaches (e.g., fairness). We should also be open to use other "transports" when more appropriate, e.g., in case of local communications.

5.15 Group work: Privacy vs. Sharing and Knowledge Creation

Panayotis Antoniadis, Nicola Dell, Thorsten Strufe

"Sharing is caring, privacy is theft, secrets are lies" – Dave Eggers (The Circle)

The Internet of People is based on individuals communicating with each other – one-on-one, in small groups, or large forums. These communications may create "leave-behind" artefacts, such as posts, photos, or videos, to facilitate the ongoing conversations, or may be shared wth a wider group (e.g. public blog post), In short, in the Internet of People, information is primarily created, curated, and consumed by the People and for the People. The creation, and especialy curation and aggregation aspects may be supported by services (e.g agents, bots, ...) and in turn leverage social relationships and cross group boundaries with great opportunities towards the commons, benefitting everybody. [...for routing and providing its services, and the aggregation and processing of the collective behavior and data may offer great opportunities towards the commons, benefitting everybody....] This also implies that individuals may be observed and tracked, their data accessed by potentially unintended audiences, with potentially adverse or even dangerous consequences for the IoP participants.

For the purpose of systematizing this spectrum it makes sense to understand notions of privacy, threats, potential benefits, and the factors that may lead to an outcome in which the benefits and drawbacks for all stakeholders can be balanced.

Privacy as an abstract concept essentially has a very different meaning in different cultures. This has been discussed at great length in the context of the difference between the Anglo-Saxon and the European notion of privacy: The former being shaped by the right to be let alone (or: freedom of processing, the regulation of markets, and an intrinsical opt-out notion; trust in companies and distrust in governments), whereas the latter traditionally follows the notion of data sovereignty and informational self-determination (or: intrinsically opt-in and control over the data throughout its lifetime; distrust in both governments and companies). This discussion, while quite prominent, has ignored the profound differences compared to other cultures. Many Asian and African countries, for example, don't only exhibit entirely different utilization of electronic devices and services, but are also characterized by different privacy expectations. The discussion also ignores the discrepancy between the legal, idealistic, and real situation: The European perspective fails to address the aggregation and continued processing of aggregates (which part can you take back? What does the difference between the aggregates before and after disclose about the data that one wants to take back?), and all current notions ignore that personal data often shares dependencies between individuals (Statistics can disclose seemingly hidden attributes that individuals do not want to share. The data of groups may disclose private attributes of its individuals, with the extreme of statistically similar DNA sequences between relatives , where some may want to publish, and others hide parts of this shared information).

Sovereignty and responsible action imply that the individuals and stakeholders actually comprehend the value of data. This raises additional challenges. It may not even be possible for an individual to assess the value of the data it is willing to share or expose in terms of recorded behavior, as the current, advertisement-driven market values the various data of individuals differently: being able to identify and analyse hyper-consumers and influencers of course is much more valuable, than collecting yet more data about the average Jane (both in terms of numbers of average vs peculiar individuals, as well as in terms of expected spending capacity and influence). However, this role in the overall audience is difficult or impossible to judge for the individual itself. It additionally is difficult, may be impossible, to gauge how the exposed data can be mined, what happens with the aggregates, and most probably unfeasible to even guess how these data sets can be linked, correlated and mined in the future [5]. Another observation is that many stakeholders (primarily companies) currently collect and store data about individuals without analysing them, nor having a clear plan or even ideas about how to process them and for which purpose in future. It's just simple to collect and to store just in case. A third observation in this context is that the market valuation and income of companies actually is only indirectly related to the data they collect, but directly related to the type and extent of audiences, whose attention they can sell. The targeting of specific groups requires knowledge about the individuals, but the business model is primarily based on selling attention, selling actual data or aggregates (at least as observed by the public) seems to be a secondary income, if it represents a notable income at all. Changing perspectives could hence be a sensible approach: Privacy should probably not so much be viewed as the value an individual allocates to its data, in the decision of sharing – but rather as the potential risk to the welfare and well-being if "lost" to the public domain, or commercial and institutional parties.

[5] This observation also challenges the initiative of the GDPR to oblige all data collectors and processors to comprehensively explain results and ramifications from data processing

An important factor in this picture is the question of trust: The privacy of different personal attributes of course depends on the audiences that get access to them. Considering an IoP, it may be perfectly acceptable for individuals to share sensitive information, like for instance their location, to their significant other, their family or friends, their colleagues, or neighbours. This could also have a geographic aspect: while it may be undesirable to share this information globally or with a remote, commercial provider, it may be perfectly fine to share the location with people in the direct vicinity, probably even with small local businesses. It is also well conceivable that this trust is based on interest or other properties, and platform collectivism, in which all participants in a system share their respective data with everybody else on the platform, is well conceivable in the IoP.

This raises the question of the architecture and stakeholders of services on the IoP. Considering social media like services, the current architectures comprise of the three immediate stakeholders of users, providers, and (advertising) customers, as well as society as a the general context. The current discussion of privacy has a strong focus on the users, who are expected to understand how their actions and their data could be collected, used, and their exploitation have a potential adverse effect. The common narrative hence claims the responsibility to be with the users, who should know what to share to whom, not to overshare, to use the audience selection mechanisms appropriately, etc. The responsibility of the providers is commonly conveniently avoided, despite the fact that only the providers could even remotely assess the value, make informed decisions about which data is rather common or sensitive, and could potentially provide effective protection of the data. The providers so far, however, have no incentive to protect, avoid, or even minimize data, and hence push towards even more sharing with even larger audiences, going as far as claiming that the post-privacy culture was the future.

This imbalance of responsibility is even more pronounced by the lack of credible information on the current uses of one's data (at least theoretically private data can be used not only for "innocent" advertisement but also for manipulation of behaviour, addition tactics, and more), but most importantly on the future potential uses, ad in the case of a change of political situation (e.g., a dictatorship).

Considering the incentives between the stakeholders it becomes obvious that they are currently not aligned, and that it may make sense to reflect on the prime driving instincts of fear and greed. The optimistic view here would suggest to create markets in which it is beneficial to sell services and devices that allow for privacy-preserving utilization and deployments of the IoP. Businesses could offer such devices that guarantee good services under protection of the sensitive, personal information of the users, and the invisible hand of the market could take care of the remaining, insecure service providers. A more pessimistic view would suggest to focus on the responsibility of the providers, and align their incentives with that of their users. An approach could be regulation and severe penalties for data loss incidents. The GDPR includes first steps in this direction, threatening the providers with fines of up to 4% of their annual turnover in case of the loss or maltreatment of personally identifiable data. This observably has caused several companies to rethink their current practice of collecting everything, just for the potential case of future opportunities (or neglect). A first step in this direction could be the requirement for companies to put the data collections they hold on their annual balance sheet. Depending on the approach this could be seen as either an asset, or a risk. In any case, this would raise the level of attention to the board of directors, and hence become a point for consideration for the CFO's and CEO's.

Sharing data may of course generate knowledge, which represents a value, potentially public, in itself. Keeping everything private may hence in fact affect not only the IoP, but even the data owner adversly. It is quite likely that the participants in an IoP will prefer to enjoy the advantages from functions over everybody's data, which is only possible if a noteworthy fraction of the participants actually do share some information. But it is also likely that if they had the power, they would enjoy to benefit also the additional value that their shared information generate (beyond knowledge, also in economic profit). Despite the fact that it is difficult to judge the sensitivity of data, a solution could be to distinguish between public and private data (or: aggregates), share the data that is less sensitive to the public domain, and allow for the local processing of the complete data under the control of each individual, consolidating the public and their own private data.

Taking the role of an engineer, it becomes apparent that the common tools will play a role in the Internet of People: It will need functionality to generate awareness in the users, and it shall provide transparency of the algorithmic results, and as a basic foundation of its design. An extension is accountability – the repudiation of acts, especially of institutional or commercial parties should be avoided. This, however, is a double-edged sword, as means for accountability can directly play into the hands of populistic or even totalitarian regimes, that may require accountability of even innocuous acts of individuals, thus preventing anonymity. A direction offering solutions to this conflict could be tools for obligations management, encapsulating both data and obligations for the recipients, thus explicitly allowing or prohibiting propagation, aggregation, or analysis. Experience with digital rights management in the past, however, has depicted the natural limitations of this approach.

A direct solution with natural fit to the Internet of People paradigm could be a personal device for secure data storage and processing, the "Decentralized Privacy Box". Sold to or built by the participating individuals, it could offer guaranteed secure computation (for example through the integration of Trusted Execution Environments, like the Software Guard Extensions of Intel, SEV of AMD, or similar extensions; or through implementations of secure multiparty computation or simplified algorithms on homomorphically encrypted data). A typical scenario could be the retrieval of public data and local processing of recommendations or added value services with access to the local, personal data. It would also allow for functionality in which two individuals share their private information with eachother, facilitating functionality leveraging both data sets, but preventing access to the private data of the opposite party. Joining various datasets, and potentially removing the sensitive personal parts, the data aggregates could be shared back to the community, the platform, or even the public domain. Micro-payments could further incentivize the participation in services on public data, with subsequent improvement of the public data after augmentation with the local, personal information.

Another, complementary, research direction to pursue in this context concerns the tools (technical but also legal, social, and political) for the "People" of the IoP to be able to create organizations of different scale (at a neighbourhood, city, or even national level), that will enable to participate in some of the aforementioned decisions and take ownership and control of their data and the value generated by it. Platform cooperativism is a recent term that resonates with such ideas, but the design space is very broad and perhaps the best strategy is to provide options, to redefine David Clark's concept of "design for tussle" in the case of IoP.

In summary, the Internet of People paradigm seems to direct towards decentralization of services, giving higher responsibility and probably less access to large entities and creating a more level playing field between all stakeholders than we see today. Sharing towards trusted audiences, providing de-identified aggregates and augmentations of public data shall further

knowledge and provide benefit to all. Acknowledging the privacy implications, this has to be done with care – and a decentralized approach, with privacy boxes implementing proven secure functionality as end-user devices seems a promising vision.

5.16 Group work: From Internet to IoP

Markus Fiedler

The discussion focused on the concept of the "Digital Twin" (DT) as a representative of the user in terms of communication-related needs and preferences, and is summarised through the following set of crystallisation points.

- **Feature list:** The DT is a repository of user-owned data and user-related settings. This mandates support of configurable levels of privacy, dependent on the context of the current usage. Likewise, the DT should take care of the user's communication, choosing the best-suited connectivity (in terms of quality, security and economy) for the user. Thus, the DT needs personalisation and configuration facilities. Furthermore, it DT needs to be reachable and thus be addressable and routable from outside.
- **Architecture:** The DT represents a peer in an overlay concept, with corresponding personalised peer-to-peer communication. Given the plethora of desired features in combination with a step-by-step development path, a modular design appears to be mandatory. More discussions on the architecture can be found in Section **??**.
- **Groups:** The DT should support groups, which entails the needs for dynamic configurations and feature interactions.
- **Governance:** Through its personalisation and configuration features, in particular with regards to granting (and revoking) access to personal information, the DT implements the principle "power to the people".
- **Enemies:** Certain social networks have been identified as having conflicting views and implementations of information ownership and (missing) user control.
- **Business models:** In order to power a system of DTs, the DT peers need to contribute to its operations, *e.g.* through using some micro-currency, as alternative to the contemporary "data milking" by large players on the ICT market.
- **Regulatory issues:** If correctly implemented, the DT concept allows for data minimisation. Furthermore, it is expected that regulatory bodies get more possibilities to act against non-compliant stakeholders (*i.e.* a "bigger stick").
- **Implementation:** In order to allow for a successful growth, parallels to the Internet development can be drawn, with bottom-up (instead of top-down) principles; trial-and-error approaches; and workable instantiations.

The presentation to the plenary had the subtitle "...and what coffee's got to do with it". Indeed, parts of the discussion were inspired by the personas of a South American coffee farmer, who should benefit from the IoP without ending up in any communication, configuration or privacy hassle.

So far, no tangible transition plan could be envisioned; the group foresees the emergence of the DT to happen in an Internet-typical bottom-up fashion. Still, the urgent issues at hand are not technical, but related to the stakeholders' attitudes, in particular regarding to ownership and privacy of user-related data. A transition away from the information ownership models of large social networks to "people in control of their privacy" is badly needed in order to pave the way towards a successful IoP.

5.17 The third day

The third day was devoted to two main aspects, i.e., discussing the outcome of the previous day group work, and identifying next steps. To accomplish the second task, we again split in three groups, one focusing on the IoP toolkits, one on IoP research agenda dn roadmap, and the third one drafting an IoP manifesto.

In the following we provide summaries of the outcome of the three groups.

5.18 Group work: IoP toolkits

Panayotis Antoniadis

Toolkits can play a key role in empowering people over the control and design of "their" Internet. The reason is that technology is not neutral and an "Internet of People" should allow for the customization of local infrastructure and services according to the needs and values of smaller or bigger groups of people that wish to democratically co-create the technologies that affect their lives.

In this context, both the design and implementation processes require significant expertise and for this only with powerful and flexible toolkits one can ensure that the Internet of People is owned, designed, and controlled, actually by the people.

Additional toolkits and guidelines are also needed other enabling and facilitating actors like researchers, community organizers and more.

In this working group we focused on two main type of toolkits needed for the Internet of People, on participatory design and DIY implementation.

First, for the participatory design toolkit of the technology itself, the IoP:

- Example: Paul's IoT toolkit, physical objects, toys, cards, maps
- geographic vs. abstractions
- boundary objects (MAZI's transdisciplinary methodology)
- 3 predefined examples

What is different in the case of IoP compared to those many existing toolkits? Mostly the concrete target technology unique, which is beyond software services but include the network infrastructure itself and most importantly the corresponding governance procedures, legal aspects, and more.

One can build on lessons learned from the participatory design literature like focusing on stories and asking people about their place in the world before going into more details.

Of course, the cost of decision making shound not be neglected and for this the IoP participatory design toolkit should include the visualization of trade-offs regarding different design variables and also comprehensive "translations" between design choices and outcome in terms of key values like privacy, anonymity, degree of individual choice, etc.

Second, the DIY implementation toolkit was quickly summarized with the "IoP in a box" concept. In this context there is related work in the context of Community Networks (CNs) and DIY networking with the toolkits by Commotion, https://commotionwireless.net/docs/cck/, and MAZI, http://mazizone.eu/toolkit/ being the most advanced today. A key requirement for such a toolkit to be effective is to include primitives that already work and at the same provide rich options for customization, configurable elements.

5.19 Group work: Agenda and Future Research Topics

Gareth Tyson

This section covers discussions from the Agenda and Future Research Directions break-out group. It lists key opportunities and research challenges. It is structured in a roughly chronological order, however, many of the tasks are closely interconnected.

Requirements, philosophy and implications of IoP. Before re-architecting any technology, it is first necessary to understand the socio-techno and even philosophical underpinnings. Hence, the first step must be to lay out a series of goals, considerations and implications. This should be embedded within a manifesto that delineates the key goals of IoP, its requirements, its intended outcomes and any desiderata. Embedded within this should be a robust state-of-the-art review to understand past pitfalls and future opportunities within this broad landscape. As part of this, we envisage that transparency will be a key aspect of the IoP, such that people can reason over the wider ecosystem (from design to deployment, and beyond). Building transparency tools (e.g. measurements, visualisations) will therefore be a major part of the manifesto.

Architecturing the Digital twin. A common discussion point within the groups was the concept of a Digital Twin (or cyber-me). This constitutes an always-on digital presence that (1) Stores and mediates access to all online data related to an individual; and (2) Acts on behalf of the individual regarding certain authorised activities, e.g. negotiating exchange of data. Consequently, a major step would be: defining the data structures that would be maintained within a Digital Twin; the ways that such data could be accessed and exchanged; the forms of agency such a Twin could have; the manner in which the Twin would be hosted and managed from a infrastructural/systems perspective; and the ways that the individual and their Twin would interact. This would further raise a number of critical legal, ethical and sociological questions regarding the extent to which the individual would be responsible for actions performed by the Twin.

Micro-level Innovations. If we assume that the Digital Twin will constitute a key primite within the IoP, it will next be necessary to exploit it to fulfil the goals specified within the IoP Manifesto. We do not intend to deviate from the current OSI-layered Internet model. However, we envisage that the Digital Twin, and its related wider social information, will feed into this modelled architecture such that layered decision making is informed by the person-centric insights captured within the Digital Twin (and any other related data structures and agency algorithms). For example, socially-informed congestion control may be introduced at the Transport Layer. These types of per-second transactional innovations are considered micro aspects.

Macro-level Innovations. If we consider micro aspects as per-second transactional activities, macro-level innovations pertain to longer-term strategic factors. Currently, the Internet is a composite of many stakeholders – dominated by a small number of hypergiants, e.g. Google, Facebook, AT&T, Cogent etc. The IoP will promote people to the equivalent power position held by these hypergiants. In othe words, the IoP will allow people to negotiate and drive forward strategy decision making with equal force to any existing hypergiant – it will democratise Internet governance. This would involve people (and their Digital Twin) unionising to exert influence on other stakeholders. On a computational-level,

this would require the specification of formal interfaces between stakeholders, allowing the exchange of negotiation-like dialogue. This would, of course, be complementary to offline interactions, whilst allowing real-time decision making to take place. Empowering users via this unionisation is critical to enabling change, and for incentivising existing hypergiants to move towards the principles laid out in the IoP Manifesto. This is particularly relevant in the face of the growing number of "gig economy" platforms, which tend to disempower individuals in favour of global operators.

Transitional Considerations: From IP to IoP. Assuming the above technical innovations are successfully designed and implemented, it would next be necessary to enable deployment. As many past efforts (e.g. IPv6, multicast, QoS) have shown, this is not always trivial. It would therefore be vital that transitional considerations are made both during the design and the deployment of IoP. This would not only raise technical challenges, but also issues of governance, business, regulation and legal factors. This would extent beyond the impact on existing network and service operators to include the needs of existing Internet users, who may not necessary wish to engage in the IoP. To be truly people-centric, such users must be considered and given the freedom to leave (whilst maintaining the benefits of the current Internet). Fundamentally, it must be possible for both IP and the IoP to co-exist -only through this will be successful evolution and transition be attained.

Use cases & Killer Application. A frequent criticism of Future Internet architectures is their lack of a "killer application" to motivate uptake. Thus, the identification of such killer applications should be integrated into the design process from the start. These use case applications would then form the basis for evaluation. Critically, it must be shown that the IoP enabled fundamentally new capabilities that go significantly beyond that offered by IP. Key Performance Indicators might include fairness, privacy, energy efficiency, and traditional measures of Quality of Experience (e.g. MOS). Applications that have been discussed include using the Digital Twin to perform offline negotiation on the individual's behalf; using social information to fulfil the needs of users, e.g. recommendations, pre-fetching of content; using the Digital Twin to mediate and protect user data. Importantly, the IoP should also underpin an innovative and open ecosystem, where any entrants can contribute and expand on these initial ideas. The IoP should therefore encourage bottom-up innovation, liberating individuals from the barriers of entering new digital markets – such principles would be laid out in the manifesto.

5.20 Group work: IoP manifesto

Anders Lindgren

The best illustration of the outcome is the manifesto itself, as in Figure 1.

6 Conclusions

The seminar was a very good opportunity to bring together a community of researchers interested in the topic of Internet of People, to discuss about this research area during an intense two-and-a-half-day seminar. People arrived to the seminar with different complementary

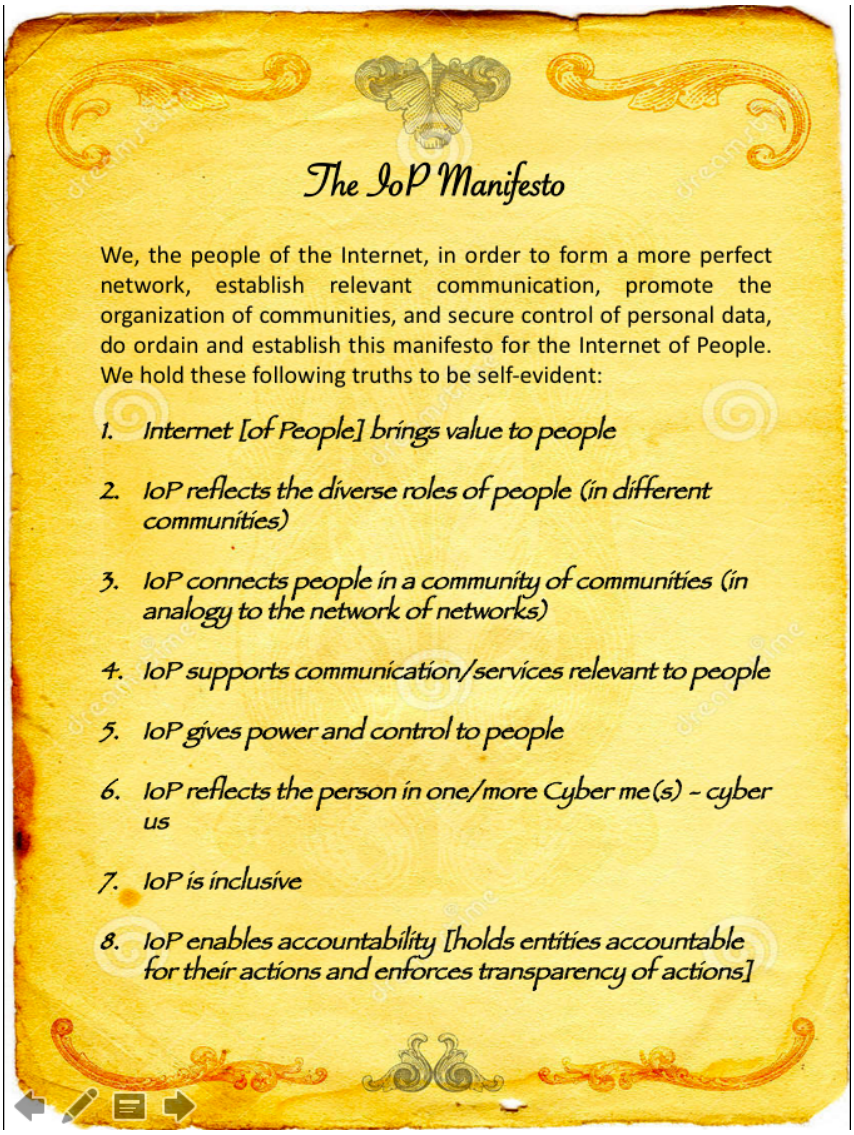

Figure 1 The IoP manifesto.

views, which helped stimulating useful discussions. Overall, we can tell, also looking at the feedback provided by attendees, that the seminar was successful, and attendees have been very happy to take part to it.

The topics discussed ranged from the definition of IoP, to privacy aspects, architectural approaches, security and privacy. We also covered topics such as QoE in IoP, and the need to account for the 80% of the population that is living in developing countries. Thus, the role of people in IoP was largely debated, as well as use cases for this brand-new concept.

Outcomes of the seminar consisted in elaborating a possible research roadmap, outline a set of toolkits, and defining an initial IoP manifesto. Even beyond that, the seminar put together a community of motivated researchers across the world, who had the opportunity to share ideas and initially shape a possibly hot research area for the Next Generation Internet. In the view of the organisers, establishing such a community was one of the primary goals of the seminar, which has been thus fully achieved.

References

1. Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019," Cisco, Tech. Rep., http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-indexvni/white_paper_c11-520862.html, 2015.
2. M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. Troster, G. Tsudik, and F. Zambonelli, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence," Pervasive and Mobile Computing, vol. 8, no. 1, pp. 2–21, 2012
3. P. Reichl, "From QoS to QoE: Buzzword Issue or Anti-Copernican Revolution?", Keynote abstract, Proc. EuroNF Workshop on Traffic Management and Traffic Engineering for the Future Internet, p. 23, Dec. 2009.
4. E. Daly and M. Haahr, "Social network analysis for information flow in disconnected Delay-Tolerant MANETs," IEEE Trans. Mobile Comput., vol. 8, no. 5, pp. 606–621, May. 2009.
5. P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay tolerant networks," IEEE Trans. Mobile Comput., vol. 10, no. 11, pp. 1576–1589, Nov. 2011.
6. M. Conti, M. Mordacchini, and A. Passarella, "Design and performance evaluation of data dissemination systems for opportunistic networks based on cognitive heuristics," ACM Trans. Auton. Adapt. Syst., vol. 8, no. 3, pp. 12:1–12:32, 2013.
7. P. Reichl, "Quality of Experience in Convergent Communication Ecosystems", 2013.
8. P. Reichl, A. Passarella: Back to the Future: Towards an Internet of People (IoP). Invited Paper, Proc. MMBNet 2015, Hamburg, Germany, September 2015.
9. Marco Conti, Andrea Passarella, Sajal K. Das, The Internet of People (IoP): A new wave in pervasive mobile computing, In Pervasive and Mobile Computing, Volume 41, 2017, Pages 1-27, ISSN 1574-1192, https://doi.org/10.1016/j.pmcj.2017.07.009.

Participants

- Panayotis Antoniadis
Nethood – Zürich, CH
- Chiara Boldrini
CNR – Pisa, IT
- Dimitris Chatzopoulos
HKUST – Kowloon, HK
- Nicola Dell
Cornell Tech – New York, US
- Peter Fatelnig
European Commission
Brussels, BE
- Markus Fiedler
Blekinge Institute of Technology – Karlshamn, SE
- Huber Flores
University of Helsinki, FI
- Heikki Hämmäinen
Aalto University, FI
- Tobias Hoßfeld
Universität Duisburg-Essen, DE
- Paul Houghton
Futurice Oy – Helsinki, DE
- Pan Hui
HKUST – Kowloon, HK
- Teemu Kärkkäinen
TU München, DE
- Eemil Lagerspetz
University of Helsinki, FI
- Anders Lindgren
RISE SICS – Kista, SE
- Pietro Lio
University of Cambridge, GB
- Kirsi Louhelainen
Barona Technologies – Helsinki, FI
- Leonardo Maccari
Università di Trento, IT
- Jörg Ott
TU München, DE
- Maximilian Ott
CSIRO – Alexandria, AU
- Andrea Passarella
CNR – Pisa, IT
- Daniele Quercia
NOKIA Bell Labs – Cambridge, GB
- Peter Reichl
Universität Wien, AT
- Jatinder Singh
University of Cambridge, GB
- Thorsten Strufe
TU Dresden, DE
- Gareth Tyson
Queen Mary University of London, GB
- Ellen Zegura
Georgia Institute of Technology – Atlanta, US
- Mariya Zheleva
University of Albany – SUNY, US
- Martina Zitterbart
KIT – Karlsruher Institut für Technologie, DE