10th Meeting of the Internet of Things Expert Group

Brussels, 14 November 2012

Tom Wachtel, rapporteur

1. Introduction

1. Opening remarks

Chair: Guiseppe Abbamonte, Head of DG CONNECT Unit H4, Trust & Security

The Chair opened the meeting by introducing himself and his colleagues Florent Frederix and Olivier Bringer, and outlined the scope and purpose of the meeting.

Scope and purpose

The objective of this final meeting is to finalise the outputs of the Internet of Things Expert Group, which has now been operating for two years, and to present its findings and recommendations on Commission policy formulation with respect to the Internet of Things (IoT). This has been a very useful exercise, with an immense amount of work done. As might be expected, given the broad range of different stakeholders represented, agreement has not been reached on all issues.

These outputs will contribute to IoT policy formulation exercise to be conducted over the next year.

The public consultation exercise is currently in the form of a draft report. Its status is currently confidential as it has not yet been published.

Q&A

There were a number of questions from the floor about the timing and outcome of the policy formulation exercise. The Chair clarified that the outcome was not predetermined and all options would be assessed before the Commission decided on the most appropriate approach. Gathering relevant input from stakeholders, as well as analysing the situation with respect to horizontal rules, in particular data protection, is essential to ensure proper assessment of the different policy options.

Minutes of preceding meeting

The meeting was asked to approve the minutes of the preceding meeting. There were no comments from the floor and the minutes were duly approved.

2. Commission presentations

1. Results of the public consultation

Speaker: Florent Frederix

Additional responses were received since the last report, with the total number rising from 500 to more than 600. These additional responses did not affect the statistics for the exercise as a whole. Some 50% of respondents fall into the "interested citizen" category rather than belonging to a particular industrial, academic or other sector.

Rather than presenting a quantitative analysis of the responses, as at the last IoT expert group meeting in June, a qualitative analysis was presented of the main issues covered.

Privacy

A conflict is evident between the generic issue of privacy and issues that arise in specific cases, and opinions vary as to the need for specific legislation with respect to IoT. Generic legislation already exists and may be appropriate for direct application in this area. However, there may also be value in introducing specific new legislation for IoT, and in developing, for example, specific data protection impact assessment measures. It will be important to consider how business cases may be affected, considering comparable issues such as the use of cookies on webpages, etc. Some argue that a potentially harmful situation could result if users had to give explicit permission for objects to function as intended or required. There are, however, converging views that privacy by default is a requirement.

Safety and Security

Diverse opinions were also evidenced on this issue. Prescriptive rules offer assurances about safety and security, and improve the effectiveness of security measures (e.g. seatbelts in cars). Time-limited certification could also be an interesting tool. However, binding guidelines and standards also introduce additional delays and costs. Some opinions suggest that no generic approach is feasible, and therefore that approaches should be driven by the specific needs of different industries.

Ethics

Ethical considerations are a new topic in the context of IoT. In consequence, it is difficult to make definitive decisions. IoT challenges user control, or at least shifts the locus of control (as in the automatic gearbox). For some respondents, this potential loss of autonomy requires proportionality and transparency. Moreover, getting informed consent from users will be of paramount importance, yet achieving informed consent in the context of IoT is likely to be very difficult. There is the additional problem of possible discrimination being introduced in terms of cost of access, age or other factors potentially affecting access to this technology.

Identifiers

The huge number of uniquely resolvable identifiers presents a number of problems. Globally unique permanent identifiers ensure interoperability and open up the possibility of creating IoT applications that draw functionality from interoperability (e.g. smart meters can assist in providing independent living applications for the elderly, temperature sensors and weather data can support intelligent home heating systems, etc.). However, they can also introduce considerable technical and design costs in advance of demonstrable proof that the benefits of this openness and interoperability are achievable. It has been shown that different naming systems can coexist, which presents to some extent an alternative approach. Also, short-lived or one-off identifiers have the advantage that they enhance privacy and security. Another point that emerges from the consultation results is that the reuse of existing protocols (IPv6) and open APIs should be promoted and can contribute to interoperability. Some opinions suggest that, in the long term, it will be markets that decide on whether open or closed platforms will be adopted (cf. past efforts such as Betamax and others).

Governance

The main consideration is whether governance should be administered using existing internet platforms or whether new platforms are required. There are three perceptions of the relationship between IoT and the internet in general:

1. The internet is simply a part of IoT
2. IoT is just an internet application
3. A range of different applications constitute IoT

These perceptions lead to different considerations for governance, including whether IoT-specific legislation is required to govern privacy and security, and whether, if needed, it should be soft (non-binding) legislation.

Arguments in favour of a multi-stakeholder governance platform hold that existing internet governance bodies are slow. Also, some argue that standards can be an appropriate instrument for this governance platform.

Standards

There are already many European norms that govern various aspects of life. The question is whether new additional norms are required for IoT. The same diversity of views emerges, where the benefits of such norms for privacy are counterbalanced by fears that they will introduce delays, and that in any case circumstances will shift over time, requiring a continuing evolution of standards.

Q&A

There was a question from the floor about what the European Commission's mandate on standards will address. In reply, it was stated that there are currently more questions than answers, and that if there is such a mandate, it will probably address issues such as privacy rather than technical issues. It was also proposed that the topic should be raised in the appropriate subgroup rather than in this plenary meeting.

2. Cybersecurity strategy

Speaker: Olivier Bringer

The objective of the European Commission's cybersecurity strategy is threefold:

1. to develop a plan to ensure a safe and resilient environment
2. to address cybercrime
3. to develop an external cybersecurity policy

Cybersecurity is a top priority for the European Commission and the European Union in general for a number of reasons:

1. There is a growing dependence on the digital environment
2. New threats are constantly emerging
3. These threats reduce trust: 30% of Europeans do not trust the internet for banking or for online purchasing, and 90% choose not to reveal personal information online
4. There is insufficient preparedness in the face of potential new threats
5. The exchange of information between various stakeholders is limited

The development of this strategy focuses on a number of key areas:

1. Fostering preparedness
2. Raising awareness
3. Developing and integrated security market
4. Fostering R&D investment
5. Addressing cybercrime
6. Formulating a coherent international cyber policy
7. Promoting European core values
8. Increasing global cooperation with Third Countries
9. Improving cyberdefence capabilities

A legislative proposal on Network and Information Security will be proposed as part of the strategy, with the objective of developing cybersecurity capabilities at national level as well as improving cooperation across Europe. New sectors (enablers of key internet services, banking, energy, transport, health, public administration) will be required to adopt risk management measures and to report security breaches to the appropriate authorities, a requirement which currently applies only to the telecoms sector.

The benefits that this legislative proposal is expected to bring include trusted cooperation between national authorities and a cross-sectorial approach that will increase the resilience of European society and its economy. This will increase trust and improve the functioning of the digital internal market.

Public consultation has just concluded and policy work is ongoing. Adoption of the strategy is expected in the coming months.

Q&A

The discussion raised the question of the relevance of these issues to IoT, in that this term is being used to mean a very broad range of concepts and technologies, and becoming equivalent to the word "technology". This risks defocusing the

work of the Expert Group, and it might be beneficial to concentrate specifically on IoT.

In response, it was pointed out that IoT is indeed part of a broader infrastructure and institutions such as banks, and others, will have to ensure that, if they adopt IoT, their products and services are provided in a secure way, including by meeting the requirements set out in the legislative proposal once adopted. Moreover, the issues under consideration are also relevant as background information to the members of the Expert Group in terms of what the European Commission is doing in areas related to IoT.

This concluded the introductory sessions by Commission representatives. Sessions reporting on the work of the individual subgroups followed.

3. Subgroup presentations

1. Ethics

Speaker: Jeroen van den Hoven

A key aspect of the work on ethics with respect to IoT is that it is hard to get people engaged in describing the issues involved, even though everyone agrees that ethics is important. What the general public have to say on the matter is crucial, but it is hard to even define what the appropriate data are when it comes to ethic issues.

Over the years, approaches to ethical issues have become ever more practical in nature. Engineers and other technical experts are becoming involved and this involvement is essential if the work on ethics is to be relevant in a practical way.

Three specific groups were involved in the consultation process:

1. The European Group on Ethics, examining how the use of IoT changes the relationship between people and objects
2. The ETICA project, addressing issues of future interest in the area, in particular by analysing 10 years of publications on ethics in ICT
3. The Expert Group on Responsible Research and Innovation, considering issues of responsibility in areas such as Smart Grids, Smart Meters, and so on

Ethical arguments in favour of IoT centre on the benefits it brings in terms of utility, wellbeing, health, safety and security, and the epistemic and moral responsibilities it brings in terms of promoted ethically motivated decision-making (i.e. better decision-making). The morally relevant characteristics of IoT include in particular ubiquity, invisibility, identification, ambiguous ontology and connectivity. Additionally, people are not accustomed to objects having an identity, or to the phenomenon of emergent autonomous agency, especially when objects act in unexpected ways or display apparently intelligent behaviour.

Issues of control also have ethical dimensions. Increasingly seamless interaction will lead to distributed control and an unpredictable, uncertain and complex environment in which informed consent could become an obsolete notion.

<u>Data protection</u>

IoT will generate enormous amounts of data. This raises ethical issues about the fundamental purposes of data protection, namely, harm prevention, equality, contextual integrity (data repurposing) and moral autonomy (the presentation of the self). In particular, IoT will introduce new difficulties for contextual integrity, the principle whereby information supplied for use in one context (e.g. a meeting with one's doctor) is not expected by the owner of the data to be used in a different context (e.g. the doctor applying for a mortgage).

<u>Social Justice</u>

IoT may increase the digital divide. Not all citizens may benefit equally from IoT. We already observe, in the financial sector, that millisecond differences in

acquiring information can be critical, and the consequences of similar effects in other areas of society must be evaluated.

Trust

It is important to distinguish between trust and confidence. Users may have trust in the use of IoT, or confidence in it, or both or neither. Ensuring that issues of trust are handled well will increase the value of IoT.

Separation

IoT will blur the boundaries between contexts and social spheres, and therefore introduce increased levels of difficulty in areas where such boundaries are not only expected but also critical.

Discourse framing

The metaphors used to express IoT are not neutral. They will affect perceptions of the benefits and dangers of IoT. For example, IoT could be framed as Orwellian Big Brother technology in which individuals have little or no say in how their environment in controlled. This would in turn impact on perception, adoption and success.

Agency

IoT will generate new difficulties in allocating responsibility and, more critically for some parties and some situations, liability where unforeseen events cause harm, damage or any other kind of undesirable consequences or effects. There will be a social contract between people and objects, and the ethical ramifications of a contract of this kind must be considered.

In conclusion, moral values should not be considered as limiting constraints on the successful rapid introduction of innovation, but as drivers of innovation itself. Values are always built into the design of any system, whether consciously or not. Being clear and explicit about the importance of value-sensitive design will help to make the transition from the desiderata expressed by people to engineering solutions and sociotechnical IoT systems. The role of engineers as "choice architects" must be recognised and managed appropriately so that principles can be developed for how to design for X, where X might be privacy, inclusion, etc.

It is important to learn from the aborted introduction of smart meters in the Netherlands, where a failure to properly consider privacy issues at the design stage led to a costly waste of technologically sound but ethically unfounded work. In short, we should not be concerned with self-parking cars but with the ethical foundations and consequences of delegating parking decisions to automotive systems.

Q&A

A question from the floor requested clarification about whether IoT should be used to minimise digital separation, the digital divide, and whether indeed such an objective was valid and possible. Would a consequence be that those with abilities and talents would be prevented from rising?

The reply stressed that the issue was about positionality rather than separation. Financial organisations may want millisecond advantages, but it is probably undesirable in healthcare, for example. It is about equal opportunity, not equal people. In general, there is a need to stimulate discussion and debate about the proper way to distribute advantages in IoT.

A further point was made from the floor that it is important to focus on IoT, not on general matters. Greater focus is needed in IoT as a stimulus for European markets. We should first create IoT and add functionality later, with markets balancing costs against benefits.

The reply was that costs must indeed be balanced by markets, but infrastructure is not neutral. Moreover, once in place, infrastructure has consequences (e.g. the design of a road network). It is for this reason that considering consequences at the design stage is important. Design choices are not value-neutral.

A further question from the floor commented on the perception of privacy concerns as a burden and an overhead, whereas in fact market research shows that there is a market for privacy and it could become a major growth area.

The reply expressed agreement and cited the German experience with environmental issues and sustainability, where apparently limiting social and political constraints have resulted, after many years, in Germany now being the leader in technologies for sustainability. Responsible innovation need not be an impediment to business success.

2. Privacy

Speaker: Andreas Kirsch

The subgroup document was submitted in June. No replies or comments were received, so it is assumed that the group as a whole accepts it.

A number of points relevant to this subgroup were covered by the preceding presentation. However, the main point that emerged from the work of the subgroup is that everyone will be affected by IoT but many will not realise it.

Privacy

The broad impact of IoT systems raises concerns about privacy and how to ensure that data protection and security are incorporated properly. The principal problem is the cross-linking of objects. This requires that profiling is done well and that information systems cannot be corrupted. We therefore need data protection and security at the design stage.

Deanonymisation and repersonalisation

There are risks associated with the possible repurposing of data. Anonymised information may be deanonymised, and large amounts of detailed information, even if anonymised, will allow the potentially damaging repersonalisation of data in IoT.

Loss of control

A further risk is that people may feel that they have lost control. IoT systems will largely be invisible, and unnoticed as long as they work as intended. Automatic decisions will be made, and it is not obvious that people will find this desirable or beneficial.

Locking in

The nature of IoT may lead to users becoming locked in with a specific service provider. Moreover, a single dominant market leader may emerge leading to a lowering of choice for users. A monopoly situation may arise, even if there is no formal monopoly, as has happened with social networks.

Health

Direct health risks should not be underestimated, including physical risks (e.g. internet connected pacemakers). Increased automation may lead to direct health risks in cases of technology failure.

Conclusions

The main conclusions relate to three issues:

1. Data protection legislation
2. Privacy by default
3. Standardisation

Effective legal data protection is needed for IoT. Policy options include risk management at the design level for issues relating to privacy, and in order to reduce costs.

Privacy by default is a priority. There is an opportunity for Europe to become a market leader in this area. Data protection legislation is on the way, or is at least being discussed. European harmonisation of such legislation is necessary, supported by enhanced enforcement.

Standardisation is very important. Technical standards in which data protection issues are considered appropriately are crucial for interoperability.

Q&A

The Q&A session revealed a significant divergence of views within this subgroup, in particular with respect to the question of introducing new legislation specific to IoT. A substantial part of the subgroup felt that such legislation would not only introduce considerable burdens, but would also quickly become obsolete, and therefore dissociated themselves from the conclusions in the formal report. While privacy by design is a valuable proposal, a prescriptive one-size-fits-all model would be too restrictive. This position has been outlined in a separate paper on principles produced by those who hold this position.

Apart from these two opposing views, a number of members expressed a middle view, holding that no decision on this issue can be made at this stage.

The members opposing the introduction of a new regulatory framework explicitly designed for IoT felt that the work of the subgroup was incomplete.

The final report had not changed substantially since the previous meeting in February 2012, as it had not always been possible for the subgroup to meet. Some of the member organisations have collaborated to produce a number of principles, such as stipulating that IoT must be seen as part of a continuum alongside other technological developments, and that privacy issues must be discussed at a practical level relating to the prevention of harm.

There were also contributions from the floor representing the opposing view, stating that there were opportunities for European companies in privacy and data protection, in creating a European ecosystem. Europe's advantages include mobility, and data that the world wants. Moreover, Europe has engineers and designers with skills that are appropriate for the development of systems of connected objects.

Moreover, discussions should not be restricted to principles and ethics, plus some issues unrelated to current internet services. For example, RFID tags will last for decades if not centuries, making opting-out a more difficult option. Therefore good design is essential, as is effective protection from malware of various kinds. It is essential to create an ecosystem for services and products to thrive. It would be a mistake not to include privacy issues at the design stage. There is a five-year window of opportunity for Europe to become the leading force in IoT, and getting the architecture right is key to this.

For a third group of experts, Europe needs to be convincing, and a new regulatory framework for data protection will address all the issues under discussion, and for all sectors. Nevertheless it is premature to decide on a new regulatory framework for IoT at this point. It is preferable to wait and see how the general IoT framework will develop, while being aware of what is different about IoT and what it might require in terms of a new regulatory framework.

In reply, it was noted that most people use the same concepts when discussing IoT as when discussing the internet in general. There is a significant difference, however. IoT involves object talking to each other without user consent, with possibly unenvisaged functionalities. Cameras, for example, might take on functions that are different from their overt primary functions. These possibilities, once perceived, may cause user anxieties to rise. Moreover, what is the role of user consent if objects may be able to talk to each other spontaneously? It will be very difficult to backtrack after the deployment of millions of chips employing a passive approach to connectivity.

Those sceptical of new regulations wished to clarify that industry does not dispute the fact that privacy protection can enhance competitiveness, but disagrees on the tools to be used, believing that existing constraints are sufficient to boost European competitiveness.

At this point, a further view was expressed wondering why only now, after two years of work, the Expert Group is being asked to consider the question of whether or not IoT is different from other internet technologies or applications in order to justify the need for specific regulation.

Another view expressed puzzlement about the to-and-fro of the discussion on privacy, holding that the core issue was the method, and that IoT is part of the internet continuum. Different devices have different constraints, (e.g. in the

medical sector), and therefore existing laws need to be applied on a case-by-case basis, as high-level generic rules are impossible to formulate.

Another supporter of the need for new regulations suggested that apparent constraints of this kind could not only be a stimulus for innovation but also for new business, citing the example of cookies, which had initially been greeted with claims that they would be impossible to implement but have now led to European businesses offering solutions. Current measures were not sufficient for IoT, and people did not know how to apply current legislation and principles. Not only will new privacy safeguards be required, but there will also be a need for guidance on how to apply the existing regulatory framework.

Another participant offered the view that the significant difference between IoT and other internet technologies is that billions of objects will be involved. The difference is quantitative rather than qualitative. In this context, the control issue is a challenge, and how to incorporate user consent into the IoT scheme. This is an opportunity for new business. In fact, the USA is currently looking at how Europe is approaching the issue of privacy.

While agreeing that guidance in the application of legislation is required, another participant pointed out that IoT is a global phenomenon, and it is therefore important not to constrain European work is a way that makes it valid regionally but hampered globally.

It was also noted that binding European guidelines would be useful as an instrument to exercise control and as industry standards. However, while European legislation is binding, guidelines issued by the Commission do not have the same force.

China is keen to embrace responsible innovation, as is Russia. China is examining its implications for cities, bridges, water distribution and roads. Europe needs to delve deeper into the ethical side before it is too late, and that means now.

The costs of failing to recognise the need for adequate design-stage data protection measures must not be underestimated. Moreover, regionality may bring additional problems, in that if there is inadequate data protection in one country, other countries will be affected. Specific legislation is therefore required.

As the session drew to a close before breaking for lunch, the Chair reminded the forum that it was in any case unrealistic to imagine that any new IoT-specific privacy legislation might be implemented ahead of more general privacy legislation.

3. Architectures

Speaker: Patrick Wetterwald

The final document has not evolved much since the preceding meeting. The main recommendations for architecture design for IoT include:

1. Fair access to infrastructures, across all devices, including cost considerations as well as technical issues
2. Spectrum management is crucial for effective wireless connectivity
3. Interoperability: there have been too many proprietary solutions in the past, a situation that must not be repeated
4. Object identifiers must be designed appropriately

In practical terms, the Smart Grid Architecture Model used in smart meters, the first deployment of IoT, may be applicable in other areas. It is also essential to have open standards, with IPR issues addressed well.

IP will be the main technology applicable to IoT. The discussion briefly questioned the difference between European Standard Organisations (SDOs) and others. IETF is the pre-eminent international standards organisation for the internet, but it is not recognised as an SDO in Europe, which represents a problem because existing SDOs do not have comparable competence in internet standardisation. The M/490 Smart Grid reference architecture will also be important. Some 100 person-years have been put into developing it, and using it imposes consistency across stakeholders and interoperability from the physical technology level to political and regulatory levels, supporting reusability in IoT domains beyond Smart Grid, which was its first deployment.

Q&A

A question was raised about how consumers fit into this framework. The reply was that consumers are part of the business model rather than the architecture.

A further comment pointed out that numerous consumer benefits were claimed for Smart Grids, but the functionality that could actually provide these benefits was not implemented, and as a result the benefits did not materialise.

4. Standards

Speaker: Marilyn Arndt

There are no updates to report since the preceding meeting of the group.

There is however an important standardisation exercise to be reported on: OneM2M (http://www.onem2m.org/), a global partnership started some 18 months ago.

Currently the industry is fragmented, with M2M/IoT solutions mainly developed under a vertical model (application-specific developments). There is therefore a need for a common service layer that fosters reuse and interoperability between applications and devices.

OneM2M was initiated and will be chaired by ETSI and will bring together SDOs and industry associations from other regions of the world (USA, Asia) and from different industrial backgrounds, i.e. not only telecom operators and manufacturers but also service providers and end-users from all industries. The first release of OneM2M standards is expected by the end of 2013.

OneM2M does not at present address privacy issues. It would therefore be valuable for members of this Expert Group to consider participation.

Q&A

The questions mainly concerned getting additional information about OneM2M, such as how to get involved, whether IP standards were being addressed and its relationship to other initiatives like ITF and the DONA project. The issue of how to resolve the issue of the classification of standardisation bodies in general was also cited as a problem.

5. Identification

Speaker: P. J. Marron

The speaker announced that there had been very little input since the last meeting, and that therefore any summary trying to wrap things up was more likely merely to raise new problems.

Identifiers

A number of issues remain unresolved, including whether an identifier should be the same as a network ID, how discovery and resolution should be handled, whether unique or multiple identifiers should be used, whether a single global scheme should be adopted (using perhaps IPv6 or 6LOWPAN) or a solution based on different interoperable schemes using routing algorithms. One problem is that global identifiers are hard to manage for all types of objects and that network addresses change as objects move through different domains. The best route therefore appears to be interoperability.

Resolution/Discovery

The current proposal is to use the ONS approach and the existing internet domain model. However, it is important to ensure that the discovery system adopted will continue to work into the future, including being scalable up to billions of devices and efficient even for the smallest and simplest objects (e.g. individual light bulbs). Moreover, different considerations may apply in different sectors. In the medical sector, the value is not in the connectivity but in the data, for example. Requirements need to be defined to determine appropriate objectives. Transparency and network independence also impose constraints, such as naming scheme not disclosing location, for example. Support for mobility must also be included, as people move around while performing a single function or role, thus requiring virtual locality (e.g. "at the office" while physically at any actual location).

Privacy

It is impossible to envisage all possible misuses or abuses of privacy or to design ways of preventing them. This does not however mean that we should abandon work in this area. Flexible authentication should also be supported, in that users may wish to adopt different personae.

Trust

Reliability generates trust. If semiautonomous cars stop unexpectedly and need to be rebooted as often as some operating systems we know, drivers will not be happy.

In general, two areas of policy making need to be distinguished, that of technical and market development, where standard methodologies are likely to prevail, and that of political discourse, which may change the rules of the game. Moreover, non-binding recommendations have limited impact, and potentially no effect at all outside Europe. Open source solutions may work better. In any case, there is no one-size-fits-all political solution.

Q&A

The Chair thanked the speaker for outlining policy options and scoping the possible consequences of different decisions, noting that this is exactly what was hoped for from the work of this group.

There were no questions or comments from the floor.

6. Governance

Speaker: Wolfgang Kleinwächter

There is nothing to report since the last meeting in Venice.

There is continuing disagreement about what is required for IoT governance, and whether IoT is new and different entity or an extension of what already exists. The majority of the subgroup appears to agree that it would be premature to propose new principles or guidelines at this point, and that there is indeed no need to do so, with current internet governance being sufficient for IoT. Likewise, there are two different views about the nature of governance mechanisms to be adopted, with one view recommending regional bodies and other organisations and the other view holding that it makes no sense to create new governance bodies as currently existing bodies are well suited for the purpose. This does not mean that discussion and debate should cease, simply that there is no agreement or consensus at present.

Three key issues are of particular relevance to policy decisions:

1. Privacy
2. Security
3. Competitiveness

No specific actions on policy are proposed at this stage. It is important, however, to remember that IoT is not limited to the territory of Europe. While Europe is in a position to contribute a great deal, actors in the USA and Asia will also be developing their own policies and plans.

As for the future of the task force (the Dynamic Coalition on IoT), most members felt that it would not be appropriate for it to close, and that it could perhaps continue as a clearing house for policy proposals, but without executive powers or functions.

Q&A

Several questions returned to the issue of whether new governance instruments were needed or not. The views expressed included:

1. The IoT concept and related apps are in early phases of development, and no new governance framework is required.
2. Existing organisations should be broadened as required to accommodate IoT if necessary, adding issues such as consumer interests, ethics and corporate social responsibility.
3. It is dangerous to envisage separate organisations for IoT governance, but existing internet governance organisations need to be benchmarked. The case of ICANN's drift from its original multi-stakeholder purpose in 1998 (and its original budget) to how it operates today (and its current budget, 25 times larger) must be avoided.
4. The new ICANN CEO wants to change its American dominance. In any case, ICANN issues should not be confused with IoT.
5. Existing internet governance has several positive aspects. For IoT, issues such as registering RFID space under DNS should be given particular attention.
6. RFID could also potentially operate directly over IP (e.g. IPv6), not necessarily over ONS.

A number of industry recommendations were also expressed.

Industry should implement appropriate safety and security requirements addressing different types of risk, with strong coordination, harmonisation and consistency across breach notification systems to avoid divergent and confusing rules. Such systems must not be made overly burdensome, however.

IoT-specific policy issues should be addressed using existing internet governance platforms. The current IoT multi-stakeholder process taking place via existing platforms like the Internet Governance Forum (IGF) is valuable. Incentives should be introduced for companies to be compliant with European guidelines, and information-sharing with EU and national authorities should be encouraged.

Interoperability and standards should be fostered as a policy goal in view of their of central importance in facilitating the innovation and marketing of smart devices, objects and applications for IoT. This will also help promote trust in IoT devices and services. Policymakers and industry should also promote interoperable standards that are consensus based, globally recognised, and market driven, with security requirements for specific applications considered appropriately at the design stage.

The Commission’s references to IoT as a cross-cutting issue in proposed legislative measures for the Horizon 2020 programme are very welcome. IoT is perfectly positioned to contribute to the goals of Horizon 2020, as it addresses broad societal problems and is an area where the EU and Member States have already achieved significant results. Further substantial research and funding remain necessary, however.

4. Conclusion

Before closing the meeting, the Chair invited a Commission colleague to describe ongoing work on corporate social responsibility.

1. Corporate social responsibility

Speaker: Marina Kirova

The Commission seeks to encourage and enable European enterprises in the ICT sector across the EU to apply social corporate responsibility policies by taking a strategic approach to corporate cooperation in partnership with other relevant stakeholders (e.g. civil society, academia, public interest actors, NGOs, etc.), and by identifying good practices through which societal benefits can be delivered via the Internet and other ICT.

Inputs are invited on the following issues:

1. Do we need a single platform for CSR issues in the ICT sector, and what priority topics should be addressed?
2. What should the general and specific goals of the platform be?
3. What should be the possible organisational arrangements for the platform (in particular, whether the secretariat should be provided by the Commission or by the stakeholders)?
4. Which tools/information should such a platform use/contain?

2. Closing remarks

The Chair thanks all participants for their vigorous engagement in the discussion and debate.

Any future policies will take stock of horizontal rules and will not be designed in isolation. It appears to be the case that existing regulatory instruments in general provide the right framework for IoT. Only issues that cannot be addressed using existing regulations should be addressed under new ones that might be created. In any case, as noted earlier, no regulatory framework specifically addressing IoT issues could possibly be adopted before other more general frameworks are adopted.

The Chair requested that final versions of all documents be submitted by 28 November 2012, taking the day's discussions into account and adding policy options for the Commission to consider and evaluate.

The meeting closed.