23.01.2019

Re: EDRi's to BEREC consultation on Indicators for Internet of Things

European Digital Rights
12 Rue Belliard
1040 Bruxelles, Belgium
www.edri.org

Contact information: Claire Fernandez, claire.fernandez@edri.org, +32 2 274 25 70

EDRi is a pan-European NGO and umbrella organisation of more than 30 European associations working on human rights issues in the digital world. EDRi follows the regulatory developments around the Internet of Things, notably challenges arousing with regards to the right to privacy, data protection rights and the right to the "silence of the chips". Following the publication of the European Commission's Communication "Internet of Things – An action plan for Europe" in 2010, EDRi participates in the EC Expert Group set up from 2010 to 2012 to work on governance, privacy and data protection, standards and interoperability, health and environment and other topics related to the development of an Internet of Things.

The contributions made to this consultation are the results of an internal collaboration between EDRi members, mainly Article 19, Hermes Center, Open Rights Group and IT-Pol.

Question 1.1:
Do you consider that the European Commission's definition of the IoT is sufficiently appropriate to collect relevant statistical information on the IoT? If not, how should the definition be changed?

Answer to question 1.1:

The Commission's definition is limited in so far as that it assumes devices/objects interact autonomously, and that is assumed they have to create action **and** value. One could imagine IoT networks which in fact report data to a human agent if there is a need for this, or that an IoT network is able to create action but no value, or value (in the form of a data asset) but no action (meaning that it only passively monitors a surrounding or environment).

In addition, the Commission definition doesn't consider the data gathering aspects of any IoT object. Because of sensors all IoT devices contain, any IoT object is a data collector. A fleet of identical objects generates a data stream that first reaches the IoT fleet management infrastructure, even before being used by other objects. The reason behind is the current way IoT objects are built, using the infrastructure and services of an IoT service provider (for example Particle Systems, Amazon, Google, etc.). The IoT service provider becomes a "hub" of all the data streams collected by an IoT fleet, and of all fleets built on top of it. As a result, providers can (ab)use this "hub" role not only to feed other objects of the same fleet with data, but to store the collected data on data mining systems, or use it in any other activity that the current "data economy" allows.

If it is anticipated that such details will present problems to BEREC while collecting statistics, the Commission's definition could be altered in the following way:

> "*objects* ***collecting and*** *sharing information with other objects/members in the network, recognizing events and changes so to react autonomously in an appropriate manner,* ***or to solicit human feedback****. The IoT therefore builds on communication between things (machines, buildings, cars, animals, etc.) that leads to action* ***or*** *value creation.*"

Question 1.2:
Please suggest any available sources for information on measures/indicators of the IoT, in addition to the information mentioned above.

Answer to question 1.2:

In addition to following market surveillance reports, BEREC could attempt to keep track of standardisation efforts in the field. This will for instance help BEREC in understanding when there is overlap between activities that fall under the supervision of BEREC and activities which may fall under the supervisory authority of other public authorities.

ETSI's website detailing their ongoing standardisation efforts is instructive, since it contains a breakdown of various projects in IoT (such as ITS and Smart Grids) that are impacted by BEREC supervision.[1]Furthermore, the IETF LPWAN[2], 6LO[3], DETNET[4], and SUIT[5] contain further information about foreseen technical capacities. Passive monitoring of these fora would give BEREC an edge beyond marketing documentation.

In view of its priorities in terms of users' protection and empowerment, BEREC could move quickly on societal aspects of IoT by encouraging its members to actively look out for information about home automation misuse.[6] Home automation enables domestic abusers to control their victims in ways unforeseen by older technologies, and ensuring that there is a European level network capable of aggregating statistics on this issue at an early stage, may help policy development and awareness raising with manufacturers. This is closely related to both the core obligation of BEREC to ensure security in electronic communications networks and services, and the accessibility of such security features to the end-consumers impacted by them (usable security).

Connected home applications (or IoT devices generally speaking) give rise to concerns about

1 https://www.etsi.org/technologies-clusters/technologies/internet-of-things
2 https://datatracker.ietf.org/wg/lpwan/documents/
3 https://datatracker.ietf.org/wg/6lo/documents/
4 https://datatracker.ietf.org/wg/detnet/about/
5 https://datatracker.ietf.org/wg/suit/about/
6 https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html and https://sverigesradio.se/sida/artikel.aspx?programid=1650&artikel=7098797 [Swedish]

market actors in non-BEREC sectors offloading risk to insurance consumers, e.g. FitBit monitoring being used to determine health insurance premiums, or smart meters for water or electricity offloading liability for accidents in the home to the home owner. Increasing "efficiency" and lowering risk does not necessarily imply a passing on of those savings to the individual, but in particular it may also place individuals in a new situation that they are currently ill-equipped to understand or control. One example would be a water leak appearing in a household when the residents are on holiday: would they have the obligation to monitor, remotely, their water consumption of their house (for instance with an app) to determine the aberration and take measures against it, or would they still be protected by their home insurance?

It may help BEREC in this regard to keep an eye on the academic conferences IEEE Security and Privacy, WEIS, EuroUSEC or USENIX Enigma.

In addition, in order to monitor the fast expanding market of IoT services providers, some sources should be monitored, like:

- Free resources[7]
- Non-free resources[8]

Question 2.1:
Do you agree with the multi-layered approach in Figure 2 above, which seeks to separate M2M/IoT from the underlying connectivity and shows the relationship to ECS?

Answer to question 2.1:

EDRi agrees with the approach featured in Figure 2, but within some understanding of separation and of intrinsic limits of a business-only representation. M2M and IoT are applications of a chain of technologies existing on various levels of a value chain. Dividing various aspects of the network into layers is however sensible.

Taking some examples from the BEREC draft, one can observe that the LoRaWAN architecture envisaged by The Things Network appears to be able to encompass roughly eight actors: the chip vendors, the device manufacturers, the gateway server, the network server, the identity management (including login/join server), application server, monitoring services and integrated services. From a regulatory perspective, it is most important to understand if all of these eight actors can be commercially distinct, or whether a full vertical integration (management within a single entity) is required for the service to work. BEREC should anchor its assessment of M2M/IoT market segmentation in which commercial actors are able to operate on which markets. Consider in this regard the IETF overview of various IoT architectures, including their vertical integrations.[9]

7 http://asiandatascience.com/wp-content/uploads/2017/12/eBook-Internet-of-Things-IoT-2018-Market-Statistics-Use-Cases-and-Trends.pdf
https://www.postscapes.com/internet-of-things-platforms/
https://www.embedded.com/electronics-blogs/cole-bin/4426992/Finding-the-right-IoT-development-framework

8 https://www.gartner.com/doc/3879512?ref=unauthreader&srcId=1-3478922254
https://www.gartner.com/doc/3819264?ref=mrktg-srch

9 https://datatracker.ietf.org/doc/rfc8376/

Question 2.2:
What is your opinion on the differentiation of IoT and M2M? Do you have any additional proposals regarding such differentiation?

Answer to question 2.2:

EDRi believes that it is not clear that supervisory activities will benefit from spending a significant amount of time on this. Furthermore, in our opinion this differentiation between M2M and IoT should not justify different regulatory approaches since the privacy and data protection interests as well as the competition risks related to these communications are not materially different, or at least not through the distinctions made in this model. We do not consider whether the presence of human interaction is an important feature of an IoT device. The transmission of data to/from the device takes places by automated means over an electronic communications network, irrespective of whether the input or measurements are received through partial human interaction or solely through automated means. An IoT device without human interaction can collect personal data if the measurements obtained by the device relate to identified or identifiable natural persons.

Question 2.3:
In relation to application solutions, do you see the three categories "Industrial", "Automotive" and "Consumer" as the most relevant? Would you suggest other categories? If so, please elaborate.

Answer to question 2.3:

Two of the proposed categories are overlapping in an unfortunate way. We propose the following four categories: Industrial, Automotive, Open to the Public Spaces and Home applications.

The broadest of these categories would be Home applications, which encompass all IoT technologies that an individual might bring with them into their home (wearables, home automotion, smart appliances, smart electricity metres, custom IoT home routers, etc.). Open to the Public Spaces IoT would encompass technologies that individuals are likely to encounter in spaces which are open to the public, such as shopping centres, public squares or government buildings, including sensors or security equipment.[10]

The Automotive category should not exclude concerns of individuals and consumers, including in terms of data autonomy and data ownership, both of which are hugely influenced by the rules and regulations established by the technical standards and regulations in the field. Note that Home and Automotive may overlap in certain respects -careful thought would have to be given to how differentiation between these two categories would influence the ability of BEREC's members to ensure the interests of the European citizens are upheld in these markets.

We consider Industrial applications to be such applications that are restricted and limited to areas to which the public does not normally have access, other than when they are in a position of

10 Note that only using the words "Public Spaces" would not encompass spaces which are privately owned and operated, but also open to the public, e.g. commercial centres. This is established under for instance freedom of association and assembly human rights doctrine.

employment at the entity whose IoT network is covered by this category. However, these boundaries may become difficult to maintain as products' life-cycles get more complicated. For example, some cars already send performance data back to manufacturers to improve the next iteration of designs in what could be classed as an industrial process.

The categories can also be further expanded. In discussions about 5G verticals there are plans for a separate Health and Energy virtual networks, for example, that could reach consumers and not just industry. Therefore, the main issue in the long term is not so much to fix these categories but to create appropriate participatory processes for the governance of any IoT space, where particular rules may be applied, for example in prioritization of traffic or access to spectrum.

Question 3.1:
In your opinion, what effects on spectrum policy is the development of the IoT expected to have, and do you think it's necessary for NRAs to monitor, and BEREC to benchmark, these developments?

Answer to question 3.1:

Spectrum policy influences the choices made by technical standards bodies with respect to what avenues for new features they pursue, as evidenced by the recent initiation of 60GHz band functionality in IEEE 802.11 Tgbd.[11] Technical standards bodies, especially in fields which are heavily dependent on the regulatory landscape, rationally adapt their activities to perceived opportunities.

But this means the influence may be flowing in the opposite direction to that which BEREC appears to be envisaging: if BEREC waits for IoT development to influence spectrum policy, BEREC may inadvertently be supporting the use of licensed spectrum for IoT since licensed - and therefore economically strong - users will have better opportunities to leverage existing allocations. BEREC could support pro-active changes, in cooperation with relevant national and European competent bodies.

Pro-active changes to spectrum policy may, on the other hand, encourage actors to make use of unlicensed spectrum for more vertically flexible infrastructures and to develop technologies which can function on such frequencies. The success story of Wi-Fi originated, for instance, with the unexpected de-licensing of several spectrum bands in 1985 -even though the first functional technology was not available until 1997, and did not achieve wide deployment until 1999. Even though IoT development is unlikely to create such expected developments within similar time-scales, spectrum policy may from this viewpoint not be seen as something that is inherently *influenced by*, but rather something with which *influence is wielded*.

Question 3.2:
With regard to the expected growth in the use of IoT devices, do you see the necessity for NRAs to monitor, and BEREC to benchmark, these developments, particularly with respect to numbering? If so, why?

11 https://mentor.ieee.org/802.11/dcn/18/11-18-0861-09-0ngv-ieee-802-11-ngv-sg-proposed-par.docx

Answer to question 3.2:

EDRi does not believe that national numberings plans will affect the growth of IoT deployment in any way. IoT devices are likely to use several different electronic communications networks, and only some of these, mainly mobile networks, will involve the national numberings plan. For mobile networks, it is EDRi's understanding that data-only SIM cards have a technical phone number even though voice calls and SMS messages are not allowed by the mobile network. In this specific area, NRAs will need to monitor the availability of mobile phone numbers that can be assigned to data-only SIM cards used for Iot/M2M devices. However, any scarcity of (technical) mobile numbers for IoT/M2M devices should be relatively easy to address by making small changes to the national numbering plan. For example, Denmark has 8 digit phone numbers for all mobile phones and landlines, but there is a special number series with 12-digit numbers for M2M communication. This does not affect voice and SMS communications, and does not cause any confusion for citizens, because these SIM cards are only used for data traffic. In the long run, EDRi expects the telecommunications industry to move away from phone numbers entirely (except technical numbers like IMSI numbers for SIM cards which come from a much bigger numbering resource). In the meantime, any temporary problems with scarcity of phone numbers because of the growth in the number of IoT/M2M devices should be manageable by the NRAs with minor changes to the national numbering plan.

Question 3.3:
Do you see the need for NRAs to monitor which national numbers for IoT devices are used outside their domestic market/territory (and vice-versa, which numbers assigned in other countries are used in the NRA's territory)? If so, please elaborate.

Answer to question 3.3:

No. There are no important management/statistical benefits, while big risks exist of misuse/abuse of this information for technical control. See also answer to question 3.2.

Question 3.4:
In your opinion, in addition to NRAs, for which entities (EU and non-EU) are the following individual matters relevant:
(a) The effect of IoT on spectrum policy
(b) The effect of IoT on scarce resources, i.e. numbering
(c) The monitoring of national numbers for IoT devices used on an extraterritorial basis

Answer to question 3.4:

Referring back to Question 3.1, it is not clear in which direction influence flows with regards to spectrum policies.

Spectrum policies are interesting for SDOs (IETF, IEEE, ETSI), CSOs (notably community networks

and open developer communities such as OpenWRT) and the usual market agents. Spectrum policies determine the liberty to act for each of these actors. Notably, a European municipality could not decide to erect a local LTE-based network for IoT at this time - why is that? More flexible spectrum policies, such as spectrum sharing in unlicensed bands, could open a big commercial space for smaller entities in the European Union and could be an important driver for innovation in the IoT/M2M area. For example, the LoRaWan technology operates in the unlicensed radio spectrum.

Question 4.1:
What is your opinion on the benefit of a BEREC common approach regarding the IoT?

Answer to question 4.1:

It seems pertinent to observe that the least integrated part of the markets that BEREC supervises is the spectrum allocation. Because of territorial constraints on spectrum licenses, any licensed network provision is de facto constrained to the territory of the spectrum license and this effectively causes the European telecoms markets to be markets plural, rather than market singular. That said, every other aspect of IoT is European or global: data management, the corporations supplying hardware, software or services, cloud services, data collection, the consumer base and even the entities which own and operate the networking infrastructures under different spectrum licenses. A common approach regarding IoT could be motivated from this fact.

See also reasoning in Q4.3 below.

Question 4.2:
Do you agree with the general areas of interest for future indicators (to be collected), presented in Figure 4 above? Could you suggest any specific IoT indicators that BEREC should consider for collection?

Answer to question 4.2:

EDRi agrees with the areas of interest for future indicators. In the response to Q1.2 a separate social issue was raised which may be of interest, and that relate to BEREC's obligations to ensure accessibility and security of electronic communications services.

Furthermore, the collection of personal data and the GDPR compliance of these collections would be a necessary addition to BEREC's areas of interest. This work should be done in close cooperation with the Member States' Data Protection Authorities, the European Data Protection Supervisor, and the European Data Protection Board.

Looking forward, BEREC may want to start considering how to monitor the potential proliferation of low power devices. Hundreds of thousands of small devices with sensors are placed all over cities

and roads with non-maintenance batteries lasting up to 20 years, potentially a lot longer than the project or business behind them. Besides the environmental problems that these may cause more research would be needed regarding potential effects of electromagnetic pollution.

Question 4.3:
Do you support the gathering of statistical information on IoT by BEREC? Please substantiate your answer.

Answer to question 4.3:

We have no objection to the collection of statistical information on IoT at the aggregate level by BEREC. Given the global nature of the industry and the heterogeneous offerings of IoT devices, it is not clear how it could effectively be regulated at a national level in the EU. All providers of services on the IoT market are already under obligation to follow European harmonized regulatory frameworks in their respective sectors, in terms of communications technologies and services and in terms of consumer rights law.

We also would like to draw your attention to the conditions for the collection of such "statistical" data. "Aggregate" data collection is acceptable, while, for example "pseudo-anonymized" or "anonymized" data is not. Methods of deanonymization of "anonymized" data are mature, powerful and widely used, so risks outlined in the Q1.1 answer must be minimized.[12]

Question 5.1;
Are there any additional issues relating to collection of statistical information on the IoT which have not been included in previous questions that you would like to address?

Answer to question 5.1:

12 See Paul Ohms fundamental paper on re-identification of anonymized data "Broken promises of privacy: responding to the surprising failure of anonymization": http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006