IGF 2016 Workshop Report: Workshop 170

Session Title	The Network of Networked Things: Finding the Internet in IoT
Date	6 December 2016
Time	9:00-10:30
Session Organizer	Number Resource Organization (NRO)
Chair/Moderator	Marco Hogewoning, Chris Buckridge
Rapporteur/Notetaker	Antony Gollan
List of Speakers and their institutional affiliations	Anya Ogorkiewicz (Keryx Group) Grace Abuhamad (NTIA) Paul Wilson (APNIC) Oleg Logvinov (IEEE) Dominique Lazanski (GSMA) Corinne Cath (Article 19) Jari Arkko (IETF) Uta Meier-Hahn (Alexander von Humboldt Institut für Internet und Gesellschaft)
Key Issues raised (1 sentence per issue):	- There is a need to encourage participation from IoT developers in multistakeholder forums and technical communities such as the IETF. - The interrelation between industry self-regulation and standards on the one hand, and government regulation on the other. - Concern about security of devices, and what motivating forces can be employed to encourage greater attention to security by manufacturers and network developers.
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	n/a
Please describe the Discussions that took place during the workshop session: (3 paragraphs)	The rapidly growing IoT isn't different to the Internet but rather part of its evolution and is therefore covered by existing policies. The architecture of the Internet encourages cooperation between network operators, who engage with one another on policies and standards, and form peering arrangements for mutual benefit, which result in interpersonal networks and relationships. No similar structural factors exist to encourage cooperation between IoT developers. There is a need to encourage participation from IoT developers in multistakeholder forums and technical communities such as the IETF, and this outreach should include a community-building element as well. A major topic was the interrelation between industry self-regulation and standards on the one hand, and government regulation on the other. The IoT creates requirements for semantic interoperability

	between a range of different devices and applications. Industry has been quick to recognise this need and a lot of work is already being done on shared standards. Qualities like effective communication and the ability to work in a multistakeholder environment will be important in these efforts. The US Department of Commerce's NTIA has also started a multistakeholder process focusing on the upgradeability and security of devices and believes that the private sector should lead the way in terms of standards. Some actors, particularly some governments, hold a different view, preferring to pre-define technical standards in their countries to achieve certain outcomes. Some participants argued that this tendency to regulate should be resisted, as it is impossible to know how the market will play out, and countries with the heaviest approach to regulation are often those with the most potential for explosive IoT growth, as their industries are already mobile-based. Policymakers should be encouraged to first explain their goals, as industry may be able to address those goals without the need for regulation.
Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)	While established companies could suffer greatly from selling unsecure IoT devices, fear may not be an adequate motivator. This can't be left entirely up to the market, as there are commercial pressures to release products in a timely fashion that conflict with the need to ensure adequate safety measures are built in. There is also an inadequate understanding of cause and effect among consumers. Aside from personal security and privacy concerns, there is the issue of devices being used to attack the Internet itself. It was noted that the M3AAWG is working on a series of recommendations for IoT developers to help them make their devices more secure. The IETF is working on something similar. There was a suggestion that identifiers could be used to create a "trust zone" for IoT devices. However, requiring permission for devices to connect to the Internet is a drastic departure from the current approach and not likely to be supported. A framework allowing "consent in advance" could potentially be used to tell devices what to do without having to be manually configured and updated. It was noted that the EU is working on a trusted IoT label. In terms of a practical IoT implementation, one IoT network developer noted that they had run into a lot of challenges in the technical and standardisation realm. There was also a lack of blueprints or implementation plans they could use. A "wait and see" approach is not an option for governments. While manufacturers can learn from failure, in the case of a local government implementation, failure means creating legacy systems that would last a decade or more.