



# GSMA response to NTIA's green paper "Fostering the advancement of the Internet of things"

March, 13<sup>th</sup> 2017

London

To:

**The National Telecommunications and Information Administration**

**U.S. Department of Commerce**

The GSMA welcomes the opportunity that the Department of Commerce (DOC) has provided to further comment on its green paper "*Fostering the Advancement of the Internet of Things.*"

The GSMA believes that IoT offers unrivalled opportunities for economic productivity and innovation. The positive impacts of IoT on citizens, consumers, businesses, and governments will include improving individual health and well-being, helping governments reduce healthcare and other costs, improving consumers' quality of life, reducing carbon footprints, increasing access to education and other public services, improving transportation safety, and energy efficiency.

The GSMA made five key recommendations in its previous submission: *First*, avoid extending legacy regulation to IoT, as IoT is fundamentally different from traditional telecommunication and policy making should recognise these differences. *Second*, encourage the development of industry-led interoperable standards without hindering innovation, policy frameworks should be technology- and service-neutral and treat equivalent services similarly. *Third*, promote the use of globally harmonized spectrum bands; widely harmonised bands help drive volumes for low cost IoT. *Fourth*, build trust into IoT devices, existing privacy and security rules and industry self-regulation will provide sufficient protection for consumers and developers. *Fifth*, engage on a bilateral and multilateral basis to ensure that international IoT activities equally promote competition and innovation. Given the low revenues and margins that characterize many IoT products and services, it is vital that IoT companies are able to sell globally without having to reengineer or customize them for particular national markets.

The GSMA is pleased to see that throughout the paper a main DOC priority transpires. This is to prioritize an IoT environment led by private sector initiative, based on technology – neutral standards, where policy making at local, national, and international levels is driven by a consensus-based, multistakeholder approach.

In addition to the above, the GSMA believes that it is of primary importance for the mobile industry to ensure that policy and regulatory institutions understand the intrinsic cross- market/ cross department nature of IoT. The global dimensions of this opportunity require continued international engagement to promote interoperable frameworks and industry-led standards.

Avoiding duplication and fragmentation is a key fundamental step to promote innovation and maximise the benefits that IoT can generate. The GSMA is pleased to see that as next steps, the DOC proposes to "*proactively engage and collaborate with other relevant agencies on IoT*" and "*coordinate the private sector as well as federal, state, and local government partners*" to minimize this risk. The GSMA supports these initiatives and believes that DOC is ideally suited to lead and promote a cross-agency working group aimed at avoiding conflicting mandates, streamline government involvement, promote and industry-led approach to IoT and minimize regulation.

GSMA would also like to inform the Department of two important developments since last filing in July. These relate to the two key areas of security and privacy:

### IoT security Self-Assessment scheme

In Q4, 2016 the GSMA launched an IoT Security Self-Assessment scheme<sup>1</sup> that enables IoT companies to demonstrate that their products are aligned with the GSMA IoT Security Guidelines<sup>2</sup> – a set of best practices developed by the telecommunications industry to share their security expertise and enable the creation of trusted, reliable, and scalable IoT services.

By completing a self-assessment, IoT companies can demonstrate the security measures they have taken to protect their products and services from cybersecurity risk, enhancing their reputation as trusted IoT service providers.

In Q1, 2017 GSMA published a case study<sup>3</sup> outlining how the *Port Authority of Seville and Telefónica used the GSMA IoT Security Self-Assessment* to test the security of their 'Techport 2025' project to ensure that this new project, designed to improve the efficiency of this important logistics hub in south west Spain, complied with GSMA IoT Security Guidelines.

### Cross-border data transfer

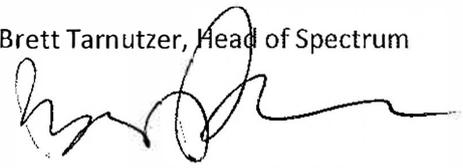
In February 2017, GSMA published a position on cross-border data transfers that underscores the importance of the global free flow of data to innovation, competition, and economic and social development. GSMA is of the view that governments can facilitate cross-border data flows in a way that is consistent with consumer privacy and local laws by supporting industry best practices and frameworks for the movement of data and working to make these frameworks interoperable, and backed by strong accountability mechanisms. The global free flow of data will be critical to the success of the IoT.

In our position, GSMA also maintained that governments should only impose measures that restrict cross-border data flows if they are absolutely necessary to achieve a legitimate public policy objective. The application of these measures should be proportionate and not be arbitrary or discriminatory against foreign suppliers or services. The imposition of data localization requirements can undermine global data flows and impede the implementation of globally interoperable privacy frameworks. Additionally, data localisation measures “could also inhibit data-driven businesses, in particular start-ups and SMEs.”<sup>4</sup> Such measures should be avoided to support the growing IoT market.

Respectfully submitted

**GSM Association**

Brett Tarnutzer, Head of Spectrum



---

<sup>1</sup> GSMA IoT Security Self-Assessment, [www.gsma.com/connectedliving/iot-security-self-assessment/](http://www.gsma.com/connectedliving/iot-security-self-assessment/)

<sup>2</sup> GSMA IoT Security Guidelines, [www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/](http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/)

<sup>3</sup> GSMA Case Study “Securing the Port of the Future”, [www.gsma.com/connectedliving/securing-port-future/](http://www.gsma.com/connectedliving/securing-port-future/)

<sup>4</sup> European Commission, [Building a European Data Economy Communication](#), p7

