The following response has been prepared based on the experiences of IOT (Internet of Things) from the following perspectives

NquiringMinds Ltd: who develop and deploy a commercial IOT platform

And NquiringMinds, who has been an active participant in the following IOT projects

- Webinos Foundation: and opens source/open standards organisation dealing with IOT interworking
- PicoSec: a research project dealing with IOT security

These comments may be publically attributed to NquiringMinds Ltd.

The following brief summary points relate to the issues raised in the consultation document

Spectrum

From our deployment experience the vast majority of real world IOT deployments involves local radio technologies (sub 100m) backhauled over fixed line connection

There are clear physical and economic reasons why this is the case

a) Device license cost: price often a critical consideration of an IOT deployment. Ignoring physical costs, the IPR licensing costs of the modem device increases rapidly as we move up the spectrum. ISM band at or close to zero. LTE close to $40.
b) Network subscription cost: licensed bands typically require an ongoing subscription cost, which impacts the total cost of the IOT service
c) Power consumption: the real costs of an IOT deployment is often the manpower cost to change batteries. We should be targeting IOT devices that need battery changes > 1 year. This is only really possible with near range networking technologies

Recommendation: IOT deployments will use heterogeneous networks. For this reason the critical features that need to be present:

- Addressing
- Discovery
- Interworking
- Security/privacy

MUST be provided at a virtual/application protocol level, and not presupposed at the networking level

Addressing

To address IOT devices we should consider the following

NonIP

There is often no I in IOT. Most real world deployments we have been involved in use physical bearers that do not support IP. For example

- ISM band 434/868 MHz devices predominate. IP is not supported
- 802.15.4 protocols does not natively support IP
- Weightless does not natively support IP

Where IP is added to these protocols, it introduces a significant performance impact

Roaming
Many IOT devices physically can roam onto different networks, implying that a different physical address will be provided.

Take the example of an accelerometer, a GPS or pressure sensor all of which sit on a mobile phone.

The physical address of this device will change depending on whether
- Phone is on GSM network
- Phone is on work wifi
- Phone is on home wifi
- Phone is connected over a local network – eg Bluetooth

An application needs to be able to connect to this sensor using an address that persists over different networks

The security/ (access control) needs to be managed in a way that persists over network connection

Web Interoperability

If the growth aspirations for IOT are to be achieved, IOT must interwork with web applications.
Web applications solve the IP roaming problem by the use of URLs, universal resource locations

URLs are recommended as a well understood well proven IOT address that fulfils all the requirements anticipated.

Compliance program

Many of the deep issues surrounding IOT deployment cannot be dealt with at pure technology or protocol level.

We believe a well-structured compliance program, with a consumer visible "kite-mark" that gives certain assurances to end users will be essential for IOT growth

At a minimum we believe the following will be essential elements to such a program

Interoperability
A purchased IOT device must come with certain interoperability assurances. We need to know a purchased device will interwork with other devices, applications and services
Without these assurances either
a) No IOT ecosystem growth with be possible
b) OR any ecosystems will be controlled by a few monopolistic suppliers

Security
An IOT device must come with certain basic security assurances, for cases where they are storing or transmitting private or sensitive data. These need not be complex, but are essential. Such as

a) Encrypted transmit: a device must not transmit sensitive data in unencrypted form (list of approved encryptions)
b) Encrypted Storage: a device must not store sensitive data on device in an unencrypted form
c) Tamper proofing: the device must be resistant to basic physical tampering

Transparency

The issue of IOT generated data, who has access to it, how long for, what can they do with it, who can they share it with, and most complex of all who can they share derived data with, is an incredibly complex problem.
Technical and/or legal solutions to this issue get complicated very quickly.

We believe a very simple, and tractable solution, that at least lays the foundation for a solution here, is based on mandatory transparency.

Simply put any entity consuming data which originated from another entity (typically an company/organisation consuming end user data) must declare the entirety of data it has access to

This requirement could be fulfilled by a very simple web based API, where this API returns raw data.
Simple consumer transparency applications can be built upon this

Identities of consumers and organisations, can be managed peer to peer through certificates (see below: peer to peer)

This places a burden of responsibility on a consuming organisation to know where the data came from and what it is being used for.

This burden however is simple best practice, data management.

This requirement simply puts and operational requirement for the organisation to be able to disclose this to the originating party

Control
The logical follow on from this requirement is the ability for the owner of the originating data to request data is deleted.

This fully empowers a consumer in their relationship with data

It is in sense a logical extension to the "right to forget" and we believe essential for responsible IOT growth

UK Initiatives

If the UK is going to be proactive in this area, the following should be considered

- UK parochialism: IOT is an international market. IOT device vendors are in reality predominantly non UK. Any initiative to be effective must be internationally palatable. This means firstly, interacting where possible with exiting international initiatives and secondly where action is taken proactively it is branded sensitively (e.g. "British" standards institute work is not going to go down well in the international community)
- Security: security is pre-eminent. Dealing with this issue upfront is essential, it cannot be left out of scope
- Core communications: basic, non bearer specific interworking is essential to do first. Some existing work has started in directory and discovery – but this is like inventing the telephone book before the telephone. The basics of interworking on heterogeneous physical networks is essential

Licensing

If IOT is to echo the success of the web, it must follow its basic ethos. Fundamentally this relates to licensing of IPR.

We strongly recommend that any technologies explicitly or supported by UK initiatives are unambiguously royalty free in nature
E.g. http://www.w3.org/Consortium/Patent-Policy-20040205/
Without this essential IPR will be simply be acquired by financial muscle. So that even if core IPR originates with a small UK player, it will rapidly be acquired by an international player essentially bestowing monopolistic control to non UK players.

Openness

> *Degree of openness: IoT services could be deployed over entirely open networks, i.e. any manufacturer's device conforming to a particular technical standard can be connected; or over a closed network, in which the operator controls which devices can access the network. We are interested in views on which of these (or similar) approaches might develop, whether particular services are suited to an approach and what the implications might be for the development of the IoT. We are also interested in views on the role of open versus proprietary standards.*

A minor point to the above quote: openness of technology specifications and openness of a specific IOT ecosystem are two entirely separate things. The first we believe to be mandatory; the second is a case be case issue for each deployment driven by commercial imperatives