Speaking points made by Robert MacDougall, Vodafone, during the IoT liability workshop as part of the 'Digital Revolution' event at the University of Münster, 2 October 2015[1]

Good afternoon everyone and many thanks to both the University of Münster and the European Commission for the opportunity to join this panel. In advance of the panel, we have been asked to consider problems stemming from either an *unclear* liability regime or the *non-existence* of a clear cut liability regime in this area. We have also been asked to consider whether this affects in any way the offer of IoT services/goods of suppliers or the confidence of users (consumers, business users) in IoT and/or data driven services and connected tangible goods.

With this in mind, I would first like to provide some introductory context to set out Vodafone's observations on the IoT market. Each year we publish our M2M Barometer to track market development and establish how businesses are adopting this technology. We do this through interviews with over 650 executives, in conjunction with Circle Research and Analysys Mason, publishing the final report on our website. As part of this research, we ask companies what they perceive to be the main barriers to IoT adoption, and liability has not, to date, been identified. Security and privacy are seen as the most common concerns – not a barrier to adoption per se – but a barrier to increasing use. In our 2015 M2M Barometer, 33% of businesses interviewed said that security is a barrier to them increasing their use of M2M. But there were important distinctions between sectors. Retail and health ranked highest for security and privacy concerns: 41% of healthcare organisations agreed "strongly" that security breaches are a major concern, compared to 36% across all sectors. Conversely, sectors like transportation ranked lower — just 23% of transportation and logistics companies agree strongly that security breaches are a major concern. This is probably because businesses in these sectors hold less personal data.

But that is not to say we do not take issues around liability seriously – we do. But our view is that we should be able to manage it contractually and via innovative, industry led initiatives. This is something I will elaborate on in relation to the other questions that have been posed by Professor Staudenmayer.

[1] I am grateful to Rod Freeman and Valerie Kenyon at Hogan Lovells for their invaluable contribution to these speaking points

1. Do suppliers and users find the legal framework balanced and clear?

The obvious frame of reference for product liability considerations in Europe is the Product Liability Directive.[2] At a high-level, the Directive establishes the principle that the "producer" of a "product" is liable for damages caused by a "defect" in his product. The Directive was notified to the Member States of the EU (who then needed to bring into force national laws and provisions to implement the Directive) in 1985. The result of a long period of negotiation and consideration, the Directive's drafting involved a careful balancing of the various interests in order to produce a workable and appropriate liability regime for products in Europe.

At a broader policy level, the question does arise as to whether it is appropriate to extend this "no fault" liability regime to technologies that are more in the nature of a service than a product. An obvious consideration is whether certain IoT technologies are "products" within the meaning of the Product Liability Directive. Some clarification may be needed over time in that regard. There are also a number of other questions that could arise in relation to certain IoT applications. In particular:

- who is responsible for safety compliance of an IoT product on an on-going basis?
- Who will be liable in the event that an IoT product causes damage?
- What will that person be liable for?
- How should their liability be assessed?
- How should the risks be insured?

So, in answer to the question raised, there are potentially areas of ambiguity in relation to the existing regime and its application to IoT products. However, many of these risks are not unique to IoT; for example, these risks exist in established technology industries. As an example, the development of after-market third party components for a product – where that component may have a fundamental impact on the use and safety of the original product – raises considerations similar to those raised about the application of the existing product liability regime to IoT products and systems. For many reasons, careful consideration and dialogue should take place before making amendments to the existing regulatory regime specifically with IoT in mind.

---

[2] Directive 85/374/EEC

2. **In any legal or voluntary framework or guidelines that cover liability issues of IoT, are there problems or gaps touching the aspects of liability in relation to such services and tangible products (e.g connected cars etc.)?**

This question focuses on the role of legal or voluntary frameworks or guidelines in the context of IoT.

As a starting point, it's crucial to keep in mind the important role that certain existing standards have to play, for example the activity that the European Commission is sponsoring to develop a common methodology for applying Privacy by Design (Mandate 530) which will be of equal relevance to IoT, as well as existing ISO standards such as ISO/IEC 27018 and ISO/IEC 27034. These technical standardisation initiatives and methodologies have an important role to play in relation to potential liability issues associated with IoT.

The question is right to highlight the important role of guidelines in this area. Within the mobile industry, the GSMA has a key part to play in developing guidelines to embed best practice. Although we don't yet have GSMA IoT liability guidelines, which perhaps reflects the fact that liability is still something of an emerging issue, there are plenty of other guidelines which are relevant and which highlight why there is no reason why industry cannot develop liability guidelines as required.

I would highlight the work the GSMA is doing in relation to IoT security to demonstrate this, as in practice I think that issues of IoT liability and IoT security will be related. The GSMA's IoT security guidelines are industry agnostic. They highlight the role of the IoT Service Provider – and make recommendations about how the IoT service provider can mitigate risks by selecting partners competent in security and by supporting standards-based approaches. They also introduce a set of 'best practice' security and privacy principles, guidance for IoT devices (e.g. secure local interfaces), network operators (e.g. subscription management), and platforms (e.g. cloud security configuration). All of this will help drive best practice and reduce risk associated with IoT applications.

3. **When it comes to liability issues of these services and connected tangible products (e.g. connected car etc.) is the existing framework fit for purpose, in particular is the legal framework future proof?**

With respect to whether the existing regime is fit for purpose, there are some important features of IoT to keep in mind – and I'll discuss these in a moment. But it's also important to recognise the inherent challenges of seeking to "future-ready" any legal framework. To a large extent, the existing legal framework may be able to cover many of the issues relevant to IoT – but where it can't, careful consideration in advance of any regulatory development is crucial to avoid a "knee-jerk" reaction that could unnecessarily slow-down the pace of beneficial change and innovation. At this stage, we haven't fully explored all the potential advantages and applications of IoT products and systems.

The rapid development of IoT technology raises a number of product compliance, product liability and insurance-related issues. Whilst aspects of the IoT give rise to special considerations in these areas, the compliance and liability issues do not give rise to a clear need for new legislation or new types of regulation. As a result of this, and as I have already set out, we should first look to manage those issues within the structure of existing legislation and regulatory regimes.

Interdependency is also a key consideration. Increasingly, the development of IoT technologies creates complex interdependencies between product and service producers. Products are designed so that they are dependent on third party technologies in order for the product to perform its basic functions, and in order to maximise the benefit of the product for the user. Those dependencies can increase and become more complex over the life of the product.

This gives rise to questions of who is responsible for certifying safety of the product, who is responsible for ensuring safety on an ongoing basis, and how liabilities should be allocated in the event that the technology behaves in an unsafe way causing damage. These issues can also give rise to challenges in identifying the root cause of product failures, and in determining where fault lies in the event of a problem. Issues relating to liability when products involve third party components are not new but are highlighted when products are increasingly connected and complex.

But I do not consider that new, detailed IoT/M2M legislation is the answer. The question highlights 'connected cars' in particular and I think we can take note of developments in the USA on this point. On July 21, 2015, new legislation was proposed directing the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to promulgate federal regulations setting minimum cybersecurity and privacy standards for all motor vehicles manufactured for sale in the United States, the so-called Security and Privacy in Your Car Act, abbreviated as the 'SPY Car Act'.

The SPY Car Act imposes new regulatory requirements and potential liability. It has also been suggested that the SPY Car Act might overlook existing automotive safety requirements enforced by regulation and common law and gives regulators nearly unlimited power. The SPY Car Act also uses terms that leave the NHTSA and FTC with very significant power to define what constitutes "reasonable measures" and "best practices" to protect against hacking and to define what will be considered a "violation" of the statute. It has also been suggested that it does not consider existing industry initiatives to address both privacy and security concerns. Existing provisions of the FTC Act have already been relied on in relation to enforcement activity in the area of IoT and are effective at providing privacy protections to consumers. Indeed, the automotive industry in the United States has already adopted privacy principles for connected cars – binding as public commitments enforceable under the FTC Act.

We should also not lose sight of the fact that liability provisions exist in the existing EU regulatory framework which govern the provision of electronic communications services and the operation of electronic communications networks in the EU. The Framework Directive requires Members States to ensure that the integrity and security of public communications are maintained. Article 4 of Directive on Privacy and Electronic Communications (the 'ePrivacy Directive') also contains specific provisions that could be relevant to liability, for example that subscribers and users of such services be fully informed by their service provider of any existing security risks which lie outside the scope of possible remedies by the service provider. Therefore, we should seek to apply existing regulation to these new and emerging areas before we seek to introduce new law and regulation designed to address specific IoT liability concerns.

4. **If not, what, in the view of the participants, should be the liability regime for these services and connected tangible goods?**

Interaction with the Insurance industry will be vital to the liability regime for IoT, as the insurance industry will need to be ready to offer insurance products which respond to the relevant risks run in a cost effective way. Where the scale and complexity of potential liabilities is too great to be managed at corporate level through conventional liability insurance it may be necessary to develop arrangements for certain IoT products whereby there is a "pooling" of risk. At its simplest, this could be an arrangement whereby all the participants in the development of a particular technology pay in to an insurance scheme designed to meet the cost of claims arising from the operation of that technology. This is a system which already operates successfully in the context of certain risk events in certain jurisdictions. Such schemes are often statutory in nature.

But let's not forget about the benefits of IoT, it's not all about risk. For some IoT products, technology can enable and empower consumers so that insurers are able to calculate risk more effectively. Adoption of new technology will lead to risk pools becoming smaller, according to research published earlier this year by Morgan Stanley together with the Boston Consulting Group. This research predicted that damage to insured homes may fall by 40-60% if smart-home devices are adopted. The risk pools for home and car insurance might shrink by up to $102 billion, the report considers.

Legislators may also need to consider existing requirements in relation to insurance to ensure they are meaningful in the light of developments in IoT technology. An example is that of compulsory motor insurance covering individual users of vehicles. It will be necessary to determine whether this model will be appropriate in an age where a fully autonomous vehicle is not operated by an individual user but by a remote operating system.

5. **Do participants think the European Union should have a role when it comes to liability issues of these services and connected tangible goods?**

The role of the European Commission is especially important given the relevance of IoT to the creation a Digital Single Market. A harmonised approach is also vital to maximise the success of the global product market (including in terms of market access for the industry, and supporting innovation in the context of the ease of

product compliance and launch), and to maintain high and consistent standards of safety for consumers regardless of their home address.

With regards to product regulation and the importance of a harmonised approach, one factor that becomes increasingly relevant is that consumers are becoming more sophisticated in their approach to sourcing products. Purchasing products from a market other than the one closest to home is now the norm, and consumers can circumvent hurdles that sellers put in place to prevent the use of products/software in non-intended countries with relative ease. For this reason, a harmonised approach to product regulation and product liability is key. That said, this issue is not restricted to the IoT. It is important that the the Commission pushes for a harmonised soft-law approach.

In this respect I would highlight the role of the Alliance for Internet of Things Innovation (AIOTI), an initiative that has recently been set up by the European Commission. The Policy Working Group of the AIOTI, which I Chair, consists of over 200 companies, active across many sectors of the economy. We are making a number of policy recommendations to address barriers that could prevent the take-up of the IoT in the context of the Digital Single Market, with a particular focus on privacy, security and liability. This highlights the role that the European Commission is already playing here to help develop an approach that is relevant to both the demand and supply sides of the economy, which is, after all, one of the key considerations associated with IoT.

Ends