Vodafone's response to the European Commission consultation "Building a European Data Economy"[1]

26 April 2017

[1] Vodafone welcomes comments or questions on the views expressed in this document. They should be directed to Markus Reinisch at Markus.Reinisch@vodafone.com

Introduction

Vodafone has many years' experience of providing electronic communications services and operating electronic communications networks in the EU. We have innovated through the development of an Internet of Things (IoT) platform, which connects many millions of IoT devices in Europe, across multiple industries. We also have an mAnalytics capability as well as a fast growing Cloud and Hosting Services business. Vodafone is therefore actively involved in building the European data economy.

In this response we set out our views on the topics that have been raised by the Commission in its Communication and accompanying consultation.[2] For the purposes of our response, we adopt the definition of 'Machine Generated data' as outlined by the Commission in its Communication, i.e. data that is created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real[3]. In summary, our responses to the four key areas highlighted by the Commission in its consultation are as follows:

- we fully support the Commission's proposed next steps to implement the principle of the free movement of data across the EU, as outlined in its Communication;
- in relation to access to machine generated data, we would support an approach whereby the Commission issues guidance on incentivising businesses to share machine generated data, highlighting specific sectoral cases where possible, and also the parameters for who can use the data and for what purposes;
- we do not see any need for the development of specific liability regime to address potential challenges associated with IoT devices, and
- we do not see a requirement to develop a data portability right with respect to 'non-personal, machine generated data'. Rather, data portability as well as the interoperability of systems should be encouraged by the promotion of industry-led standards, guidelines and best practices.

[2] This response supplements Vodafone's response to the Commission's questionnaire on the same topic.
[3] Section 3.1 of the Commission's Communication

1. Data Localisation

Vodafone very much supports the Commission's policy to address any undue barriers to the free movement of machine generated data across the EU. This is a concern that may manifest itself in a number of different ways, ranging from specific sector-specific requirements (such as those that we have observed apply to customers in the utilities or financial services sector) to a perception that data is more 'secure' if held within the boundaries of a specific geographic region.

There can be a number of negative socio-economic impacts associated with data localisation rules, including:

- increased costs to service providers and customers resulting from the additional capex and operating costs (exacerbated by loss of economies of scale) associated with developing in-country data centres and platforms where multi-jurisdiction architecture was previously in place;
- reduced economic contributions of service providers linked to lost revenues from the range of products and services that they may no longer be able to provide if local architecture is required;
- reduced economic contributions from enterprises if data localisation rules (or the costs associated with complying with these rules) remove the commercial viability of their digitised products within the market;
- reduced range of services available to customers, preventing them from realising the benefits associated with their use, (e.g. cost savings associated with expense management solutions and SIM monitoring and management through an IoT platform); and
- increased complexity and cost to industry due to the lack of consistency across jurisdictions, which hampers moves towards greater digitisation.[4]

Localisation measures may also have a specific negative impact on IoT, given IoT devices are likely in many cases to cross borders. In our experience, our European enterprise customers that are integrating IoT into their operations in both B2B and B2B2C capacities very much value the benefits of a harmonised solution for IoT. This enables them to achieve efficiency benefits of being able to deal with a single

[4] For further analysis of the potential socio-economic impact of data localisation requirements see the KPMG report (in conjunction with Hogan Lovells) 'Securing the benefits of Industry Digitisation' produced for Vodafone, which is available at https://www.vodafone.com/content/dam/vodafone-images/public-policy/policy-papers-and-news/Vodafone-Industry-Digitalisation-Report-051115.pdf

provider to meet their needs across multiple EU countries and the associated time and cost savings in particular. A purely national approach would undoubtedly lead to fragmentation.

In summary, we would support a legislative instrument to ensure the free movement of data across the EU. If that is not possible, we would also support the Commission's proposed next steps to implement the principle of the free movement of data, as outlined in its Communication.

2. Access to and re-use of non-personal machine generated data

Vodafone is actively involved in ensuring that European companies are able to generate, analyse and utilise valuable data associated with their operations, by connecting them to our IoT platform. If IoT is defined by anything, it is defined by the breadth of applications it can support, and we have published numerous case studies that illustrate the benefits of this capability, for example;

- the generation of real-time anonymous traffic data from navigation devices with detailed updates every 3 minutes[5] ;
- non-invasive, tail mounted sensors on cows which gather over 600 pieces of data a second and which inform farmers of impending labour[6], and
- device diagnostics and data from robotic exoskeletons to help improve the mobility of stroke and spinal cord injury patients[7].

We are also actively involved in identifying how to maximise the value associated with the data generated by our own operations. One example is our mAnalytics programme which has analysed anonymised aggregated traffic information along a major transport route. This can improve transport planning and provide broader societal benefits, by understanding movement patterns along transport routes and in areas where people congregate.[8]

---

[5] See 'Vodafone and Tom Tom take the Jam out of traffic' at http://www.vodafone.com/business/global-enterprise/case-study/tomtom

[6] See 'Moocall – connecting cows to save the lives of calves and improve farm profitability' at http://www.vodafone.com/business/iot/case-study/moocall

[7] See 'EKSO BIONICS ROBOTIC EXOSKELETONS GAIN GLOBAL CONNECTIVITY WITH VODAFONE IOT TECHNOLOGY' at http://www.vodafone.com/business/iot/ekso-bionics-robotic-exoskeletons-gain-global-connectivity-with-vodafone-iot-technology-2016-06-07

[8] For more information, please see "Vodafone Analytics: Using network data to help society" at https://www.youtube.com/watch?v=fj353Sj8zdI

We also make available APIs to our IoT platform to ensure that our customers are able to innovate themselves using our connectivity and therefore grow the overall ecosystem. Our platform is therefore by no means 'closed'; there is also an active installed base of resellers leveraging this IoT functionality.

Existing contractual and legal frameworks relevant to 'data ownership'

Our experience in relation to data access is that there is not yet a problem that needs to be solved, per se. As set out above, our technology enables our customers to innovate and generate data. We typically agree contractually with our business customers (whether multinational, corporate or SME) who has access to data in given situations. The contract can specify who acquires the rights to the data generated as part of this process.

Rights are also acquired consistent with existing legal frameworks. Personal and other types of data are subject to well-established existing legal frameworks tailored for specific needs, e.g. copyrights, database rights, notice and take down as well as data protection laws.

Principles that we believe should guide the Commission as it develops its policy in this area

We understand that the European Commission is concerned that a lack of regulated access to machine generated non-personal data may impede market growth. In considering this topic, we consider that four guiding principles are relevant.

Maintain the incentives for industry to generate machine data in the first place

First, Vodafone believes it is vitally important to maintain the appropriate incentives for industry to generate the data in the first place. Data is arguably the most valuable asset in the digital economy and its use should be encouraged for economic and social benefits. The digitisation of industry is creating many new opportunities for data to be created and used in ways that promote European economic growth. Industry must have the right incentives to create these new applications that generate this data. It is essential to ensure that we have an efficient framework for interoperability and IPR that adequately compensates those market players that are investing in innovation and contributing key technology.

With this principle in mind, we see a concerning, emerging trend of national statistics agencies across the EU seeking to access operator data in bulk, in raw and free of

charge. Provision of these huge data assets to national statistics agencies would create new security vulnerabilities (such as new unnecessary copies of data in environments that we know very little of). Furthermore, even law enforcement bodies do not typically have access to bulk data, so we do not see why it should be any different for statistics authorities. We would be prepared to discuss the provision of appropriate analytics data to the public sector, as a service, ensuring that we retain the value of our data asset and appropriate safeguards can be built in. But operators should not be obliged to provide data for undisclosed 'public interest' reasons.

There should be a presumption in favour of existing horizontal law and regulation

Second, in such a new and fast-moving, fluid market, transcending many different industry sectors, ex-ante regulated access to data 'across the board' could have a damaging or chilling effect. Regulatory focus should remain on ensuring that we extract maximum value for access to public sector data, consistent with the European Commission's existing priorities in this area. There should be a presumption in favour of relying on existing horizontal legal frameworks (in particular competition and consumer protection law) to address any issues that arise. As the Commission notes in its Staff Working Document, cases such as MAGILL[9] demonstrate the effectiveness of such a remedy (in this case, opening up a new market for access to TV listings data).

Any regulatory intervention should be consistent with the principles of economic regulation and should be on a market by market basis

Third, any ex-ante regulatory Intervention should be premised on a market power analysis where there is a clear competition and consumer protection rationale for intervention in a market, consistent with established regulatory practice.

We need only look at the ongoing debate on "Access to in-vehicle data and resources" as an example of the complexities associated with such potential intervention. Even within this sector-specific environment, the ITS report (published in January 2016 by DG Move[10]) recommended "*a scenario-based analysis on legal,*

[9] RTE and ITV v Commission ('Magill'), Case C-241/91 P and C-242/91 P, [1995] ECR I-743.
[10] http://ec.europa.eu/transport/themes/its/c-its_en.htm

liability, technical and cost-benefits aspects is required to further progress and also to help answering legislators' request regarding an open-access platform".[11]

Furthermore, we note that the Commission has recently focused on the agricultural sector, in order to evaluate, amongst other things, the benefits for farmers of the most promising data governance models as well as to identify which constraints hamper their involvement in these models.[12]

Leverage existing industry best practices

Fourth, there are also a number of existing regulatory best-practices already underway regarding access to data. The ongoing work of organisations such as the GSMA (through its IoT Big Data activity which will make harmonised data sets from multiple sources available to developers and third parties through common APIs[13]), the AIOTI and ETSI (for example its newly established Context Information Group on Smart City interoperability) have roles to play in advancing market development related to 'private' machine data.

A potential way forward

Vodafone's own research (via its Annual IoT Barometer) supports a view that businesses are already sharing IoT data and that this will further emerge over time. Our most recent IoT Barometer, published in 2016[14], found that sharing data is problematic only for organisations new to IoT. We further found that selling, exchanging and sharing data can be valuable, and we expect it to become a greater focus area in the coming years — indeed, nearly a third of adopters are already engaged in using IoT to build ecosystems in this way.

To examine these issues, we asked if enterprises felt safe sharing their data with others. We found that there were striking differences between our whole base of respondents and those who already have live IoT projects, and specifically those that have reported "significant" ROI from their live projects, as set out in Figure 1 below:

[11] Specifically, the ITS report suggested the following 5 considerations were particularly relevant in assessing the rationale for regulatory intervention: (a) Data provision conditions: Consent, (b) Fair and undistorted competition. (c) Data privacy and data protection, (d) Tamper-proof access and liability. (e) Data economy.
[12] See for example https://ec.europa.eu/eip/agriculture/en/content/eip-agri-workshop-data-sharing
[13] See for example http://www.gsma.com/newsroom/press-release/gsma-launches-iot-big-data-directory-support-growth-innovative-new-iot-solutions/
[14] http://www.vodafone.com/business/iot/the-iot-barometer-2016

Figure 1: Organisations with live IoT projects are more comfortable sharing data.

The analyst commentary[15] accompanying this finding is also is also insightful, as it highlights the importance of agreeing rules or parameters for data sharing, as follows: "*In multi-tenant systems such as that envisaged in the IoT, everyone needs to agree on a certain set of parameters, for example about who can use the data and for what purposes. At first, data sharing will emerge within what we term 'subnets of things', i.e. common interest groups with a shared understanding and trust on how data can be used. The earliest of these to materialise have been based on smart cities data, where diverse data sets are made available to third parties to build applications. Our expectation is that the next emerging areas will be healthcare and supply chain*".

In summary, in relation to future Commission activity in respect of machine generated data, we would support an approach whereby the Commission issues guidance on incentivising businesses to share data, highlighting specific sectoral cases where possible, and also the parameters for who can use the data and for what purposes. If such an approach does not prove successful in addressing the Commission's policy objectives, then additional options, such as the development of standardised protocols for APIs, could be assessed. We would guard against the introduction of default contract rules or the introduction of a fair, reasonable and non-discriminatory access regime for machine generated data, as there is no evidence presented in the Commission's communication that such an interventionist approach is warranted.

[15] Machina Research

3. Liability

In its Communication, the Commission considers that a lack of clarity as to which party is responsible for the transmission of erroneous data by a sensor, due to software defects, connectivity problems or incorrect operation of a machine, could impede the emergence of a data economy.

Vodafone considers that the development of a new liability regime specifically with IoT in mind would not be the right approach. There is no evidence to date that a lack of clarity as to liability is holding back investment in IoT services or consumer take-up of IoT applications. We would also caution against grouping together IoT, autonomous systems and robotics for the purposes of a liability assessment – they can be very different, and we would advise the Commission to study each separately.

In relation to IoT, this is a topic that has been considered in some detail by the AIOTI, of which Vodafone if a founding member, and we would refer the Commission to this guidance for a more detailed treatment of the issues.[16]

In general, however, we believe there a number of considerations which mean that a new liability regulation, designed with IoT in mind, is not required.

The role of safety standards

First, there is an important role to be played by the development of existing globally aligned standards – these might be expected to contribute to, for example, issues around ensuring the reliability of communications between devices (already an established element of electronic communications standardisation) , and how that can be tested as between connected products.[17]

B2B contractual liability will have been addressed by the contracting parties

Second, the apportionment of liability B2B is almost certainly something that the relevant product manufacturers will have already considered. Depending on the

[16] See 'AIOTI –Alliance for Internet of Things Innovation: Policy Report, 15 October 2015' at http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11815 and AIOTI Digitisation of Industry Policy Recommendations at http://www.aioti.org/wp-content/uploads/2016/11/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf which both make a number of recommendations related to IoT Liability.

[17] See for example DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

factual circumstances (including how "open" the devices' communication systems are), contractual arrangements should deal with this type of liability risk. Vodafone's experience is that it is standard practice for the parties to IoT contracts to attribute liability in this way.

Enforcement of existing legal and regulatory frameworks have an important role to play

Third, in terms of B2C liability, the relevant court or enforcement authority would need to apply the current definitions and existing legal framework. In fact, a number of recent IoT enforcement cases show how regulators and consumer protection agencies have been well able to take action where required. For example:

- In 2016, the US Federal Trade Commission took action to address the liability of equipment manufacturers in relation to the IoT. One of the concerns the FTC had in this action related to a web application that included multiple vulnerabilities that would allow attackers to gain unauthorized access to consumers' files and router login credentials. The FTC addressed security issues that may arise in relation to connected devices and the IoT.[18]

- Recent complaint filings by members of the consumer association BEUC in Europe also highlight the important role that enforcement of existing consumer protection rules (for example the EU Unfair Contract Terms Directive and EU Data Protection Directive) have to play in relation to the attribution of liability for failure to implement satisfactory security or data protection measures for IoT products. [19]

The need for a sector by sector approach and the role of the insurance industry

Fourth, consistent with the approach to data access set out above, analysis of potential issues related to liability should be assessed on a market by market basis. In the UK for example, the Government has published the Vehicle Technology and Aviation Bill which sets out provisions related to automated vehicles, electric vehicles, vehicle testing. This legislative Bill also envisages that insurers will be liable for damage where an accident is caused by an automated vehicle when driving itself, the

[18] https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf
[19] http://www.beuc.eu/publications/consumer-organisations-across-eu-take-action-against-flawed-internet-connected-toys/html

vehicle is insured at the time of the accident, and an insured person or any other person suffers damage as a result of the accident.[20]

Therefore, in summary, Vodafone believes that the Commission should not develop new liability regulation specifically to cater for potential issues associated with IoT.

4. Portability of non-personal data, interoperability and standards

Vodafone does not consider that it would be suitable to develop rights to data portability with respect to non-personal, machine generated data. Mandating standard contract terms or introducing legal obligations requiring the service provider to implement the portability of a (consumer or business) customer's data risks stifling innovation and the adoption of technology, with questionable benefit to the customer.

Rather, data portability as well as the interoperability of systems should be encouraged by the promotion of industry-led standards. Discussions on portability standards should be supported in global standards bodies. Moreover, guidelines and best practices are helpful to advise cloud users before standards become available. As the Commission recognises in its Staff Working Document; "*It has been argued that for certain types of platforms, namely the online social networks, the effects of data portability on competition might not be as strong. For these types of actors, platform interoperability rather than data portability might be an alternative way to increase competition and level the playing field.*"[21]

Benefits of a portability right for 'non-personal, machine generated data' are unclear

Data portability has at its heart the objective to foster competition by preventing customer "lock-in" to a particular service. Data portability has also sometimes been suggested as a consumer protection measure. Outside of a direct consumer protection context, such issues are best addressed by competition law, rather than by a data portability right which may or may not achieve that objective depending on the service in scope. This is especially the case in a nascent market, which is still developing.

[20] https://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0143/cbill_2016-20170143_en_2.htm
[21] Commission Staff Working Document, page 48.

The potential for customer "lock-in" is only one type of competition issue where data is concerned. Introducing a data portability right is not the "magic bullet" to solve it alone - as the Commission recognises in its Staff Working Document when talking about switching platforms; "*Even when switching platforms would be possible for business users, it is not consistently true that they would be locked-in only/mainly because of restrictions on data portability.*"[22] In our view the issue of "lock-in" would be more appropriately addressed by competition law.

Where consumer protection is concerned, consumers already benefit from the Unfair Commercial Practices Directive 2005/29/EC which prohibits traders from imposing onerous or disproportionate non-contractual barriers when a consumer wishes to, for example, switch to another product or trader[23] – as the Commission recognises in its Staff Working Document[24]. Furthermore the proposed Digital Content Directive introduces a requirement on suppliers to provide consumers with the technical means to retrieve all content provided by the consumer and "*any other data*" produced or generated through the consumer's use of the digital content, when the consumer terminates their contract.[25] This is in addition to the portability right consumers benefit from with respect to their 'personal data' under the GDPR.

We also question whether introducing a data portability right as a 'business protection measure' is necessary on the basis that it is common practice for businesses to negotiate the ability to move their business information from a service provider in the service contract, before procuring the service. This is usually found in the 'post termination/exit' clause of the service contract. Furthermore, and as set out in the access to data section above, businesses are already starting to share IoT data.

Costs of a 'non-personal, machine generated' data portability obligation would be material

Our view is that the cost to business of building the technology and operational processes to support a data portability right for 'non-personal, machine generated data' would be material – and risks stifling innovation and the adoption of an emerging technology in doing so.

[22] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy dated 10 January 2017, page 48.
[23] Unfair Commercial Practices Directive 2005/29/EC, Article 9(d)
[24] Commission Staff Working Document, page 46.
[25] COM/2015/0634 final – Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, Articles 13(2)(c) and 16(4)(b).

Clarity of scope is vital

Data portability as a concept is one that we are beginning to see in a number of Commission consultations or legislative proposals presently. It was first introduced in the General Data Protection Regulation with respect to 'personal data' 'provided' to a controller. It has also been introduced in the proposed Digital Content Directive as a consumer right – this time with respect to 'content' and 'any other data' produced or generated through the consumer's use of the service. Finally, we see data portability proposed in respect of 'non-personal data' in this Data Economy Package.

If a common theme links these three separate proposals, it is that their precise scope remains unclear. The Commission acknowledges that with regard to the GDPR's portability right "*one point which needs interpretation concerns the precise scope of the provision.*"[26] Meanwhile the meaning of 'other data' has been criticised in the ongoing review of the Digital Content Directive as being ambiguous to the point of meaningless (in the digital domain 'data' is anything which exists above the hardware).[27]

It is important that any discussion about data portability in the context of the Data Economy Package is clear as to its scope and objective. While we can understand, in principle, the rationale for an appropriate, targeted, data portability requirement in a consumer context, the need for a machine generated data portability requirement is not at all obvious.

[26] Commission Staff Working Document, page 46. Since the Staff Working Document was published, the Article 29 Working Party has issued its final guidelines on the GDPR's portability right. These guidelines have introduced some clarity – but uncertainties remain owing to the fact that the guidelines adopt a wider interpretation of the portability right's scope than that in Article 20 of the GDPR.

[27] A related point is that curation of critical vs non-critical data sources may implicate how much interoperability is likely to exist in practice. We would contend that market forces in critical data verticals, not legislation, can best drive machine generated data interoperability.