CK Hutchison's comments on the roadmap for regulation of Artificial Intelligence

The Commission has published its roadmap on Artificial Intelligence (AI), listing the regulatory options available, from doing nothing, issuing guidelines and voluntary labelling, to mandatory regulation of some or all AI applications.

We agree with the need for a regulatory framework for AI. Having "trustworthy AI" will help with consumers' acceptance of AI. At the same time, a regulatory framework should also give developers and businesses the confidence to deploy AI in a stable legal and regulatory environment.

A new, comprehensive regulatory framework is required, similar to the Electronic Communications Code for telecoms or the GDPR for privacy, empowering national regulatory authorities with its detailed application, while ensuring a harmonised approach at the EU level to promote consistent development of AI.

Any framework for regulating AI should cover all applications and all aspects (including the regulation of risk and liability), rather than a subset, and should establish clear definitions of the different actors in the AI value chain.

Limiting regulation to a subset of AI aspects and applications, such as those that are high risk, would require an *ex ante* determination of risk and this would likely need constant revision to keep up with new applications. It is unclear what such an *ex ante* determination would entail: the identification of situations where employing AI is high risk requires exceptional competence and foresight on behalf of the designers, owners and operators of AI. The notion that humans need AI to provide better situational choices, and yet that humans must (from a regulatory perspective) be able to anticipate and guard against all and any prejudicial outcomes is difficult to envisage. It could result in many uses of AI being regulated in categories that are not appropriate to their risk. It must also be acknowledged that limiting regulation to a subset of AI applications would fail to provide a regulatory framework for other (non-high risk) AI applications, leaving them with the uncertainty of an unregulated environment.

We are concerned that the European Commission would have to frequently update AI regulation as the field of human expertise (for managing AI) develops, and market experiments mature. However, regulatory updates and amendments may become problematic, and humanly unscalable, when developments occur at the speed of machine learning. It is not clear that the very slow speed of human oversight, nor iterative regulatory structures, will always be capable of constraining AI appropriately due to the limitations of humanly foreseeable consequences.

We are also concerned by the Commission's list of obligations that would fall on high-risk AI applications. The proposed regulatory obligations, for example the rules on training data, record-keeping about datasets and algorithms, should be framed in a way that does not create unnecessary burdens that limit the options for deployment and use. Imposing too many obligations would impact the ability and incentives to deploy AI, undermining the business cases, with the result that the EU becomes an unattractive market to provide AI solutions.

In summary, we are not convinced that the Commission's approach of incremental AI regulation is practicable.

Instead, to provide certainty, we propose that any EU-wide regulatory framework should, as simply as possible, set out the rules and obligations for <u>all</u> aspects of AI. This includes having clear definitions of the various roles in the supply chain (e.g. developer, user) and identifying where the responsibilities

and any liabilities fall. A clear liability framework should therefore be part of the regulation. For telecoms businesses it is especially important that network operators are not held liable for AI applications they carry but in which they are otherwise not involved. This requires a provision similar to the exemption from liability for content carried over a telecoms network (the "mere conduit" provision).

The Commission should also recognise that AI will be a tool employed for criminal and state security ventures, and in such cases is beyond the scope of regulation. Examples include the criminal use of AI tools to disrupt network automation, to poison data, to construct deep-fake facial images to purchase a SIM and many other situations.

John Blakemore
Director of European Regulatory Affairs
Hutchison Europe

September 2020