Connectivity: The Edge

Published 28 October 2019

Tim Ryan is a Partner and Head of Technology at international law firm DAC Beachcroft. In a series of viewpoints on technological connectivity, he considers the impact of real time data analysis on information law, ahead of the ITech Law Conference in Dublin.

A new engagement and computing architecture

By 2025, the role and volume of data generated worldwide will have risen exponentially, with nearly a fifth marked as 'critical' to daily life, and nearly a tenth as 'hypercritical[i].' At the same time, the amount of data stored and analysed could rise from 1 percent today to 37 percent by 2025, implying up to $5 trillion in annual benefits[ii]. However, current infrastructures will be unable to deal with this volume of information in a timely manner.

Indeed, volumes alone suggests sending it all to the cloud will be uneconomic[iii]. By 2025 and as the impact of 5G is felt, nearly 30 percent of the data generated is forecast to be in real-time[iv] and over 50 percent of data could be managed autonomously[v].

What does it mean?

All time-sensitive data could therefore be processed in near real-time, at the edge of networks such as the IoT, with the bulk of non-critical data still sent to the cloud. Since the future of computing is at the edge, IT strategies and infrastructure must reflect that it will increasingly be embedded in IoT devices and in many cases outside of traditional organisational or IT boundaries.

While businesses' IT and data strategies are at stake, the broader shift is likely to impact consumer journeys, and redraw both business and operating models. Real-time consumer engagement – such as an insurance company offering a contextual time-limited micro-policy for your upcoming ski trip - is likely to boom. Many organisations will look to position themselves as advisors, build new services or even switch business models completely.

Collaboration and ecosystem partnerships will gain prominence as many organisations don't have the direct-to-consumer reach necessary to engage with the 100 billion or so IoT connected devices expected by 2030. Fundamental shifts in risk management are likely. Security and privacy controls will need to be built at the edge and intrinsically part of every device and network. By 2025, the average data generated per person, each year, is expected to reach almost 300 gigabytes. About 90 percent of this data is forecast to be vulnerable to unauthorised capture or theft and less than half of it is likely to be secured[vi].

The risk of retroactive judgement for misusing or mishandling data, allied to sheer volume, will likely create a need for regulated third party data markets. Common forms of dataflow will be necessary if partners are going to be able to work collaboratively and common third-party security standards will be required. Those leading the edge could transform industries but care must be taken that it does not become the bleeding edge.

[i] Source: IT Pro, 2018

[ii] Source: Forbes, 2018

[iii] Source: FT, retrieved 2019

[iv] Source: ZDNet, 2018

[v] Source: Oracle, 2019

[vi] Source: strategy+business, 2019

Authors

Tim Ryan
London - Walbrook
+44(0)20 7894 6978
tryan@dacbeachcroft.com

DAC BEACHCROFT