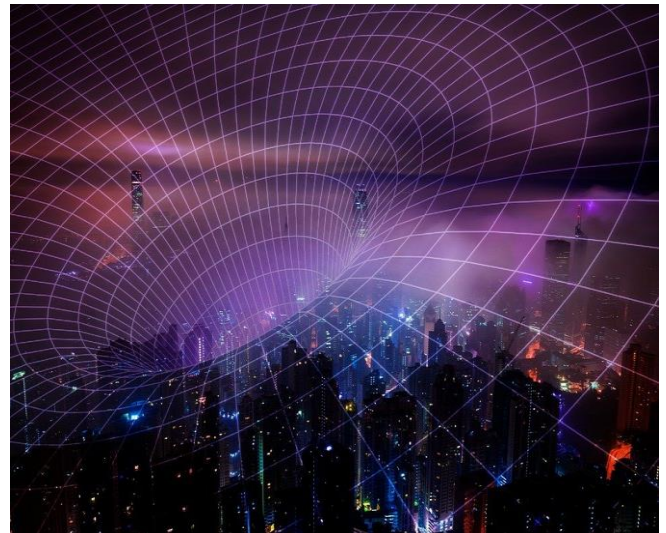


Data haven: a Sealand of hope and glory?

8th January 2021

Tax havens, offshore havens and low-regulation havens are all well established in the world of international business, even if they are not universally liked. With the looming final advent of Brexit on December 31, however, the UK could be about to adopt a fourth variant of the term: a data haven. While governmental defenders would likely scoff at any comparison between the UK and nations such as Russia and China, the possibility is stark and the description apt. Who would have thought that ‘taking back control’ could possibly mean giving more of it up?



A citizen's right to their private data, and moreover to know who has that data and how it is collected/used, has only increased in importance with the deepening hold of technology into every aspect of our lives. Data havens essentially thumb the nose at these sorts of concerns and hold data without concern for how it was acquired, or even what it would be used for (everything from being sold to repressive regimes to being exploited by the very nation that holds it). The Cambridge Analytica scandal brought the issue of mass collection and unclear use of personal data into public consciousness for perhaps the first time, but in truth it was a pervasive problem for as long as social media and Internet giants have collected every scrap of information that they can, with 'tailored ads' being only the tip of the iceberg in terms of one's data profiling.

Some data havens would propose themselves as bastions of free speech and the idea that 'the Internet is for all', by acting as receptacles for politically/socially controversial material or by offering platforms (such as the Tor onion browser) for people to conduct activity without being overly monitored. The most famous example would be the haven set up on Sealand, a supposed 'sovereign principality' in a North Sea WW2 fort which claimed that intellectual property laws did not apply to any data hosted within its servers, and that virtually anything except child pornography was fair game. But as 'harmless' as these types of venture may seem (and HavenCo mysteriously disappeared in 2008, never to return), the modern-day form of a data haven is far more authoritarian and insidious: even as its proponents, everyone from Mark Zuckerberg ("People want to be tracked for ads... [and] Facebook does not collect more information than it needs to") to Dominic Cummings ("GDPR [is] horrific... idiotic"). Data is seen as a resource to be gathered and exploited through algorithms, rather than as something to be treated with the utmost reverence.

Free of the EU regulations, not only would a UK data haven be able to reduce a citizen's right to data privacy (something perhaps hinted at in the recent 2020 National Data Strategy through seeing 'data as an opportunity' and speaking of a need to 'challenge legal barriers, cultural blockers and risk aversion'), but it would be able to play host to data belonging to, or desired by, politically questionable regimes and morally dubious companies in return for a profit. Whether this data was acquired according to the highest standards of regulation in the first place, and what it might be used for, would arguably not matter to a government that sees regulation as the enemy and privacy as something to be tested to its furthest limits.

As the most apposite example, the UK government has come in for sustained criticism over the alleged laxity in protecting any data submitted to Track & Trace and concerns that it will not always be used 'safely, legally and competently'. A public health crisis this may be but considering that there was no Data Protection Impact Assessment submitted by the Department for Health, the entire service (originally, at least) was an illegal operation. Hardly engendering confidence in how the government treats its own citizens' data, much less anybody else's. The problems of knowing where your data is, and who has use of it, are spread far and wide and proper data audits to offer the bigger picture are only increased in importance in light of situations like this.

In this light, the new Digital Markets Unit, a newly-created part of the Competition & Markets Authority, could prove to be a major factor in curtailing the power of the biggest tech firms and ensuring the rights of the consumer with regards their information, and their choice. But if the post-EU country operates its data regulation on the same principle that it does everything else – doing nothing to curtail the power of the elite at best, and actively illegal at worst – it cannot be said that hopes are high and the impetus will fall once again to the individual companies to ensure that they understand the full range of risks, weaknesses and threats that their data may face.
