

Written Evidence Submitted by UKCloud Ltd (COG0008)

Science and Technology Select Committee Inquiry: Commercial Genomics

About UKCloud Ltd

UKCloud is a British cloud services company and one of the fastest growing British technology businesses. Since 2011, we have grown from a start-up of just six people to a company employing more than 200 with a turnover of over £40million.

As a UK company, our cloud platform - and the data that resides within it - is only hosted in the UK. Our services have been accredited by NCSC on behalf of our customers as suitable for data at OFFICIAL (including OFFICIAL-SENSITIVE) level. Customers include the Ministry of Defence, the Ministry of Justice, the Home Office, and many other public-sector bodies that hold sensitive data.

Our healthcare unit, UKCloud Health was specifically established to accelerate the adoption of digital technologies in healthcare and pioneer digitally enabled approaches. UKCloud Health supports healthcare organisations across the public and private sector including NHS Digital, Cinos, Babylon, and Genomics England.

We provide the IT infrastructure for Genomics England's 100,00 Genomes Project to create a genomic medicine service within the NHS and kickstart the UK's genomic industry. We securely and privately store de-identified data from hospitals, clinics, and trusts on our networks.

Below we have responded to the Committee's terms of reference (TOR) most relevant to our experience.

TOR no.2. The industrial strategy opportunity for genomics within the UK biotechnology sector, and how the Government could support UK growth (including for exports)

Data will be the world's most valuable asset in the 21st Century, and if harnessed effectively, the monetisation of data can create new insights, industries and trading platforms which will generate significant national wealth, supporting the economy, industry and communities.

The UK has some of the most valuable health and genomics data in the world and has the foundations and strong legal framework to create a national data capability that could keep the UK at the forefront of the global stage. In 2019, EY determined NHS patient data to be valued at £10 billion per annum, with each patient record worth up to £5,000 if combined with genomic and phenotypic data¹.

As the UK develops a successful and prosperous biotechnology and genomics sector, it must also invest in its cloud services and ensure that the economic benefits of research and data storage are retained domestically. Recent attempts to monetize health data, such as the recent partnership between the NHS and Amazon's Alexa, have seen data shipped overseas and held with multinational tech companies headquartered abroad instead of with British suppliers. Recent analysis from the CEPS think tank estimates that 92% of the western world's data is now stored by companies in the United States, with just 4% held in Europe².

¹ https://www.ey.com/en_gl/life-sciences/how-we-can-place-a-value-on-health-care-data

Some European nations have already woken up to the opportunities afforded by cloud and the creation of a sovereign digital ecosystem. In October 2019, the German and French Governments announced they are collaborating to launch a European cloud network this year, Gaia-X, in a bid to put data back in European hands. To secure the UK's national capability and deliver, protect, and monetarise data from genomics, the UK should follow the lead of our European counterparts and develop our own domestic cloud infrastructure network.

Developing our own national capability would enable the UK to have more control over the storage of our health data, grow citizen trust and enable the UK to reap the economic benefits. In the same way that we built our great industrial heritage, we need to invest in people, skills, a supporting infrastructure, and a solid regulatory framework to support genomics research and data collection.

By nurturing and growing our vibrant native health-tech and genomics industries and supporting them through a procurement policy that has the national interest at its heart, we can build an infrastructure that keeps our data and economic returns in the UK and subjects it to the highest regulatory, ethical and jurisdictional standards.

TOR No.6. What data obtained from genomic testing could be used for and if sufficient protection is in place for consumers using commercial genomic tests

It is paramount that data from genomics and other health-tech activities is stored safely and securely in the UK to retain public trust and alleviate data privacy concerns. A June 2019 YouGov poll found that although 71% of people were happy to share patient data if it were anonymised, 70% would be unhappy if analysis were undertaken by a multinational 'big tech' company. Only 13% of participants responded that they trusted such companies to handle anonymised data confidentially³.

Moreover, since the US government enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act in March 2018, law enforcement agencies (from local police to federal agents) can demand access to data stored on servers hosted by US-based tech firms, such as Amazon and Google, regardless of the data's physical location and without issuing a request for mutual legal assistance, placing UK health data at risk⁴.

Furthermore, in recent years Government departments procurement processes have displayed an increasing preference for these large US tech giants. In the cloud sector alone, we have seen the emergence of hyperscale US cloud service providers dominating the landscape, heavily concentrating the market and making it increasingly difficult for smaller providers to permeate.

The increased consolidation of UK Government data provokes privacy and security concerns as well as issues regarding the public purse. In April 2020, over 300 privacy experts raised concerns around NHSX's ill-fated plans to introduce a centralised NHS Test and Trace application to track the spread of coronavirus as it would struggle to gain public trust⁵.

² https://www.ceps.eu/wp-content/uploads/2019/09/Hidden-Treasures-Book_WEB.pdf

³ <https://www.digitalhealth.net/2019/06/yougov-survey-reveals-willingness-for-patient-data-to-be-shared/>

⁴ <https://www.bristows.com/news-and-publications/articles/data-protection-day-2019-the-us-cloud-act-and-uk-business/>

⁵ <https://www.theguardian.com/world/2020/apr/20/coronavirus-digital-contact-tracing-will-fail-unless->

Further, in June 2020, civil liberties organisations objected to government's decision to allow data analytics companies to build an NHS datastore and profit from access to patient data⁶.

Data consolidation should be of particular concern for the Government, given the potential damage only a single hack or inadvertent leak can do. Only last year, the National Cyber Security Centre published a blogpost on the ease with which data 'buckets' can be left unprotected and open to the public⁷. In practice, data stored with large hyperscale US companies has been inadvertently left unprotected on multiple occasions. Sensitive data held by sophisticated companies including Dow Jones, Facebook, Experian and Verizon has been left open to the public and vulnerable to being accessed and copied. In 2019, 540m Facebook users' personal information records were left exposed when hosted on AWS's platform⁸.

This shows how easily a data leak can occur, with the potential ramifications hugely exacerbated by the consolidation of data with a single supplier. Such a leak of UK health data would be catastrophic, as the data consolidation means there would be millions of pieces of highly sensitive personal information freely accessible.

The potential for cloud services to influence the way we store, and share data is huge. However, an overreliance on a small number of international companies creates unnecessary risks which can ultimately breed a lack of trust in the sector. This will deprive the UK of the full benefits of using cloud services and stifle UK investment and innovation in the sector.

(June 2020)

[privacy-is-respected-experts-warn](#)

⁶ <https://www.computerweekly.com/news/252484257/NHS-Covid-19-datastore-contracts-published-under-pressure-from-privacy-groups>

⁷ <https://www.ncsc.gov.uk/blog-post/theres-hole-my-bucket>

⁸ <https://www.upguard.com/breaches/facebook-user-data-leak>