Q2. What barriers do individuals, businesses, or other organisations face in the uptake of the right to data portability or other data subject rights?

The data brokers and intermediaries (largely the same thing) would prefer to ignore citizens rights rather than comply with them.

The data practices of the UK Biobank insist that they may sell genomic data to eugenicists, to hostile states, and to shell companies because they believe they have got permission to do. Data brokers like Our Future Health believe the same with the distinction that for the same reasons as Biobank insist they can sell data to China, OFH believe they can't.

Data brokers and intermediaries will collapse like the 1990s did to mutual building societies and the financial crisis of a decade later.

Q3. Aside from personal data protection laws, how do other areas of law interact with the operation of data intermediaries?

Most intermediaries ignore bits of the law they don't like.

Q9. Can you provide any evidence on potential risks for the wider exercise of data subject rights by third parties (such as data stewards) on behalf of a data subject? Can you identify any risks associated with the activities of data intermediaries?

All data Trusts turn into intermediaries which turn into data brokers when they run out of money. 23andMe collapsed with the genetic data of millions, UKBiobank fearing competition sells data to anyone who'll buy it (including eugenicists operating out of the same address as QAnon front companies). Online pharmacy Pharmacy2U sold their patient list and the first people in line were convicted fraudsters and scammers. All data brokers fail.

Various health charities have looked at creating their own intermediary in the wake of the ongoing NHS data scandals, and none of them consider it viable. If they can't make it work, no one else can without selling out the data subjects. But facebook etc will quite happily take the research that shows that a bunch of people would give up their work passwords in return for a chocolate bar, and use that to prey upon the British public. And they'll use "data trust" as a brand to do it.

Q11. Can you provide any evidence of a best practice approach to managing those risks? What should the roles of Government, regulators, and the market be?

All "best practice" gets abused.

The ICO is clear that anonymisation and pseudonymisation of data is processing, and that pseudonymised data remains personal data, yet even the Department of Health in England doesn't care about the law.

Following the law would be a start, and if DSIT can't make another department do it, the private sector will run rings around you.