Table of contents

XIV. Data protection post-Brexit – the hot topics

1. Introduction

The framework of data protection legislation that takes the UK into the post-Brexit age will form the background for many issues that frequently require attention in our court system. The year 2020 for instance saw a significant case on employer responsibility for wrongful actions of staff who compromise personal data reaching the Supreme Court (see section 2 below).

The issue of what freedoms there should be to transfer data outside of the UK's data protection system is another area of continuing contention.

As noted earlier in this Special Report, the increasing role of AI in the processing of personal data has opened up another battlefront between data privacy campaigners and promoters of innovative solutions for many of the challenges that society confronts, including health, good educational outcomes and even policing.

A particularly controversial application of AI-based systems that affects the life of virtually every computer and smartphone user is behavioural-based advertising, where the user's interests expressed through online activity are captured, processed and turned into

"The [Supreme Court] judgment [in Morrisons*] sends a message to all employers that the issue of vicarious liability remains a potential route to compensation for a data subject."*

targeted advertising promoting products and services highly likely to be of interest. The topic has become even more controversial with service providers such as Google even interrogating email content (with its Gmail product) as part of their tracking of user behaviours.

In this final chapter we look at these areas and how the ICO endeavours to appropriately balance the encouragement of innovation with the protection of the rights of the individual data subjects. This chapter also looks at a case in which the courts had to navigate tricky waters to the background of a significant data breach, leading to a class action by a large group of affected individuals and the long-standing rule that employers can be vicariously liable for the wrongful actions of employees.

2. The *WM Morrison Supermarkets plc* case[58]

When a massive data protection breach involves a major employer as its direct victim and more than 5,500 personnel as collateral damage, it is no surprise that this leads to a major civil case taken up to the highest decision-making court in the UK – the Supreme Court.

The case concerned a disgruntled employee of WM Morrison Supermarkets plc (trading as Morrisons) with a very high-level access to the data of the business due to his involvement in the internal audit

function. Having resigned from the business in unhappy circumstances, the employee – Andrew Skelton – chose a dramatic way of demonstrating disenchantment with his former employer. On leaving he took with him the personal data of the company's personnel, later making this accessible through a public file-sharing website.

A class action raised against Morrisons was initially successful, with the High Court finding in favour of the plaintiffs – the basis for this being the long-established rule that an employer should be found responsible for actions engaged in by an employee where third parties suffer loss.

The Supreme Court reversed this decision, but in doing so scrutinised the circumstances and careful consideration of how far employee Skelton had departed from the usual course of his duties owed to his employer.

While the Supreme Court decision went in favour of Morrisons, the judgment given by Lord Toulson sends a message to all employers that the issue of vicarious liability remains a potential route to compensation for a data subject with particular regard being had to the function that the employee performed within the organisation and the degree of connection between the wrongdoing that occurred and the functions performed by the employee. In short, the question is: was the wrongdoing sufficiently closely connected to the role played by the employee for the employer to be found liable?

It seems likely that cases of this kind will arise again. Employees losing data sticks, leaving computer monitors on close to windows and working on documents electronically on trains are just three examples of risks that employers will routinely encounter.

As we saw in Chapter X, information governance is an area that demands close attention on the part of organisations to ensure that effective procedures are in place to minimise, or even eliminate, risks of this kind.

3. The impact of Brexit, including the relevance of data protection to the effective conclusion of trade deals

One of issues that had been the focus of attention during the period in which arrangements were being made with the EU for the UK's departure from EU membership was whether the EU will judge the UK's data protection legislation as affording adequate protection for EU citizens. The issue is of significance because having an adequacy decision leads to a streamlining of transfers of data from the EU to the UK as a 'third country'. Without such a decision, transfers of personal data from the EU to UK organisations will require additional legal

safeguards – usually referred to as 'standard contractual clauses' – and the taking of increased due diligence steps relating to the security of the data and limitations on other parties (eg, surveillance authorities) to access the data.

Standard contractual clauses are a set of requirements that may be bolted into commercial or other contractual agreements that would lead to a UK data processor committing to protect personal data in terms that meet the expectations for protection set within the EU under the EU GDPR.

The EU committed to support the securing of an adequacy decision within the Brexit political declaration, but the decision making on previous adequacy decisions (11 have been made in relation to other non-EU or EEA countries) can be lengthy – 18 months being the record to date and with the timeline for the EU and UK being significantly shorter.

By contrast, the UK has made it clear that it regards the EU data protection regime as adequate, with data controllers free, accordingly, to transfer data to EU entities without additional formal data protection compliance measures of the kind the EU expects of the UK.

Protection of personal data is now an important consideration in all free trade arrangements given the increasing role played by digital services in international trade. The UK having adopted its own version of the EU GDPR will make this aspect one of the most straightforward issues to consider when negotiating trade deals with other countries across the world.

4. Advertising and personal data

This is one of two particularly controversial areas concerning the use of personal data – the second, facial recognition technology, being addressed in section 5 below.

The EU is developing legislation to regulate behavioural advertising – the EU Parliament in particular having been subjected to intensive and sustained lobbying on the issue. The argument is that there is a growing propensity for individuals to be targeted under mass surveillance strategies that connect potential advertisers to sales opportunities on a customised basis involving the use of personal data.

The processes that lead to the placing on webpages of what some describe as 'personalised advertising' has become a significant economic activity with powerful technology harnessed, enabling businesses to apply their marketing budgets to real-time bidding processes, with advertisers given access to website visitors almost in

"Protection of personal data is now an important consideration in all free trade arrangements given the increasing role played by digital services in international trade."

real time against the subject of the browsing that the user has engaged in.

Regulators across the EU are carefully scrutinising the practices adopted in the context of GDPR compliance. A preliminary finding of the Belgium regulator is understood to have found that a tool used by digital marketing and advertising association IAB Europe to secure user consent fails to meet the GDPR requirements, placing that business in a position in which all the processing it embarks on is unlawful.[59]

In the UK, the ICO published an updated report on this activity (described as 'adtech') in June 2019.[60] The ICO expresses considerable caution over the practices adopted and is now engaged in further research with a view to reaching conclusions that it considers appropriate. A particular concern surrounds the access gained to data subject special category data – an implication being that data controllers will have difficulties demonstrating that the greater requirements for consent to the use of such data have been met.

The data profiles that are created through the processing of personal data are referred to in the report as sometimes "disproportionate, intrusive and unfair, particularly when people are often unaware that it is happening".[61]

Behavioural advertising is recognised as a marketing tool of advantage to businesses both large and small. It can be argued that it also benefits data subjects who are thus spared exposure to information of little or no relevance.

The issues surrounding behavioural advertising will be a significant area of controversy for some time to come.

5. Facial recognition technology

Facial recognition technology is a further area in which the application of AI is proving controversial. This is particularly so with regard to its use by police forces, with a Home Office programme encouraging the placement of cameras in areas with significant footfall, such as busy high streets and around sports stadia – the intention being to identify individuals who are of interest to the police authorities.

The technology involves capturing facial detail of data subjects which is then processed to establish whether there is a reliable match against a database of targets. A case reached the Court of Appeal in early 2020, with judgment delivered in August 2020[62] declaring the particular application of technology involved unlawful. The basis of the decision provides a useful appreciation of one of the key risks that are understood to exist in connection with the use of AI – this being in the context of equalities duties.

The Court of Appeal determined that the preparatory steps taken in the development of the system were insufficient and led to a bias against women and people of colour. The police force had also failed to conduct an adequate data protection impact assessment.

To help develop an understanding of the risks of bias and discrimination that may be inherent in AI systems, the ICO has published a blog titled "Human bias and discrimination in AI systems".[63] This provides a useful explanation of what is, in the eyes of the ICO, a key compliance issue as highlighted in Chapter XIII of this Special Report.

*This chapter 'Data protection post-Brexit – the hot topics' by Frank Suttie is from the Special Report '*Data Protection and the New UK GDPR Landscape*', published by Globe Law and Business.*