The Future of Data Protection Litigation

JACK MCCRACKEN

We give every single case the care and attention it deserves.

ROPEWALK CHAMBERS

+44 (0) 115 947 2581 - www.ropewalk.co.uk

"This case is being determined in the twilight of the DP Directive regime, with the first light of the GDPR already visible on the horizon".

Warby J. on 13 April 2018.

***NT1, NT2 v Google LLC* [2018] EWHC 799, paragraph 105.**

Part 1: Overview

1. The purpose of this paper is to consider what data protection litigation might look like under the new regime of the GDPR and the Data Protection Act 2018: in other words, the brave new world that follows 25 May 2018.

2. The public perception of the GDPR is that it heralds a revolution in data protection law. The reality is probably more prosaic, in that the GDPR builds on the rights established by the European Data Protection Directive 95/46/EC ('the DP Directive'), whilst significantly expanding the rights of data subjects into new areas by embracing additional categories of personal data and imposing more onerous obligations on data controllers when they process personal data. It is that combination which should provide fertile ground for litigation by aggrieved, and likely better informed, members of the public wishing to vindicate their data rights.

3. As for the GDPR, it is difficult to think of another four-letter acronym that has inspired more fear in the hearts of the corporate world (USSR perhaps?). No one with an email account can have escaped the great bombardment of requests to update privacy settings of April and May 2018, which preceded the coming into force of the GDPR on 25 May 2018.

4. But that episode of mass hysteria via email illustrates a truth at the heart of the GDPR: the greatest impact of the new regime is likely to fall on companies with a large online presence who digitally process vast quantities of personal data for marketing purposes, and make extensive use of data profiling. It might reasonably be said the misuse of personal data to allow companies to target users online is an obvious area of future litigation. The GDPR should make such litigation easier by increasing substantive rights and the remedies available for breach of those rights. A few specific examples of likely areas of litigation should suffice for the purposes of this introduction.

5. Historically, companies that collect personal data online have relied on users or customers ticking a single consent box after providing their personal data to say buy a book on Amazon, or to create an account on Twitter. As will be seen, those sorts of businesses will no longer be able to process

personal data for marketing purposes in reliance on of a single instance of the provision of generic consent.

6. Online search engines and social media giants, and indeed all companies collecting digital data, face an even greater challenge because of the expansion of the meaning of 'personal data' to encompass IP addresses and the other digital footprints left by people browsing the internet. So now it is not just names, addresses, telephone numbers etc. that are caught within the definition of personal data.

7. So what form might the conflicts take? At one end of the spectrum, the Cambridge Analytica scandal exposed the allegation that the personal data of about 50 million American Facebook users were improperly passed to CA to be used in the dark arts of 'psychoanalytics' (a form of data analytics), a technique of apparently doubtful effectiveness whereby a person's internet history and other personal data are used to try and determine whether they might want to vote for a particular presidential candidate, or support a certain referendum campaign, and then target them with tailored political advertisements.[1]

8. At the other end, there is the use of the same data for targeted 'ads', the sort that pop up when one browses the internet. The same point applies, there is now greater public awareness that companies may be using personal data provided legitimately for one purpose, and then allowing that data to be used by third parties to market their products i.e. a different purpose to that for which consent was provided. This stands out as an area ripe for litigation.

The Brexit angle: A brief comment on implementation of the GDPR

9. It is impossible to escape Brexit, and this discussion of data protection law is alas no exception. The result of the referendum on the United Kingdom's membership of the European Union, held on 23 June 2016, cast into doubt (at least temporarily) whether the UK would go on to permanently implement the GDPR, being as it was another piece of EU legislation, a subject of much derision during the referendum campaign (and for many years beforehand, and continuing to the present day).

10. Despite the referendum result, there has never been any real suggestion that the UK Government intended to exercise the nation's newfound sense of national sovereignty and reject implementation

[1] On Wednesday 11 July 2018 the Information Commissioner's Office published several documents, including 'Investigation into data analytics for political purposes – update', in which an update was provided on various regulatory action in this respect. Amongst other action, the ICO announced it was taking steps with a view to pursuing a criminal prosecution against the parent company of CA (SCL Elections Limited), and that it had issued a Notice of Intent against Facebook to issue a monetary penalty in the sum of £500,000, the largest possible under the old DPA 1998 regime.

of the GDPR: it was always more a question of form rather than substance i.e. after Brexit *how* would the GDPR apply in UK law?

11. In a speech titled 'Our future economic partnership with the European Union' delivered on 2 March 2018 (known as the Mansion House speech), the Prime Minister spoke of the 'five foundations' that must underpin the future trading relationship between the UK and the EU.[2] The fourth of those was an arrangement for data protection, about which the Prime Minister said:

> *"the free flow of data is also critical for both sides in any modern trading relationship too. The UK has exceptionally high standards of data protection. And we want to secure an agreement with the EU that provides the stability and confidence for EU and UK business and individuals to achieve our aims in maintaining and developing the UK's strong trading and economic links with the EU.*
>
> *That is why we will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the UK's Information Commissioner's Office. This will ensure UK businesses are effectively represented under the EU's new 'one stop shop'[3] mechanism for resolving data protection disputes".*

12. Prior to this speech, there had been speculation about whether the UK would seek, in respect of the GDPR, what has been called the 'implementation option' (needed for the UK to pursue the EEA/EFTA/customs union future relationship options) or the 'equivalence option' (the third country option where the UK has no special relationship with the EU) which is largely based on proving its laws provide adequate protection for personal data.[4] The Prime Minister's words seem aimed at the former rather than the latter option i.e. where she says 'more than just an adequacy arrangement'.

13. Of course, on 23 May 2018 the Data Protection Act 2018 received Royal Assent, with its main provisions coming into force on 25 May 2018, the same day as the GDPR enters into force by reason of the UK's current membership of the EU. The Act can be seen as implementing the GDPR subject to the modifications and exemptions contained within the Act. That is so despite the preamble containing no explicit reference to the GDPR, in contrast to the provisions of the DPA 2018 itself.

14. The Explanatory Notes to the DPA 2018 speak principally of the Act implementing something different, namely a commitment in the 2017 Conservative Party manifesto to 'repeal and replace the UK's existing data protection laws to keep them up to date for the digital age'. But it goes on to state that the DPA 2018 'replaces the [DPA 1998] and provides a comprehensive legal framework for data protection in the UK, in accordance with [the GDPR]'.[5]

---

[2] Transcript of the speech. https://www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union
[3] This must be an implicit reference to the creation by the GDPR of the European Data Protection Board (see Section 3 of the GDPR), which is to be the 'one stop shop' for the consistent application of the GDPR.
[4] Rosemary Jay, *Guide to the General Data Protection Regulation,* pp 6 – 8.
[5] *Data Protection Act Explanatory Notes*, p8.

15. To bring matters up to date, after some internal wrangling, the UK Government published the 'Brexit White Paper'[6] in July 2018. In Chapter 3, the White Paper says this in relation to the continued exchange and protection of personal data:

> *The UK and the EU start from a position of trust in each other's standards and regulatory alignment on data protection. The UK's recent Data Protection Act 2018 strengthened UK standards in line with the EU's General Data Protection Regulation (GDPR) and the Law Enforcement Directive, providing a unique starting point for an extensive agreement on the exchange of personal data that builds on the existing adequacy framework. The UK is ready to begin preliminary discussions on an adequacy assessment so that a data protection agreement is in place by the end of the implementation period at the latest, to provide the earliest possible reassurance that data flows can continue.*

16. Arguably this suggests it is the 'third country option' based on equivalence/adequacy rather than implementation that is to be pursued. For now, we have 'implementation' and the GDPR will apply by virtue of the UK's continued membership of the EU until 29 March 2019. After that, it seems likely that the GDPR/Data Protection Act 2018 regime is here to stay as one of the foundations of the future relationship between the UK and EU.[7]

Jack McCracken

July 2018

[6] *The Future Relationship Between the United Kingdom and the European Union, Cm 9593*
[7] Subject to domestic political uncertainty.