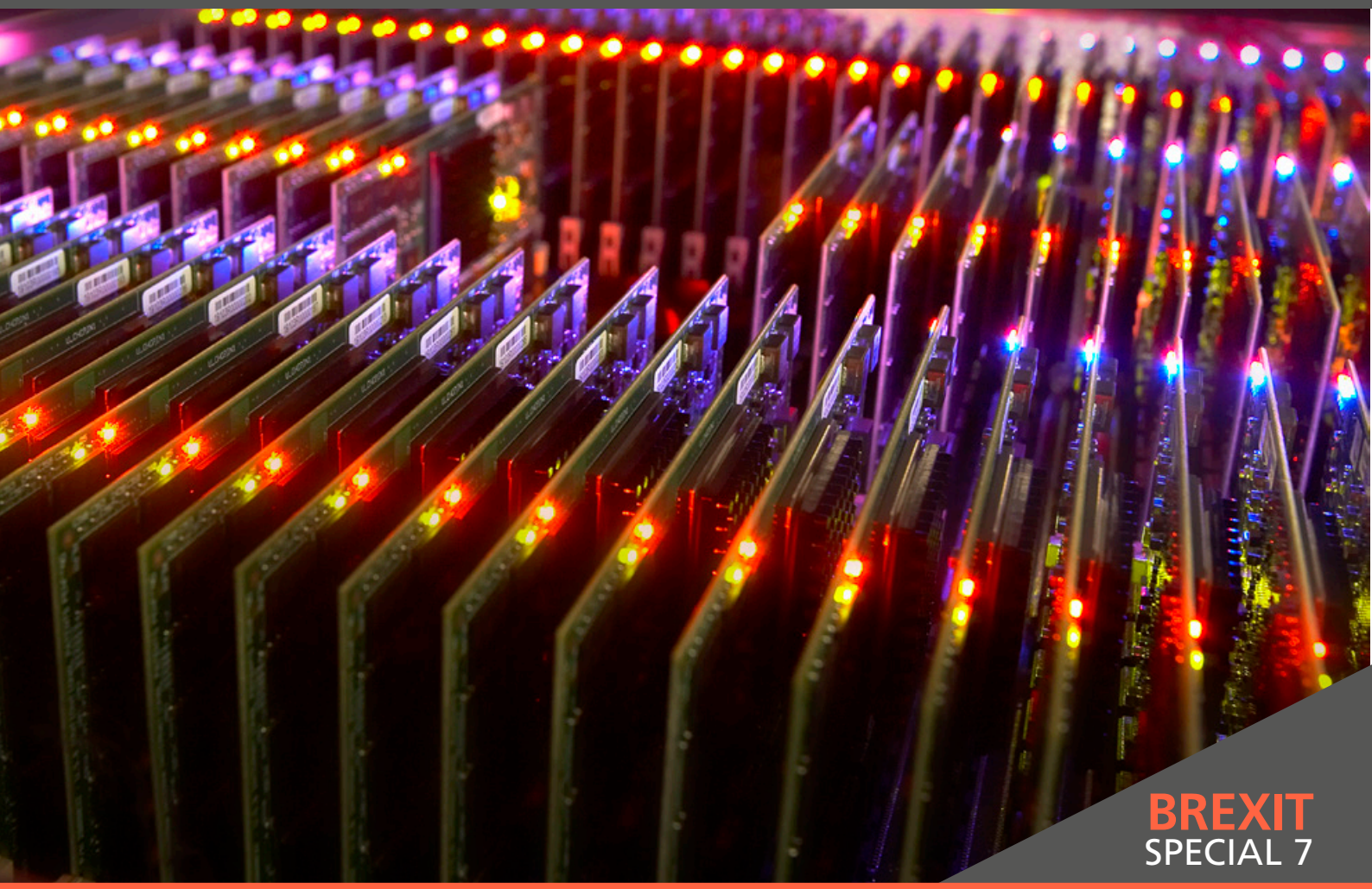
LSE LAW POLICY BRIEFING SERIES



BREXIT
SPECIAL 7

Brexit And The UK's Tech Industry

Dr. Orla Lynskey

POLICY BRIEFING 26 | 2017

LSE Law

Electronic copy available at: https://ssrn.com/abstract=2941375

Brexit And The UK's Tech Industry

The UK's digital economy is currently growing at twice the rate of the wider economy, and now contributes an estimated £97 billion per annum to the economy. As such, the Prime Minister has singled growth in the technology industry as a priority for the UK after leaving the EU. Understanding the implications of Brexit for the tech industry requires us to think about the changes to the UK's regulatory framework once EU law ceases to apply, and the constraints that EU law imposes even after Brexit.

Brexit itself may challenge the ambition of growth in the tech industry in a number of important ways. For instance, the UK may find it difficult to attract the skilled staff necessary to continue growing at the current rate, particularly given the impact of Brexit on the university sector which is expected to help to sustain this growth. Early indications also seem to suggest that investors in the tech industry are developing cold feet, which might have an impact on the UK's much-lauded ability to nurture tech unicorns.

Perhaps the most significant implication of Brexit for the tech industry will however be its impact on the cross-border data flows that underpin key components of this industry, such as cyber-security, data analytics and artificial intelligence. At present, the UK, like other EU/EEA countries, benefits from a presumption that its data protection regime offers an adequate level of data protection to individuals. This presumption will fall away once the UK leaves the EU unless it retains EEA membership. In order to maintain personal data flows between the EU and the UK, the UK will therefore need to prove that it offers an 'adequate' level of personal data protection, a standard that is likely to prove illusive in light of recent jurisprudence of the EU Court of Justice. This is one crucial policy area where having one's cake and eating it may prove to be impossible, leaving the UK in the unenviable position of having to chose between, on the one hand, its preferred standards of data protection and privacy (typically below EU standards) and, on the other, the free flow of personal data sustaining the domestic tech industry.

Relevant EU legal framework

Until 2009, and the entry into force of the Treaty of Lisbon, EU data protection law was comprised solely of secondary legislation, most notably the 1995 Data Protection Directive. This legislation was justified on the grounds that a uniform level of fundamental rights protection was necessary in order to ensure the free flow of personal data in the EU's internal market. This secondary legislation has subsequently been reinforced, and its fundamental rights dimension pushed to the fore, by the introduction of a right to data protection in the EU Charter of Fundamental Rights and a specific legal basis for data protection in Article 16 TFEU. These provisions therefore reflect the 'mainstreaming' of the right to data protection across areas of EU policy, and its new standing in the EU legal order. The EU Court of Justice has been eager to embrace these new legal provisions. Indeed, the seminal cases where the Charter was invoked to invalidate provisions of EU secondary legislation and, subsequently, an entire legislative instrument, on the basis of incompatibility with the EU Charter both involved the right to data protection.

These EU provisions – both primary and secondary – have received a mixed welcome in the UK's domestic legal order. The 1995 Data Protection Directive was implemented by the Data Protection Act 1998 (DPA 1998). However, whether the DPA 1998 has been correctly implemented is a matter of longstanding dispute. Indeed, the European Commission has been investigating the UK for an infringement of its data protection obligations since at least 2010. While both the UK and the EU have remained tight-lipped regarding the status of these proceedings, the Commission investigations remain ongoing. According to materials obtained via freedom of information/ access to documents requests by Dr Chris Pounder, key elements of the data protection framework such as the notion of 'personal data' and a 'filing system' remain incorrectly implemented while there are several problems relating to the enforcement of data protection rights in the UK. The UK's implementation of the EU's E-Privacy Directive, a lex specialis that sets out rules for privacy in the context of certain electronic communications, has also culminated in a European Commission infringement investigation. These discrepancies contribute to the impression that the UK has adopted a lowest common denominator approach to data protection.

The right to data protection initially received a similarly sceptical reception into the domestic legal order. There is traditionally no right to privacy or data protection in the UK legal order, although the right to privacy has been gradually incorporated by the jurisprudence of the courts. However, the right to data protection is distinct from privacy, and therefore entails additional protection for personal data. This was lamented by euro-sceptics, and noted with disapproval by Mostyn J in the High Court judgment *AB*, when he observed that the right to data protection in the EU Charter introduced all of the ECHR's 'missing parts and a great deal more'. The Charter right

to data protection has subsequently been used by the **Court of Appeal** to disapply conflicting provisions of national law, and to broaden the circumstances in which individuals can claim remedies for breach of data protection law. This additional protection for individuals afforded by the right to data protection could potentially be lost post-Brexit. However, the incentive for the UK to depart from this high level of data protection is constrained by the EU data protection's 'adequacy' framework, as mentioned above.

In essence, the 1995 Data Protection Directive provides that data transfers from within the EU to 'third-countries' outside the EU/EEA are only possible when an 'adequate' level of protection can be guaranteed in that third country. Pursuant to Article 25 of the Directive, in the absence of an adequacy assessment by the EU Commission, the Member States assess the adequacy of third countries. To date, the Commission has only recognised **11 third countries** as 'adequate'. Article 26 therefore allows data flows between EU/EEA countries in the absence of an adequacy finding, in specified circumstances. For instance, ad hoc data transfers can take place when the individual concerned consents to the transfers, or the transfer is necessary for the performance of the contract. Other legal mechanisms have however also been used to ensure that once transferred from the EU/EEA personal data is offered an adequate level of protection. For instance, the entity transferring the data may agree with the recipient of the data upon standard contractual clauses containing safeguards.

The overall effect of these rules is therefore that third countries are held to the high level of protection of personal data aspired to by the EU when data are transferred from the EU to these countries. This has been confirmed by the jurisprudence of the EU Court of Justice. 'Adequate' was interpreted as 'essentially equivalent' in the ***Schrems*** judgment. In that case the Court held that this assessment of essential equivalence must examine the content of the applicable rules in that country as well as the practice designed to ensure compliance with them. Furthermore, the situation should be checked periodically in order to ensure that the finding of adequacy remains factually and legally justified. It followed from *Schrems* that the primary mechanism for EU-US data transfers, the 'Safe Harbor' scheme, was invalidated as the US did not offer this essentially equivalent protection. In particular, the Safe Harbor scheme provided that 'national security, public interest, or law enforcement requirements' had primacy over its principles, thereby enabling certain US authorities to violate the rights to privacy and data protection of EU individuals in an unjustifiable manner.

The EU is set to replace the 1995 Data Protection Directive with a new 'General Data Protection Regulation' **(GDPR)** in May 2018. The GDPR retains this adequacy-based framework and thus, post-Brexit, the UK may need to demonstrate that its data protection framework offers protection that is 'essentially equivalent' to that offered by the EU. It follows from *Schrems* that this adequacy assessment will incorporate a holistic interrogation of the UK's legal framework for personal data processing, including an assessment of the legal provisions applicable to data processing for national security purposes.

Assessing the adequacy of the UK's legal framework

In its **Brexit White Paper**, the UK Government recognises that the stability of data transfers is important for many sectors of the UK economy, and states that it will seek to maintain the stability of these transfers. Members of the **regulator** – the Information Commissioner's Office (ICO) – and **Government representatives** initially indicated that the UK might consider alternative data protection frameworks. However, the Government has subsequently confirmed that the GDPR will be implemented in May 2018, while ostensibly leaving open the possibility that what is perceived to be a more business-friendly approach might be adopted at a **later stage**. Indeed, given the current lowest common denominator approach to compliance with EU data protection laws, many suspect that the UK will take full advantage of the flexibility inherent in the GDPR. Any desire to take such advantage of flexibility will however be tempered by the fact that any variations in legislation may convince firms that it more cost effective and less cumbersome to host data in the EU rather than **the UK**. This flexibility would need to be utilised in a way that would not undermine the UK's bid for adequacy. Moreover, formal reception of the GDPR into the domestic legal order will not suffice: the current implementation deficiencies will be subject to renewed scrutiny and attention will also turn to the effectiveness of domestic data protection. The UK will need to improve its record in order to pass muster on these fronts.

Nevertheless, the most significant challenge to a finding of adequacy will be the recent finding of the EU Court of Justice in the joined cases of ***Tele2 Sverige and Watson***. In this case, the Court was asked to consider, amongst other things, whether its previous judgment in ***Digital Rights Ireland***, firstly, prohibited general and indiscriminate data retention as a matter of principle, and, secondly, set out 'mandatory requirements' that subsequent national legislation for communications data retention and access must respect. The Court reached the momentous conclusion in *Tele2 Sverige and Watson* that general and indiscriminate data retention legislation, even when it serves the justified objective of fighting serious crime, exceeds what is necessary and is therefore disproportionate. Thus, in order to comply with the EU Charter rights to data protection and privacy, telecommunications data retention must be targeted on the basis of objective criteria, rather than general and indiscriminate in nature. This finding is at odds with the findings of the UK Supreme Court in **Catt**, a judgment concerning the police's powers to collect and retain data about the participation of non-violent individuals (including 91 year old Catt) in political protests on its Domestic Extremism Database. Lord Sumption suggested in that case that 'intelligence is necessarily acquired in the first instance indiscriminately' and that 'its analysis can only be judged in hindsight', a finding diametrically opposed to that of the EU Court of Justice in *Tele 2 Sverige and Watson*.

Equally relevant is the fact that the UK has only recently adopted

the **Investigatory Powers Act 2016**, an Act designed to regulate interception of communications and the acquisition and retention of telecommunications data in the UK. Section 87 of this Act provides the Secretary of State with the power to require telecommunications operators to retain electronic communications metadata of all customers for up to 12 months while section 136 allows the Secretary to issue 'bulk acquisition warrants'. Pursuant to such warrants, telecommunications operators are required to disclose general or specified electronic metadata they possess or can assess (including metadata outside the UK) to intelligence agencies. These provisions of the IPA 2016, amongst others, are clearly at odds with the EU Court of Justice finding in *Tele2 Sverige and Watson*. Moreover, given that the findings in *Tele2 Sverige and Watson* are anchored to an interpretation of the EU Charter, without amending the Charter the EU position will not, and cannot, change. The UK post-Brexit may therefore be left with a choice between its existing mechanism for targeting serious crimes (i.e. general data retention) and adequacy, which allows for uninterrupted data flows between the EU and the UK.

Dr. Orla Lynskey
(Department of Law,
London School of Economics
and Political Science)

ORLA LYNSKEY

Orla Lynskey is an Assistant Professor at LSE Law. She teaches and conducts research in the areas of data protection, technology regulation, digital rights and EU law. She holds an LLB (Law and French) from Trinity College Dublin, an LLM in EU Law from the College of Europe (Bruges) and a PhD from the University of Cambridge.

LONDON | MARCH 2017

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Department of Law
The London School of Economics
and Political Science
Houghton Street
London WC2A 2AE