Case No. UKSC 2019/0213

IN THE SUPREME COURT OF THE UNITED KINGDOM

ON APPEAL FROM THE COURT OF APPEAL (CIVIL DIVISION)

BETWEEN:-

RICHARD LLOYD

Claimant/Respondent

-v-

GOOGLE LLC

Defendant/Appellant

SUBMISSIONS ON BEHALF OF

techUK LIMITED

---

1. techUK is grateful for the opportunity to intervene in writing before the Supreme Court in the present appeal. techUK is an incorporated body established in 2013 to represent and promote companies working in the UK's technology sector. Its membership consists of approximately 850 companies in England, Scotland, Wales and Northern Ireland that collectively employ about 750,000 people, which is approximately half of all the UK's technology sector workers. The UK Government estimates that in 2020 the data economy made up about 4% of GDP in 2020[1].

2. This appeal concerns two matters which are of profound significance to the members of techUK:
   (1) The circumstances in which an infringement by data controllers or data processors of an obligation contained in data protection legislation may give rise to an entitlement to compensation ("**Issue 1**").
   (2) The availability of "opt out" representative group actions under data protection legislation ("**Issue 2**").

[1] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy [18 April 2021]

3. In overview, techUK respectfully submits that the Court of Appeal erred in its conclusions in relation to both of these issues. techUK supports the UK's legal and regulatory framework for the protection of personal data and has spoken out in favour of responsible data use and appropriate data safeguards[2]. The Court of Appeal however failed to take into consideration the complexity of the framework that already exists, and its conclusions in relation to Issues 1 and 2 will have significant unintended consequences, including a marked chilling effect on the continued development of the technology sector in the UK.

Context in which Issues Arise

4. It is important to delineate three aspects of the context in which the two issues arise for consideration, that context being critical to techUK's intervention.

(1) General Data Protection Regulation

5. Although the claim in which this appeal arises is brought under section 13 of the Data Protection Act 1998 ("**DPA 1998**"), which has since been repealed[3], the decisions reached on this appeal will be of critical ongoing importance as the structure and wording of the provisions concerning compensation are substantively replicated in Article 82 of the General Data Protection Regulation ("**GDPR**")[4] [5].

---

[2] For example, in techUK's report, "*Trust, Innovation and Global Leadership: getting data governance right in the UK in 2021*" (published March 2021), accessible at https://www.techuk.org/resource/techuk-on-the-future-of-data-governance-for-the-uk.html [18 April 2021]

[3] Repealed on 23 May 2018: DPA 2018, Schedule 19, paragraph 44. Section 13 continues to apply to any act or omission pre-dating the implementation of the GDPR: DPA 2018 Schedule 20, paragraph 6(1). The underlying Directive 95/46/EC ("**the Directive**") was repealed by the GDPR: Article 94(1)

[4] The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("DPPEC Regulations") amended the GDPR as 'retained EU law' brought into UK law through the European Union (Withdrawal) Act 2018 ("**Withdrawal Act**"), the DPA 2018, and other data protection legislation to fit the domestic context. References in these submissions to the GDPR include references to the UK GDPR unless otherwise indicated.

[5] The Court of Appeal "*found it helpful although not decisive*" to consider material provisions of the GDPR: [64]

6. Section 13(1) provides that "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*". Article 82 provides that "*An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage*."[6]

7. In this regard, at least one action has been commenced under the GDPR after the Court of Appeal's decision in this case seeking damages for "*loss of control of personal data*"[7]. Given the materially identical operative wording in the relevant provisions, this is unsurprising and it is difficult to see on what basis a different approach could reasonably be adopted by a domestic court in relation to Issue 1 under Article 82. A consideration of the GDPR and its development is also necessary when addressing Issue 2.

8. The GDPR will provide the framework for processing data for the foreseeable future. It is the "*global benchmark*" for data protection[8]. It is designed to be technology-proof so as not to require replacement in the face of technological advances[9]. The UK has retained the GDPR in substance despite its departure from the European Union ("**EU**") in the UK GDPR[10], and in light of the requirements related to transfers of data into and out of the EU is highly likely to do so in future[11].

---

[6] Section 169 of the DPA 2018 similarly provides: "*A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the [UK] GDPR, is entitled to compensation for that damage from the controller or the processor…*"

[7] The representative action in *S (A Child) v TikTok Inc. & Ors* [2020] EWHC 3589 (QB). The claim has been issued but "*those representing the claimant do not wish to press on with the case until the outcome of the appeal in Lloyd v Google is known*": [6]. Other claims have been threatened or stayed pending the outcome of this appeal.

[8] *The EU General Data Protection Regulation, A Commentary, eds. Kuner, Bygrave, Docksey, OUP 2020, p.2*

[9] See e.g. Recital (15): "*In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used*"

[10] The amendments made by the DPPEC Regulations are mostly of a technical nature, such as deleting references to "Member States" or adjusting terminology.

[11] GDPR Article 45(3). A draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom was published on 19 February 2021. It stated that "*The Commission considers that the UK GDPR and the DPA 2018 ensure a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU)*

9. As a corollary, there is no reason why the autonomous EU law meaning of concepts contained in the GDPR must be identical to the meaning of the same concepts contained in the UK GDPR[12]. This raises the practical concern that data controllers and processors in competing technology sectors and industries in other jurisdictions would gain a significant competitive advantage if the terms of the UK GDPR were interpreted in the way determined by the Court of Appeal.

(2) Dual Aims of Data Protection Legislation

10. Both the GDPR and the Directive contain a built-in balance between two different aims. The first is to ensure a high level of protection of personal data. The second is to maintain "*the free flow of personal data*"[13]. The two instruments are a consequence of the legislative striking a balance between these two aims[14].

11. Under the Directive, and in particular under the GDPR, this balancing act has resulted in a complex and intersecting series of provisions providing for rights and responsibilities. In the UK, there are overlapping civil, criminal and regulatory regimes concerning the processing of personal data in both the 1998 and 2018 Acts. The scope of the Directive is "*very wide and the obligations of those who process personal data are many and significant*"[15]. The GDPR is even more expansive. It places onerous requirements on data controllers and creates requirements for data processors[16]. Responsibility is calibrated towards consequences and risk[17], as evident most clearly in the gradations in required responses to personal data breach events. There is also a significant element of

---

2016/679" (Recital (266)) but also that "*The Commission shall continuously monitor the application of the legal framework upon which this Decision is based*" (Article 3(1)):

[12] European Union (Withdrawal) Act 2018, section 6.

[13] Directive, Article 1. Similarly, Article 1(3) of the GDPR "*aims to give effect to the economic underpinning of data protection…*" *Kuner, Bygrave, Docksey*, ibid at p.51

[14] *Rechnungshof v Osterreichischer Rundfunk (C-465/00)* [2003] 3 CMLR 10, para.39

[15] *Criminal Proceedings Against Lindqvist* [2014] QB 1014 at [88].

[16] Data processors can be drawn into an action for compensation, for example under GPDR Article 82(4) and (5).

[17] "*At a high level, the risk-based approach consists in adjusting some of the data protection obligations to the risks presented by a data processing activity*": *Kuner, Bygrave, Docksey*, ibid at p.26

no-fault liability. A wide range of remedies aside from compensation are available to data subjects[18], which can be enforced through legal proceedings[19].

12. The result is a "*coherent data protection framework*" which seeks to provide enhanced "*legal and practical certainty*" to enable the development of the digital economy[20]. Considerations of proportionality necessarily arise in relation to construction and interpretation. It is also important to consider the framework as a whole when considering any individual element, since altering any part could radically upset the carefully calibrated legislative balance.

(3) UK Government Strategy

13. The Government has repeatedly emphasised the importance of data as part of its development of the economy in the aftermath of the UK's departure from the European Union. The Government's National Data Strategy[21] ("**NDS**") describes the benefits of data and states the explicit aim of "*positioning the UK as a global champion of data use, and encouraging the international flow of information across borders*" as "*a central part of the government's wider ambition for a thriving, fast-growing digital sector in the UK, underpinned by public trust. We want the UK to be a nation of digital entrepreneurs, innovators and investors, the best place in the world to start and grow a digital business, as well as the safest place in the world to go online*."

14. Moreover, during the Covid-19 pandemic, the Government described the UK technology sector as essential and its use of data as "*a lifeline*" for pandemic-affected individuals, businesses and public authorities: "*The fact that governments, businesses, organisations and public services were able to share vital information quickly, efficiently and ethically during the pandemic has not only saved countless lives, but has enabled us to work from home, keep the economy running and stay connected with loved ones during a period of unprecedented disruption.*"

---

[18] GDPR Chapter 3: "*Rights of the Data Subject*"; Articles 12 to 23; including rights to: access data; rectify data; restrict processing; erase personal data; and ensure data portability.
[19] GDPR Article 79.
[20] GDPR Recital (7); reflecting DPD Recitals (2) and (3).
[21] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#the-data-opportunity (updated 9 December 2020) [18 April 2021]

15. The data controllers and processors that comprise techUK's membership are a critical part of this sector and they are central to the Government's stated aims. They share the concerns expressed that it is necessary closely to "*weigh the priorities and potential trade-offs of data in a deliberate and evidence-based way*".

16. Finally, a series of major policy interventions in the form of the Government's response to the National Data Strategy consultation[22] in April and a Digital Strategy[23] by the end of the year are likely to raise issues of further legislation to be detailed in the Queen's Speech on 11 May.[24]

First Issue

17. The Court of Appeal wrongly concluded that "*loss of control of personal data*" was itself a form of "*damage*" that entitled claimants to compensation under section 13 of the DPA 1998. This conclusion is not compelled (or indeed supported) by the statutory wording[25], by the wording of the underlying Directive or by any decision of the CJEU or domestic authority. It elides the careful difference drawn in the instruments between the "*breach*" and the "*damage*" that the breach may or may not give rise to.

18. That natural persons should have control over their personal data is undoubtedly an animating idea behind the Directive and the GDPR. The Court of Appeal's decision however isolates and elevates that idea to, in essence, an actionable right in and of itself. This is not supported by a consideration of those instruments as a whole and upsets the careful calibration of rights and responsibilities they contain. It is indeed a seismic transformation in how the operation of the wording in the Directive and GDPR had previously been understood. The critical considerations of risk and consequences are sidestepped, since any breach may now give rise to a right to compensation,

[22] https://www.gov.uk/government/consultations/uk-national-data-strategy-nds-consultation/uk-national-data-strategy-consultation [18 April 2021]
[23] https://www.gov.uk/government/publications/build-back-better-our-plan-for-growth [18 April 2021]
[24] https://www.gov.uk/government/news/queens-speech-to-be-held-on-11-may [18 April 2021]
[25] As acknowledged by the Court of Appeal at [45].

without any consideration of any consequences of that breach or the scale of risks it created.

GDPR Recital (85)

19. In reaching its conclusion, the Court of Appeal drew attention to recital (85) to the GDPR which contains the following excerpt: "*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*".

20. Contrary to the approach of the Court of Appeal, when the whole of recital (85) is considered in its proper context it does not provide any support for a conclusion that "*loss of control*" over personal data is a form of damage for the purposes of the legislation:
    (1) The recital does not address or seek to define damages – it sets out a non-exhaustive list of potential consequences that might arise from a data breach event from the very general "*significant economic or social disadvantage*" to very specific "*financial loss*". Indeed, the recital which does directly relate to Article 82 does not seek to define damage either: recital (146) provides "*The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation.*" Both recitals contain the same structure as Article 82 (and section 13) differentiating between a breach and its possible consequences[26].
    (2) Recital (85) specifically relates to the obligation placed on data controllers to notify supervisory authorities[27] of the existence of personal data breaches[28]. In addition to the text quoted by the Chancellor (as he then was), Recital (85) continues: "*Therefore, as soon as the controller becomes aware*

[26] The operating wording of Recital (85) is "*A personal data breach may… result in physical, material or non-material damage*".
[27] In this jurisdiction, the Information Commissioner's Office ("**the ICO**").
[28] Defined as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*": GDPR Article 4(12).

that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons..." The possibility that a data breach need not be reported to the ICO if it is "*unlikely to result in a risk to the rights and freedoms of natural persons*" undermines reliance on the recital as supporting the conclusion that "*loss of control*" is a form of damage since (as is the foundation of the Respondent's case) it would always be suffered by a data subject in the event of a data breach.

(3) A consideration of the whole of the provisions in the GDPR relating to data breaches further undermines the Court of Appeal's conclusion. Articles 34 and 35 provide for three different types of personal data breach event in Articles 33 and 34. Those that are likely to result in a "*high risk*" to the rights and freedoms of natural persons must be communicated to both the ICO and data subjects directly[29]. Those that are "*unlikely*" to result in a risk to the rights and freedoms of natural persons do not need reporting to anyone[30]. Those that fall between these categories must be reported only to the ICO. Given the acknowledged requirement for an effective remedy, this gradation[31] provides strong support for the view that "*loss of control*" is not a type of compensable damage. If it were, it would be presumed that the GDPR would require that all personal data breaches be notified to data subjects, since they would have suffered loss of control of their personal data.

(4) This differentiation appears to be supported by the position of the Article 29 Working Party which formally advised in relation to the data breach notification requirements**: "***the key trigger requiring communication of a breach to data subjects is where it is likely to result in a high risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or*

[29] Article 34(1)
[30] Article 33(1)
[31] A similar gradation exists in relation to administrative fines (Article 83); recital (148) introduces the concept of "*minor infringements*" when "*a reprimand may be issued instead of a fine*"

non-material damage for the individuals whose data have been breached."[32] This approach is inconsistent with "*loss of control*" being a facet of "*non-material damage*".

Personal Data Breaches

21. The Court of Appeal decision on "damage" exposes techUK members to an increased risk of serious unintentional adverse consequences in relation to the potential for data breaches. This is for three principal reasons.

22. Firstly, given the number and variety of risk vectors, personal data breaches are inevitably commonplace. In the latest statistics produced by the ICO[33], between 1 July and 30 September 2020 there were 2594 reported personal data breaches across all sectors, including 737 "cyber-security incidents".

23. Secondly, the business model of many techUK members involves an online platform which provides a "one-to-many" service that, by its very nature gives rise to an enhanced exposure to data breach events.

24. Such a service uses different data points to allocate resources and facilitate the efficient delivery of the good or service. An example is a platform used for the sale or leasing of medical equipment to the NHS. The platform manages stock, customers, orders, returns, repairs and customer relationship management (CRM) information. The data required to run this system includes a range of personal data points from the names and contact details of sellers to possible patient and health data associated with orders. The business has a number of economic as well as social benefits, by providing an efficient allocation of equipment across the health and research sector, reducing prices through a better allocation of resources while also enabling better planning with orders and requests managed via a single platform.

[32] Article 29 Working Party "*Guidelines on Personal data breach notification under Regulation 2016/679*", revised and adopted 6 February 2018. These guidelines were endorsed by the European Data Protection Board ("EDPB"), in Endorsement 1/2018 published on 25 May 2018.
[33] https://ico.org.uk/action-weve-taken/data-security-incident-trends/ [15 March 2021].

25. Accordingly, even a single data breach event involving such a platform could affect a very substantial number of data subjects. If the event itself gives each individual a claim for compensation, the potential liability arising from that single event could be vast, even if there are no specific adverse consequences for any individual.

26. Thirdly, as the standard of liability for data breaches is based upon risk, it is in any event inherently uncertain and wide. The Court of Appeal decision stands substantially to add to this uncertainty.

27. The obligation on data controllers is not to prevent data breaches occurring per se, but to ensure that personal data are "*Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*"[34].

28. This must be read together with Article 32, which provides that "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*"[35].

29. A similar duty[36] was contained in the Directive and DPA 1998, which was considered by this Court in *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12. This Court concluded that the DPA 1998 did not exclude vicarious liability:

"*Since the DPA is silent about the position of a data controller's employer, there cannot be any inconsistency between the two regimes. That conclusion is not affected by the fact that the statutory liability of a data controller under the DPA, including his liability for the conduct of his employee, is based on a lack of reasonable care,*

[34] GDPR Article 5(1)(f)
[35] A number of potentially relevant factors are set out in Article 32(1) to (3)
[36] Schedule 1, paragraph 7 of the DPA 1998: "*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*" ("the Seventh Principle")

whereas vicarious liability is not based on fault. There is nothing anomalous about the contrast between the fault-based liability of the primary tortfeasor under the DPA and the strict vicarious liability of his employer."

30. Thus, the obligations imposed by the Directive and the DPA 1998 (as well as the DPA 2018) already involve a significant degree of risk and – although standards have developed to attempt to ensure that data is processed securely – there is no straightforward way to ensure that all risk is excluded.

31. The Court of Appeal's conclusion therefore transforms the analysis of risk. A finding of liability in respect of an event affecting a substantial number of individuals would inevitably result in exposure to claims for damages beyond the financial means of many small and medium-sized enterprises, and certainly start-ups. The resulting unintended adverse consequences for techUK's members, particularly of claims in the form addressed in Issue 2 below, include commercial pressure to settle such threatened litigation, loss of investment in UK technology businesses, and a weakening of the competitiveness of the UK sector against foreign rivals.

32. Moreover, this risk will affect data processors as well as controllers. There will necessarily be a number of data processors involved to support the platform operated by the data controller business, from the cloud service provider to email and CRM systems. Data controllers may face increased costs in engaging with data processors if the latter face increased risk from processing activities, or even the risk that they may not be able to engage processors at all if they are low-value prospective clients. This in turn may affect the ability of start-ups to enter the sector, impacting consumer choice.

33. Some of these pressures would exist whether or not a body had complied with its data protection obligations. But even if it had not, the body could face substantial sanction without the imposition of disproportionate liability for compensation. This is the role of the regime of financial sanctions under both the DPA 1998 and under the DPA 2018. Substantial monetary penalty notices

can be (and have been) issued by the ICO. The powers under the current legislation are extensive.

Misapplication of de minimis threshold

34. A further indicator of the problematic nature of the finding that "*loss of control*" is a form of damage is in relation to the threshold of seriousness applicable to claims under the Directive and GDPR. Before the Court of Appeal, it was or became common ground that a court would be entitled to refuse to make an award of compensation if it was determined that the claim was *de minimis.*

35. In *Vidal-Hall v Google Inc [2016] QB 1003* the Court of Appeal had described the threshold as applying when "*a case is not serious in terms of its privacy implications*", and that if not, "*that by itself is likely to rule out any question of recovery of compensation for mere distress"* at [82]. This orthodox approach might be understood to equate broadly to the Court of Appeal's statement here that, "*trivial loss will not attract compensation*" [44], focussing as it does on the consequences for the individual in question.

36. However, the Court of Appeal also made a number of conflicting (and, it is submitted, incorrect) statements about how the *de minimis* threshold is to be ascertained. In [43] it stated that the question was whether the "*infringement*" was "*trivial or de minimis*". This would appear to focus on the nature and abstract seriousness of the breach in question, rather than the consequences.

37. The Court also went further still in [55], stating that:

"*That threshold would undoubtedly exclude, for example, a claim for damages for an accidental one-off data breach that was quickly remedied. But that is far from this case. On the case pleaded, every member of the represented class has had their data deliberately and unlawfully misused, for Google's commercial purposes, without their consent and in violation of their established right to privacy*."

38. This would appear to suggest a range of circumstantial factors would be relevant to the issue of whether a claim reached the de minimis threshold, including whether "*for example*" the relevant breach of data protection

legislation was "*accidental*" or "*deliberate*", "*one-off*", "*for commercial purposes*", "*quickly remedied*". This is not a *de minimis* threshold at all, but an "all the circumstances" test of wide and uncertain ambit. As such, it is of little if any practical effect and unlikely to function as any filter to claims for loss of control damages, but rather it is likely to make it very difficult for techUK members to be able to predict with reasonable certainty whether certain risk might lead to more than *de minimis* infringement. In particular, it would not be known whether the threshold of seriousness had been reached until the litigation was advanced (potentially at a summary judgment stage or even at trial), and after the data controller had incurred substantial costs defending the action.

39. These problems also demonstrate the serious difficulty with the existence of a *de minimis* threshold if damages can be awarded simply for loss of control of personal data, without distress or damage. Loss of control is simply a fact that follows from, for example, a personal data breach. If it is treated as such, the question of whether or not it has occurred is binary and there is no room for an orthodox *de minimis* question.

40. If loss of control is not binary and a *de minimis* threshold does apply, its application cannot depend on the characteristics of the claimant as these are specifically disavowed by the Respondent[37]. If it is not going to become a multi-factorial test denuded of all meaning, its application can only then be determined by the quality of the affected data – what 'control' had been lost[38]. Even if it were possible to address this question without taking into account personal characteristics (which would seem impossible[39]), there is nothing in the Directive or GDPR to support the proposition that loss of control damages are available in respect of some breaches but not others.

[37] Court of Appeal judgment at [75].
[38] "*loss of <u>that</u> control must also have a value*" [47] (emphasis added)
[39] Factors such as the precise personal data affected must be material, which would undermine the conclusion reached by the Court of Appeal that each affected individual had the "same interest" for the purposes of CPR 19.6.

41. These difficulties strongly suggest that loss of control damages do not fit with a de minimis threshold (the existence of which is common ground). They further undermine the Court of Appeal's approach to Issue 2, addressed below.

Second Issue

42. Generally, legal proceedings may only be brought with the authority of the persons whose rights are sought to be enforced[40]. The Court of Appeal's approach to the "*same interest*" requirement in CPR 19.6(1), however, converts the rule into a previously-unrecognised generalised "*opt out*" collective procedure, with huge implications across many fields of litigation. techUK's submissions are confined to its impact in relation to proceedings for breaches of data protection legislation which could affect its members.

43. Both Parliament and Government have consistently elected not to implement an "opt out" collective procedure in respect of all forms of civil liability. It is submitted that it is only Parliament which can introduce such a procedure. However, the decision of the Court of Appeal cuts across the policy decisions that such a scheme should not be introduced, including in respect of data protection.

44. In 2009 the Government concluded that such procedures should be considered on a "*sector by sector*" basis and "*introduced only where there is clear evidence of need*." This was because "*there are potential structural differences between the sectors which will require different consideration*" and "*it will be necessary to undertake a full assessment of the likely economic and other impacts before implementing any reform*". Since that date Parliament has only enacted such a procedure, with detailed accompanying rules, in the field of competition law[41].

[40] *Mastercard Incorporated & Ors v Merricks* [2020] UKSC 51 per Lord Sales and Lord Leggatt (dissenting on the disposal of the appeal) at [92]
[41] Enacting the Consumer Rights Act 2015 ("CRA 2015") amending the Competition Act 1998 ("CA 1998") to introduce such a mechanism for claims before the Competition Appeals Tribunal.

45. Consideration has been given to the value of a similar procedure in data protection law. In 2013, the EU Commission published a recommendation[42] which recognised that "*protection of personal data*" was an area where "*the supplementary private enforcement of rights granted under Union law in the form of collective redress is of value*"[43]. The Commission noted that "*In order to avoid the development of an abusive litigation culture in mass harm situations, the national collective redress mechanisms should contain the fundamental safeguards identified in this Recommendation*" which included that "*The claimant party should be formed on the basis of express consent of the natural or legal persons claiming to have been harmed ('opt-in' principle). Any exception to this principle, by law or by court order, should be duly justified by reasons of sound administration of justice*".

46. Alongside this, work had begun to replace the Directive. The GDPR began with an EU Commission Communication dated 4 November 2010 which indicated that, while the core principles of the Directive remained valid, in light of technological developments and global shifts, it required revision[44].

47. The result was the mechanism for collective redress for data protection claims contained in Article 80 of the GDPR[45]. Article 80 prohibits bodies from seeking compensation on behalf of data subjects without their mandate. Recital (142) states in terms that "*That body, organisation or association may <u>not</u> be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate*" (emphasis added). Instead, Article 80 provides that certain "*not-for-profit*" bodies may be able to exercise other rights on behalf of data subjects

[42] European Commission (2013) Recommendation on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violation of rights granted under Union Law, 2013/396/EU.
[43] Recital (7)
[44] EC Communication 2010. The GDPR Proposal was issued on 25 January 2012, followed by a series of consultations and then the EU ordinary legislative procedure requiring agreement between the European Parliament and the Council of the EU.
[45] In the UK GDPR Article 80(2) is deleted on the basis that it is a permissive provision directed at Member States that is no longer material. The provisions of the DPA 2018 are materially unaffected.

without their mandate[46]; and to exercise rights on their behalf (including the right to claim compensation) *with* their mandate[47].

48. As Sorace[48] writes: "*Essentially, it was decided that the Regulation should not impose class action in the data protection litigation field*". This was precisely to "*avoid the development of a commercial claims culture in the field of data protection*"[49].

49. Article 80 had direct effect in the UK and in addition Parliament enacted sections 187 to 190 of the DPA 2018. Section 189 creates a duty on the Secretary of State to review and prepare a report for Parliament on a number of matters, including by subsections (2)(c) and (d) the following:

> "…(c) the merits of exercising the power under Article 80(2) of the GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise some or all of a data subject's rights under Articles 77, 78 and 79 of the GDPR without being authorised to do so by the data subject),
> (d) the merits of making equivalent provision in relation to data subjects' rights under Article 82 of the GDPR (right to compensation)"

50. Section 190(1) provided that after the relevant report was laid before Parliament, the Secretary of State may by regulations[50]:

> "(a) exercise the powers under Article 80(2) of the GDPR in relation to England and Wales and Northern Ireland,
> (b) make provision enabling a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise a data subject's rights under

---

[46] Article 80(2)
[47] Article 80(1)
[48] Sorace, "*Collective Redress In The General Data Protection Regulation: An Opportunity to Improve Access To Justice In The European Union?*" 7/2018 Working Papers Jean Bonnet Chair (2018), accessible at http://diposit.ub.edu/dspace/bitstream/2445/123425/1/WP_2018_7.pdf
[49] Statement of the Council's reasons: Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal C 159, 03/05/2016), para. 9.2.
[50] Under the affirmative resolution procedure: section 190(5)

Article 82 of the GDPR in England and Wales and Northern Ireland without being authorised to do so by the data subject…"[51]

51. Parliament therefore enacted provisions specifically to consider the merits of introducing an "opt-out" representative procedure for claims seeking compensation. This is unlikely to have been considered necessary or proportionate if such a procedure already existed under the civil procedure rules.

52. Pursuant to section 189, on 16 February 2021 the Government published a Report following a lengthy consultation process[52]. The Government concluded that "*Having considered the evidence, the government has concluded that there is not a strong enough case for introducing new legislation*".

> *"The current regime already offers strong protections for individuals, including vulnerable groups and children, and routes for redress. In the government's view, there is insufficient evidence of systemic failings in the current regime to warrant new opt-out proceedings in the courts for infringements of data protection legislation, or to conclude that any consequent benefits for data subjects would outweigh the potential impacts on businesses and other organisations, the ICO and the judicial system."*

53. In reaching this conclusion, the Government took account of a wide range of factors. This included that the ICO "*should be given space to regulate"* and Parliament was able to hold the ICO to account if it considers that the "*risk-based approach set out in its Regulatory Action Policy is not being implemented effectively*".

54. The Government also considered in detail the risks of further legislation. It was concerned that "*new legislation could increase uncertainty for data controllers*"[53]; that "*new legislation could increase litigation costs and insurance premiums during a period of economic uncertainty*"; and that "*Changes in the level of risk and a hardening in the insurance market could affect all data controllers, including those*

[51] Provision for the exercise of these powers is detailed in subsections (2) to (4) and includes a power to make provision about "*the assessment of the amount of compensation*" and "*the persons to whom compensation may or must be paid*".
[52] There were more than 300 written responses.
[53] Report, paragraph 1.5

with a good record of compliance"[54]. In its Call for Views the Government had also recognised that new legislation could lead to "*an increase in the number of speculative claims*"[55] [56].

55. These concerns are recognised and reflected in general observations about "opt-out" representative actions in *Merricks v Mastercard*[57], where Lords Sales and Leggatt refer to the "*risk that the enormous leveraging effect which such a class action device creates may be used oppressively or unfairly*" [98]; particularly given the involvement of "*commercial investors whose dominant interest is naturally to make money on their investment from the fruits of the litigation*".

56. The EU has also consistently rejected the creation of a regime providing for "opt-out" representative actions in respect of claims for data protection damages[58].

57. Each of the concerns identified above applies *a fortiori* to the "*scheme*" created by the Court of Appeal[59], the premise of which has been repeatedly rejected. As predicted, the scheme created will have serious adverse consequences for techUK members, in particular smaller businesses and high-tech start-ups. Merely the threat of litigation will discourage growth and investment in the UK by creating a more costly and risky environment for business operations.

---

[54] Report, paragraph 6.16

[55] "*Call for views and evidence – Review of Representative Action Provisions, Section 189 Data Protection Act 2018*"

[56] Although the Report at [2.6] and [6.17] referred to the Court of Appeal's judgment as demonstrating the "*potential for a form of representative action to succeed under existing rules*", this needs to be seen against (i) the Government's stated lack of confidence that a change to allow opt-out proceedings in data protection law was "*right*" (in [6.16]), and (ii) its overall conclusion that such opt-out proceedings were not justified.

[57] *Mastercard Incorporated & Ors v Merricks* [2020] UKSC 51

[58] The latest EU instrument, is Directive 2020/1828 on representative actions for the protection of the collective interests of consumers, which by Annex 1(56) applies to actions governed by the GDPR. Representative actions are limited to "qualified entities" who must have, inter alia, a non-profit-making character: Article 4(3)(c). The Directive states in recital (43): "*To best respond to their legal traditions, Member States should provide for an opt-in mechanism, or an opt-out mechanism, or a combination of the two*."

[59] None of the safeguards contained in the Competition Appeals Tribunal are replicated, for example.

58. These considerations were absent from the Court of Appeal's judgment, and, if properly taken into account, would or should have led the court to decline to interfere with the Judge's discretion to prevent the claim from proceeding as a representative action pursuant to CPR 19.6, or to exercising its own discretion in the same manner.

Conclusion: Consequences for UK Technology Sector

59. The consequences for techUK members are particularly severe when the Court of Appeal's conclusion in relation to Issues 1 and 2 are combined. In particular:
    (1) A hugely burdensome potential liability is created for the mere fact of a data breach irrespective of its lack of consequences. Coupled with the threat of substantial financial penalties being imposed by the ICO, this will inevitably lead to a significantly more risk-adverse approach across the technology sector, undermining the Government's strategy of encouraging the sector to promote economic and social benefits.
    (2) This risk averse approach will affect both business-to-consumer and business-to-business relationships. Data processors are likely to be more wary due to their own potential liabilities, with the result that the cost of necessary processing services will increase. Small or start-up enterprises with low revenues (including those outside the technology sector themselves) might be unable to obtain such services. Further, start-ups may be deprived of the ability to offer free data services (a key component of such new technology businesses), due to the increased risk of liability. A similar risk-averse approach is likely to be taken by potential investors, and foreign businesses considering establishing centres in the UK. It is also likely that insurance and associated costs will increase substantially.
    (3) The "*enormous leveraging effect*" of such litigation being brought under CPR 19.6 would transform the risk-profile even further, as individuals affected by the hypothetical infringement would not need to consent to the litigation. Compensation could be sought on their behalf by third parties acting in their own commercial interests even if the individuals themselves

were "*indifferent*" to what had taken place, or even "*quite happy*" and "*would have consented if asked*"[60].

(4) Commercial pressures to settle litigation (or threatened litigation) would be substantial, even if data controllers or processors were advised that they had complied with their safeguarding obligations under the Directive or GDPR. The financial risk of losing any such action would be enormous.

(5) The competitiveness of the domestic technology sector would be undermined if the UK adopted a different approach to other jurisdictions. Neither the definition of damage used by the Court of Appeal nor the existence of an opt-out mechanism are necessary under EU legislation and jurisprudence. A different approach could moreover lead to substantial trade barriers and inhibit or prevent the free flow of data.

60. These are severe consequences which were not taken into account by the Court of Appeal. The Government warned in its NDS that data has the ability to "*affect the structure and competitiveness of entire markets*". The Court of Appeal considered small parts of the complex framework for data protection in isolation, without taking into account the impact that they may have on the whole.

61. For the reasons set out above, techUK respectfully submits that the Court of Appeal erred in its conclusions in relation to both Issues 1 and 2. techUK respectfully submits that the appeal should be allowed.

catrin evans

CATRIN EVANS QC
IAN HELME
MATRIX CHAMBERS
19 April 2021

[60] Judgment at first instance of Warby J at [74].