Submissions to DCMS on Review of Representative Action Provisions, Section 189 Data Protection Act 2018

I. INTRODUCTION

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the UK Department for Digital, Culture, Media & Sport (DCMS)[2] Consultation on the Review of Representative Action Provisions under Section 189 of the Data Protection Act of 2018 (DPA). Our remarks primarily focus on specific questions that we feel we are in a position to address and that are most pertinent to CIPL member companies, namely:

- With regard to actions brought with authorisation:
    - Q10. "What, if any, impacts might the provisions discussed in Chapter 2 have had on data controllers which might be the subject of a complaint or legal claim, particularly businesses, including any increase to compliance and other costs, or risks? Please explain."
    - Q11. "What, if any, impacts might the current provisions have had on the ICO and the judicial system and their capacity to handle claims? What, if any, measures might help to manage pressures?"
- With regard to actions brought without authorisation:
    - Q12. "Do you think the data protection legislation should be changed to allow non-profit organisations to act on behalf of individuals who have not given express authorisation? Please explain whether and why to permit such action in relation to the exercise of some or all of a data subject's rights."

II. CIPL COMMENTS

1. <u>The Expansion of Existing Rights of Redress to Include Unauthorised Actions is Unnecessary and May be Counterproductive</u>

    - **No clear benefit to expansion and the existing redress options are working**: There appears to be no clear benefit to extending existing rights of redress and we suggest that such extensions should only be considered where there is clear evidence of benefit. Currently, individuals may exercise their rights and seek redress using several means, including bringing

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] DCMS: Call for views and evidence - Review of Representative Action Provisions, Section 189 Data Protection Act 2018

an individual claim in the High Court (Queen's Bench Divisions, Media and Communications List), opting in to a group action, or opting out of a representative action. These avenues for redress are robust and in regular use, and are increasingly prominent in terms of their press coverage. These existing avenues are setting a standard for protection of data subject rights globally, putting data subjects front-and-centre with respect to control over their own personal data, and empowering individuals to hold organisations to account. It is right that individuals drive such accountability wherever possible, rather than delegating such responsibility to organisations to act on their behalf. Where such delegation is required or preferable, privacy activist organisations such as Privacy International and NOYB are increasing in prominence and are already regularly representing the interests of individuals and having a dramatic impact on the data protection market, as evidenced by the recent judgment in *Schrems II*.[3] It is clear that these existing avenues are therefore sufficient for the purposes of representing individuals, and that representative actions should be a last resort for those individuals not able to make full use of the rights afforded to them under data protection law. The addition of a multitude of third party funders to this ecosystem would be an unnecessary complication. It is also notable that in some cases those that provide for group actions already encourage or facilitate the threat or launch of unmeritorious claims, which would likely be exacerbated if additional legal routes were added.

- **Expansion would divert resources from investment in compliance programs**: The avenues of redress outlined above, particularly those by which data subjects directly enforce their rights, are better served by proactive facilitation of such rights through internal investment. The more resources are spent fighting and settling representative actions, the less capacity organisations have to invest in improving their internal accountability procedures, complaint handling processes, and other infrastructure for ensuring transparency and communicating directly with data subjects. Proactive investment in compliance programs is likely to offer a more effective mechanism to achieve the aims of the GDPR and DPA than legal action taken up following a singular incident.

- **The Information Commissioner's Office (ICO) is an active and experienced regulator and is well set-up to receive and resolve a variety of complaints by data subjects**: Data subjects are afforded various rights under existing data protection law, and are able to enforce those rights, including by submitting complaints to the ICO. The ICO is best placed to deal with such complaints having been a proactive and responsive regulator for many years, since before the introduction of the GDPR and the DPA. The ICO has issued various fines since May 2018. Overall in the year 2019/20, the ICO stated that it took regulatory action in 236 instances in response to breaches of the legislation it regulates.[4] During the same year it conducted over 2,100 investigations and resolved 39,860 data protection complaints cases. Further, in relation to protecting the rights of children specifically, the ICO has sought to achieve industry-wide change, publishing its Age Appropriate Design Code which establishes design standards for online services that target children.

  We believe that the ICO possesses the relevant expertise and tools to take appropriate enforcement action to safeguard individuals' rights. The ICO issues guidance to organisations explaining how data protection requirements should be implemented and met, and is best placed to assess whether its guidance has been followed in individual cases. In addition, the ICO is able to review shortcomings with organisations and provide guidance as to how data

[3] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18).
[4] ICO: Annual Report 2019-20 - this included 54 Information Notices, eight Assessment Notices, seven Enforcement notices, four cautions, eight prosecutions and fifteen fines.

protection practices can or should be improved. Ultimately, this process is likely to result in faster, more consistent and more effective data protection for both the organisation and the data subject than a protracted and costly legal process. Data subjects are already well served by a regulator that actively enforces their rights.

Finally, the ICO is only in the early stages of exploring the new powers afforded to it under the DPA. Time is therefore needed in order to judge the effectiveness of the ICO's enforcement before the rights of less experienced organisations are expanded. In addition, it should be for the ICO, and legislators, to determine enforcement priorities with respect to the data protection sphere. When representative actions focus solely on those areas likely to reap the greatest settlements or damages, such as data security breaches, this will likely lead to other areas of compliance programs, such as infrastructure around facilitating data subject rights, being neglected in terms of resources and investment. While the ICO has made clear that it will be pragmatic and take a risk-based approach, focusing on those practices that present the most risk to individual data subjects, there are no such assurances from the litigation sector. In the long-term, this will lead to more reactivity, rather than proactivity, from the perspective of organisations with respect to data protection, which in turn will lead to worse outcomes for data subjects. The ICO is better placed to direct organisations' attention to those areas of compliance that require the most attention, both at a specific business level, and more generally by "agenda-setting" (for example through publishing guidance that establishes good practice).

- **Existing remedies and rights of redress should be afforded time to become established before expansion is considered**: Some of the legal avenues discussed above are still relatively new. Nonetheless, data subjects and organisations acting on their behalf have already utilised them to launch numerous actions. As commented in the Class Actions Law Review: "the combination of increased protection of personal data rights as a result of the GDPR, the Cambridge Analytica scandal and the decision in *Lloyd* means that data breaches are likely to be a key growth area for class actions in future."[5] The same publication comments that the past five years have seen the group litigation sector undergo rapid development and expansion. It is essential that we allow time and an opportunity for the system to work fully and to evaluate how these existing avenues are utilised, how effective they are, and what additional remedies might be required, before expansion is considered. The Call for Views and Evidence notes that the uptake of representative actions has been low to date.[6] We would suggest that this is due to the fact that we are still in the early days of the implementation of the new regime. Also, the other avenues of redress (such as individual complaints – the ICO state that they received 38,514 data protection complaints in 2019-20, and 41,661 in the prior year)[7] have proved appropriate and sufficient for the requirements of data subjects thus far.

- **The suggested expansion of existing remedies and rights of redress to include unauthorised actions goes beyond the scope of the GDPR**: While the GDPR provides for non-profits to exercise the rights to lodge a complaint with the supervisory authority and seek a judicial remedy on behalf of individuals, it does not envision, under Article 80(2), the right for non-profits to exercise the right to compensation on behalf of data subjects that have not provided authorisation. Such an expansion would go beyond the scope of the GDPR's provisions. Indeed, while Recital 142 allows for the possibility that Member States might enable not-for-

[5] Class Action Law Review, Edition 4

[6] DCMS: Call for views and evidence - Review of Representative Action Provisions, Section 189 Data Protection Act 2018

[7] ICO: Annual Report 2019-20

profit bodies to bring representative actions without a data subject's mandate, it specifically states that they "may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate."

- **There are more appropriate, alternative forms of redress that should be considered**: If additional or alternative forms of redress are to be explored, we believe that certification bodies, or an ombudsman, would be more appropriate tools for the outcomes that are being sought. Data protection certifications and codes of conduct are already envisioned in the UK GDPR and we know that there is considerable interest among organisations to make full use of and develop these accountability tools further. Codes of conduct will entail monitoring bodies with certain oversight functions, which could include dispute resolution and complaint handling functions and the ability to sanction member organisations for non-compliance with the code. Article 40(2)(k) GDPR specifically provides that such codes may provide for out-of-court proceedings and dispute resolution procedures. Such procedures could be similar to those operated by the Financial Ombudsman Service or the Independent Press Standards Organisation.

  Similarly, the certification provisions in the UK GDPR could potentially be developed to afford analogous provisions. Code and certification bodies would have the requisite expertise, and would act without an agenda other than enforcing their code or certification in taking action against organisations (unlike some non-profits, as discussed below). They would also have a broader, holistic overview of data protection issues, being well placed to act more swiftly, and more consistently over time and across issues. Courts may lack this ability at times, as they are presented with isolated issues relevant to separate claims, and cannot have a proactive role in identifying non-compliance. They also do not have the benefit of everyday experience that would allow them to identify trends and patterns over time and consult with stakeholders in the same way as regulatory bodies, certification bodies, monitoring bodies, or ombudsmen. Such expert bodies may therefore be better placed than the court system to understand the seriousness of a data protection breach or an act of non-compliance and accordingly determine appropriate remedies or assess damages.

  The more these codes and certification bodies (as well as organisational internal complaint handling mechanisms in general) provide a more productive and streamlined alternative to dispute resolution than litigation, the more likely organisations will be to invest in *ex ante* accountability, including through such formal mechanisms and organisational compliance and accountability programs generally, thereby decreasing the need for a litigious *ex post* approach to compliance.

2. <u>Gratuitous and Excessive Use of Data Subject Rights and Unmeritorious Claims Leading to Litigation</u>

- **Current exercise of data subject rights is frequent, extensive and, at times, burdensome**: The purpose of the data subject rights under the GDPR is to ensure that individuals are empowered in relation to processing of their personal data and have some level of control over it, including to remedy inaccurate, obsolete, or other unsuitable processing.[8] The

[8] Note GDPR Recital 2: "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should…respect their fundamental rights and freedoms, in particular their right to the protection of personal data". Note also Recital 39: "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and

experience of the first two years of the implementation of the GDPR shows that on occasion, these rights have been used excessively and gratuitously, and even for purposes entirely unrelated to data protection, and not envisaged by data protection law (for example, a request for access to CCTV footage that might assist with an insurance claim). Organisations have previously reported that in a significant number of cases (more than 50%), requests to exercise rights are entirely speculative.[9] In addition, various exemptions in the DPA limit the scope of data subject rights, which are often not well understood by data subjects. Each request requires that organisations dedicate time and resources to evaluating the request and responding appropriately. Organisations are already finding that dealing with such requests is creating a significant burden, even where an exemption applies to much or all of the data requested, as each piece of data must be assessed and the reasons for not complying, partly or fully, with the request must be explained to the requestor.

- **Litigation should not be encouraged as the next step for unsatisfied data subjects**: Because data subjects are often not fully appraised of the limitations on their rights under data protection law, and the exemptions that may have been reasonably and legitimately applied to a request that they have made, they are often left dissatisfied by an organisation's response. Any claim based on such dissatisfaction would be unmeritorious, and ultimately fruitless for the individual. At present, data subjects are able to complain to the ICO when their requests are not fulfilled to their satisfaction. We believe that this is the right avenue, as the ICO is well placed to assess the legitimacy of such complaints. Often the ICO redirects complaints back to the organisation itself, often with guidance as to how the complaint may be resolved. Ultimately this approach is more likely to lead to a satisfying result for the data subject and, importantly for future compliance, an improvement in an organisation's policies and procedures for dealing with data subjects' rights. In addition, as discussed, once there are certifications and codes of conduct in place, the monitoring bodies and certifiers may be able to take on a complaint handling and dispute resolution role as well.

  Even where they would be justified in applying an exemption, there are already examples of organisations being put under significant pressure to respond fully to data subject requests or action them in their entirety, for fear of requestors potentially commencing litigation if not fully satisfied. This requires disproportionate use of resources in tracking down and disclosing unnecessary information, and cumulatively this can have a substantial impact on the resources of organisations, particularly where an organisation is small, or a non-profit.

3. Encouraging Spurious Claims and Facilitating Unnecessary Third Party Service Providers

- **Representative actions are often not motivated by the enhancement of data protection**: The UK may not want to encourage the US approach of activist organisations actively seeking out cases to bring for profit motives rather than for the benefit of individuals. Generally speaking, we find that not all representative claims seek to enhance the protection of the relevant data subjects under data protection law. This is in contrast to actions initiated by privacy activists, who generally seek to enforce and enhance data protection standards. As the Call for Views

---

communication relating to the processing of those personal data be easily accessible and easy to understand…That principle concerns…further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing."

[9] CIPL: White Paper: "Data Subject Rights under the GDPR in a Global Data Driven and Connected World"

and Evidence emphasises, the representative action provisions in the GDPR "are designed to help individuals who may not have the capabilities or resources to exercise their rights effectively on their own."[10] Instead, the experience of global organisations suggests that representative claims may be launched primarily for the purposes of financial gain (either through an award of damages or by pressuring an organisation into a financial settlement), or to harass organisations undertaking processing activities that the claimants are adverse to, regardless of whether or not such activities are undertaken in a manner that complies with data protection law. The use of biometric data is a good example of the latter. Representatives may dislike new technologies, focussing primarily on the risks of data use while ignoring the benefits to individuals and society. The addition of litigation funders, who are motivated by financial return may lead to additional pressure on both organisations and the court system, which must deal with a case lacking in merit that in other circumstances may not have been launched.

In fact, the representative action market is already advertised as an "investment opportunity" through litigation finance, offering a share of settlements or awards in return for investments of tens of thousands of pounds. Through this market, entirely disinterested investors provide funds for law firms to pursue consumer claims which, as noted in the advertising material for one such finance provider, increase during recessions. Not only does this clearly not pursue the aims of data protection for individuals envisaged by the GDPR, it also encourages investment in a relatively new and risky market (with respect to data protection-related actions) and encourages the funding of litigation without any assessment of the merits of such actions by those funding it. Such practices also encourage non-profits and lawyers bringing claims to seek the greatest possible return for their investors, rather than focus on the actual damage suffered by the relevant class. Further, where such markets have expanded in other sectors, such as financial services, CIPL members have found that the conduct of claims has largely been aggressive and unproductive, even where the claims themselves have legitimate bases. For example, in May 2019 the ICO fined one organisation £120,000 for sending 3,560,211 direct marketing text messages relating to PPI compensation claims. More than 1,300 complaints were made by the recipients of these messages.[11]

This US-style litigation market is expanding in the EU, with US firms opening branches in the UK and advertising for claimants to join in class actions. On opening its Liverpool branch, a founding partner of one firm commented: "We want to bring the "US approach" to group litigation to our UK clients".[12] The EU and especially UK are regarded globally as having a data protection regime with comprehensive, enforceable individual rights that is setting a precedent for many other jurisdictions. The expansion of an aggressive litigation finance market within the data protection sphere, as a market operating purely for its own financial purposes, risks undermining the reputation of the EU and UK as jurisdictions that treat the interests of individuals, and their fundamental rights with respect to data, as paramount. Finally, and importantly, this may also be detrimental to the competitiveness of the UK market and the UK inward investment, especially from January 1, 2021, when the Brexit transitional period ends (as discussed further below).

- **Unwarranted reputational damage may be caused**: As well as the resources and potential costs involved in an unmeritorious claim, organisations also suffer serious reputational

[10] DCMS: Call for views and evidence - Review of Representative Action Provisions, Section 189 Data Protection Act 2018

[11] ICO fines PPI claims company £120,000 for millions of nuisance texts

[12] Law Society Gazette: "Liverpool mayor hails ambitious offshoot of US class action firm"

damage when representative actions are launched. These actions are generally very well publicised, and likely to result in a fall in customer confidence. If these claims are launched without an unbiased assessment of their merit, such as by an independent ombudsman or monitoring or certification body, as discussed above, and later prove to be unwarranted or even vexatious, there is little that can be done to reverse the reputational damage suffered by organisations.

- **Representative bodies may lack expertise**: Organisations that bring representative claims may lack the requisite specialist knowledge of data protection to assess the merit (or lack thereof) of the claim. This can result in wasted resources, both from court resources and resources of the organisation defending the claim.

- **Third parties sometimes seek to benefit from the data protection regime**: In the wake of the GDPR's introduction we have seen organisations attempt to provide "services" purportedly allowing individuals to exercise their rights more easily, such as by submitting access or deletion requests on their behalf. Not only is this not required – the GDPR requires that organisations facilitate data subject requests (and a complaint may be filed if they do not) – but it misleads individuals as to the nature of their rights and the limitations on them. This adds an additional administrative burden both to organisations, which may be required to verify the identity of both the third party and the requestor, and to individuals themselves, who need to verify that the request originated from them. These requests may also come from a no-reply e-mail address that make it impossible for the controller to ask further questions, for example, to verify identity or the individual's location so as to establish that they fall within the scope of the GDPR's protection, or to clarify the scope of a request. Again, this diverts or uses resources that could be better invested in compliance activities. Relationships and communications between organisations and data subjects are often most efficient and productive when they do not involve a third party.

- **Organisations and data subjects should not be cast as adversarial**: It is unhelpful for organisations processing personal data and data subjects to be cast as adversarial parties, which these third party "service providers" or representatives sometimes encourage. The use of personal data should be for the benefit of the data subject as well as the organisation, and a symbiotic relationship between the two results in greater transparency, leading, in turn, to better data literacy for data subjects. Where data subjects are able to understand how their data is used, and what their rights are, there will be less pressure on organisations, the ICO and the courts.

- **Standards should be put in place for representative bodies**: We believe that minimum standards should be established for bodies that are able to bring these claims, to encourage sensible practices and discourage speculative actions. Only trusted, regulated and experienced organisations should be responsible for bringing claims, and claims should be led by those with a vested interest in the outcome from a data protection perspective. This reflects the GDPR's intention under Recital 142 that non-profits with a mandate to lodge complaints on behalf of data subjects have "statutory objectives which are in the public interest" and that the organisation be "active in the field of the protection of personal data", as well as the requirements under Section 187(3) of the DPA that any such body have "by virtue of its constitution… objectives which are in the public interest". Any expansion of the rights of redress under UK law must include strict vetting criteria to evaluate qualifications for the formation of such bodies and their authorisation to bring representative claims.

For example, there could be a requirement that only organisations that have been established for (say) five years and with a proven track record in the relevant area should be permitted to represent such claimants. Where organisations purport to act on behalf of children, the relevant criteria should be more stringent. Also, the non-profits working in this space should have the appropriate CAT qualifications for consumer complaints under the CAT Rules 2015, in particular Rule 78 (Authorisation of the class representative) and Rule 79 (Certification of claims)) and also be qualified entities under the proposed EU directive for collective redress.[13] Regulating such organisations would be an additional burden for the ICO. Also, there should be a process by which the merit and seriousness of claims is determined outside of the court system prior to commencement, as well as whether or not they are duplicative, to ensure that the courts are not overwhelmed with unnecessary claims. Finally, court claims could be subject to preliminary certification to ensure that only meritorious claims can proceed.

The advocacy community is still in its infancy within the data protection sphere. Accordingly, to the extent that there is any expansion in the power that it wields, there should be a robust and extensive debate as to who within the community should be entrusted with such power and the safeguards that should be put in place to ensure that it is used responsibly, particularly with regard to the level of transparency that is required with respect to litigation funding.

4. Stifling Digital and Data Innovation and Growth in the UK

- **Data use plays a significant role in innovation and economic and societal growth - unmeritorious litigation threatens innovation and the competitiveness of the UK**: The value of personal data in innovation and technical progress is well understood, including by DCMS's consultation on the UK National Data Strategy, which states: "Data is an incredibly valuable resource for businesses and other organisations, helping them to deliver better services and operations for their users and beneficiaries."[14] If organisations are subjected to unmeritorious representative actions, this is likely to encourage three types of behaviour that would undermine innovation and effective and beneficial use of data in the UK, leading to loss of competitiveness and inward investment:

    - Concentration of resources and data processing activities outside of the UK due to increased costs of business, depriving the UK of the benefits to be reaped from such activities. Given the growth of group actions in the UK and their increasing sophistication, any expansion may result in businesses choosing to concentrate their EU operations in a less litigation-heavy environment;

    - Processing data in the most conservative manner within the range of behaviour permitted by data protection law – "risk reticence". For example, it is well understood that, when developing artificial intelligence systems a balance is required between the data minimisation principle and the need to train the system using large amounts of data. This balance is essentially between the rights and protection of the data subject and the realisation of the full potential of the AI. Organisations are already exploring how best to strike this balance. However, in a litigious environment, organisations may retreat from more innovative data processing activities in an effort to avoid potential complaints. As a result, the UK would likely fall behind other

[13] Article 4, Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC
[14] DCMS: UK National Data Strategy Consultation

countries where organisations are freer from the fear of vexatious complaints. This is particularly true for SMEs, many of which have a business plan that is entirely dependent on the use of personal data, leaving them greatly exposed. While larger organisations may be able to weather the storm of a representative action and its associated costs and reputational damage, SMEs will rightly fear that one action, even if proven, ultimately, to be spurious, could put them out of business. DCMS has recognised the value of SMEs in its 2019 SME Action Plan, stating: "SMEs are vital to the UK economy, driving growth, opening new markets and creating jobs, therefore their contribution is vital. As the source of innovation, they encourage competition and bring fresh ideas that challenge the status quo."[15] SMEs need to be protected from unmeritorious litigation. This reputation of the UK as a "world leader in technological innovation" (according to DCMS) would be put at risk if organisations were incentivised to avoid innovative data processing activities, even where they were compliant with data protection law.

  - Organisations become less transparent with regard to their data practices. Thus far, the ICO has found that organisations are more likely to over-report breaches and non-compliance than under-report, in an effort to remain transparent. In an environment with heightened litigation risk, this transparent behaviour would likely decrease.

- **Resources should be directed towards responsible and innovative data use, not unnecessary litigation**: Aside from the behaviour discussed above, the costs associated with greater exposure to litigation and regulatory burdens adds greatly to the cost of business, diverting resources from investment in growth and innovation, again limiting the capacity of UK organisations to compete in the tech market. Organisations are already in the habit of setting aside finance for potential regulatory fines – if they are also required to budget for costly legal proceedings this soaks up further capital that would be better invested in proactively developing data protection compliance programs. The increase in the cost of business will also stem from the increased cost involved in doing business with third parties, for example negotiating with respect to liability for such claims. In an increasingly complex data ecosystem, these types of additional burdens are likely to create even more uncertainty for businesses. In addition, as the cost of business increases, it will again be SMEs that are hit hardest, and many are likely to be driven out of the market before they can even gain a foothold. This would also come at a time when the UK needs to be more focussed than ever on growth and job creation. Ultimately organisations should be investing in proactive and pre-emptive data management and privacy compliance programs that include privacy impact assessments, privacy by design and policies and procedures designed to deal with individuals' requests. They should not direct important and scarce internal resources to dealing with representative actions.

5. Unauthorised Representative Actions Do Not Enhance, and Risk Undermining, Data Protection

- **Class actions often do not truly benefit individuals**: The nature of representative claims, and the large pool of claimants involved, are such that individuals may gain little financially, even where the claims are successful. In addition, because these actions require that all claimants must have suffered the same loss, the damage claimed will generally be the least serious loss suffered among the claimants, as this is the only common loss among all participants in the class (the "lowest common denominator" approach). This means that those who have

[15] DCMS Small and Medium Enterprises Action Plan

suffered more substantial loss may be required to settle for a lesser sum than they would otherwise pursue. This does not achieve the aims of the representative action provisions under the DPA, which are intended to compensate data subjects for their loss. As this issue exists already with regard to authorised representative actions, it would likely be exacerbated in actions run entirely without the involvement of data subjects.

- **Representative actions do not permit a true assessment of the loss suffered**: It has been established in the case of *Lloyd v Google*[16] that "loss of control" over personal data may constitute a form of loss for which damages may be recoverable. However, this does not mean that loss of control over data is directly comparable to economic loss. The latter is objective and measurable and is suffered in the same way by all claimants (though the extent to which it affects each of them may differ). Loss of control over data is more subjective – while some individuals may feel greatly damaged, others may consider such loss of control to be simply a part of the dynamic of engaging with the digital environment, and a necessary trade-off for the benefit of using the relevant services. Any claim brought should be rooted in a real, specific and identifiable harm suffered by the data subject, but often representative actions do not permit a true assessment of the damage caused to data subjects. As such, in many cases an individual claim or a complaint to the ICO is a more appropriate avenue of redress for an individual than a representative action. This is an issue that would be exacerbated by the introduction of unauthorised representative actions that involve no communication with the data subjects involved.

- **Unauthorised representative actions will likely include "phantom claimants"**: Because of the low threshold for establishing common loss discussed above, and the motivations created by an investment market for litigation funders, representative actions are likely to include a number of "phantom claimants", included despite having no interest in the complaint or its outcome. Those bringing representative claims are incentivised to include such phantom claimants in order to generate the largest reward/settlement possible.

- **Data subjects should retain control over the enforcement of their own rights**: If the view that "loss of control" over data is a loss worth compensating from the perspective of a data subject is accepted, it would follow that data subjects themselves should have control over any consequential claim, rather than having it conducted on their behalf and without their knowledge. The GDPR and DPA envision data subjects taking control of their data via its provisions, not having third party organisations determine for them how and when they should enforce their rights. If data subjects are to have the choice to enforce their rights, the choice *not* to enforce their rights should equally be left in their hands. If they choose not to directly enforce their rights against an organisation through the existing avenues discussed, their choice *not* to engage in litigation should not be taken away.

- **The focus should be on better publicity for, and facilitating use of, existing mechanisms before expanding avenues of redress for data subjects**: Rather than encouraging the creation of new grievance processes (other than through codes of conduct and certifications or the establishment of competent ombudsmen) the focus should instead be on providing clarity to individuals regarding their rights under data protection law, and the limitations on those rights. The data subject requests that organisations commonly receive are driven, in part, by

[16] *Lloyd v Google LLC* [2019] EWCA Civ 1599

the public's lack of understanding of data uses and by a variety of GDPR myths.[17] Focusing on clarity and facilitating better use of existing avenues of redress would relieve the pressure on organisations from unmeritorious claims and requests, and allow for a more productive relationship between organisations and data subjects, with the aim of avoiding unnecessary litigation in the future.

6. Nudge Theory is More Effective than Punishment and Deterrence

- **Enforcement and monetary damages should be a last resort**: The ICO is a pragmatic regulator and works with organisations to enhance data protection practices, for example by encouraging organisational accountability, taking a risk-based approach to oversight and enforcement and treating enforcement actions as a last resort. This cooperative approach enables organisations to continue to conduct their everyday business without the fear of looming court deadlines and, if appropriately responsive to the ICO, to avoid or reduce a fine by moving their practices into compliance with the ICO's requests. This approach allows organisations to identify where they are going wrong and to fix it. There is no such incentive in a court process. In fact, in a representative action organisations are incentivised to justify their data protection practices in order to argue their case, whereas in a more collaborative process they may admit that such practices fell short of the requirements of the law. This limits the capacity of organisations to learn and progress.

- **The focus should be on learning, not punishment**: The GDPR and its implementing legislation are relatively new, and guidance on compliance is still being published by regulators, demonstrating that implementation has not always been straightforward with respect to every one of its provisions. It is important that organisations are given time to develop their compliance programs, for which they will often need the guidance of regulators like the ICO, since many are likely to face stumbling blocks along the way. The threat of litigation for every shortcoming in compliance, regardless of the efforts taken to comply, has the potential to severely disrupt business operations.

  A cooperative approach between organisations and regulators should instead be encouraged, as it will lead to more responsible data processing, transparency and innovative data use. CIPL understands that organisations are less likely to volunteer information where they fear attracting criticism or blame, so an "open culture" of sharing and questioning should be encouraged rather than an adversarial relationship with regulators and the courts, except where there has been serious wrongdoing. The model of deterrence through punishment is outdated in the modern-day digital economy and, as CIPL has commented in the past: "A great deal of research now endorses "responsive" regulation where the emphasis is on engagement through information, advice and support rather than deterrence and punishment."[18] In fact, smart regulation should proactively encourage and reward good behaviour and organisational accountability, thus enabling the race to the top in the marketplace and achieving better outcomes for both individuals and the organisation. There is potential for this open culture to be undermined if growth of a litigation market is encouraged, particularly where non-profits and third party litigation funders use investigations undertaken by the ICO as a springboard to commence group actions.

[17] CIPL: White Paper: "Data Subject Rights under the GDPR in a Global Data Driven and Connected World"
[18] CIPL: "Regulating for Results: Strategies and Priorities for Leadership and Engagement"

III. CONCLUSION

In CIPL's view, the existing avenues of legal redress open to individuals in the data protection and litigation market, while still relatively new, are proving sufficient, and there has been significant activity from data subjects directly exercising their rights, and from organisations instigating group actions, since May 2018. Any expansion of these avenues should be undertaken only where there is compelling rationale, such as where there is evidence that a particular group of individuals is not sufficiently provided for. There is a significant risk that such expansion would not only encourage the growth of an aggressive litigation market, funded by those with little or no interest in upholding data protection law principles, but would also undermine the reputation of the UK as a jurisdiction with high standards of data protection for individuals, and as a competitive and innovative force within the EU and global market.

Individuals stand to benefit most from actions taken by pragmatic regulators with the experience required to understand the nature of the damage done, and to take proportionate action, rather than parties motivated by financial gain. If additional avenues for legal redress are to be explored, there are various alternative mechanisms that would likely provide more meaningful redress to individuals, in line with the intention of data protection law provisions, than unauthorised representative actions would be able to.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Bridget Treacy (btreacy@hunton.com); Markus Heyder, mheyder@huntonAK.com; and Olivia Lee (olee@hunton.com).