2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Data Protection Team
Department for Digital, Culture,Media & Sport
4th Floor
100 Parliament Street
London
SW1A 2BQ

21 October 2020

Which? Response to the Call for Views and Evidence for the Review of the Representative Action Provisions in Section 189 of the Data Protection Act 2018

Which? welcomes this opportunity to submit its views and evidence to the Government for the statutory review of the Representative Action Provisions, Section 189 Data Protection Act 2018.

Which? has been interested in this area for a number of years and welcomed the introduction of the provisions in question in its submission of evidence to the Committee for the Data Protection Bill. Which? continues to seek the implementation of Article 80(2) GDPR and the measures that would better enable consumers access to redress. **Access to adequate redress is a necessary consumer right in the data space and Which? believes there is a compelling need for better provisions**.

In order for the Government to achieve its stated objectives of ensuring that the UK is the 'best place to start and grow digital business, trial new technology and undertake advanced research', a collective redress mechanism on an opt-out basis needs to be introduced for breaches of the data protection principles, including significant data breaches. This will aid in creating an environment where data subjects have confidence in the way that organisations are using their data and are assured that there are processes in place to protect their rights if something goes wrong.

Summary

1.) Which?'s position is informed by our expertise of working in consumer protection. Adequate redress mechanisms for data breaches are needed in an economy and society fueled by data.

2.) The current 'opt-in' system is not working to adequately serve consumers who suffer at the hand of data breaches and business practices that breach data protection principles. This is evidenced by the low uptake of the current provisions. A fundamental reason for this, is that the current model presupposes that affected consumers are aware that their data has been breached, that they know their right to appoint a representative body, and that they see the value in expending time on such an appointment in circumstances where the individual harm suffered may seem relatively small even though it may have had a much greater collective impact.

3.) Data breaches have and are continuing to happen with consumers suffering real harm as a consequence but without having access to the redress they deserve. Multiple high-profile data breaches have occurred in the years since the introduction of the legislation. Which? recently published an investigation which showed the real-life impact data breaches can have on consumer lives[1].

[1] The Human Cost of Data Breaches
https://www.which.co.uk/news/2020/09/data-breaches-how-your-personal-details-end-up-in-the-hands-of-criminals/

4.) More needs to be done to hold businesses to account when they do not adequately protect consumers' data or engage in business practices which contravene the data protection principles - more needs to be done to incentivise them to improve their data processing practices. Facilitating redress through an opt-out mechanism would be a complementary method to incentivising good practice alongside existing measures. Which? recently published an investigation which found that a number of major travel companies who have been the subject of major data breaches were still failing to protect their users and had serious data security vulnerabilities on their websites[2].

5.) We have seen the introduction of opt-out mechanisms in other areas of consumer protection - an opt out collective redress regime for competition law claims was introduced by the Consumer Rights Act 2015 and has not led to a wave of spurious claims. Data protection is well-suited to this kind of redress mechanism due to the nature of the harm suffered. It often affects a vast number of consumers with relatively small individual harm and large collective impact.

6.) Which? envisages a proportionate and effective system of collective redress that incorporates appropriate safeguards to ensure the system works in the interests of consumers, companies and the courts alike.

Our Readiness

Should the statutory review result in the introduction of opt-out representative action provisions, allowing not-for-profit organisations to bring actions on behalf of consumers, Which? is well prepared for this responsibility and the practicalities of this mechanism. As a not-for-profit organisation with the necessary expertise, resources and safeguards in place, Which? would be well placed to bring meritorious cases where deemed necessary to seek the redress consumers deserve for detriment suffered as a result of infringement of their data rights.

GDPR specifies the type of organisations that are currently able to be mandated to bring representative actions on behalf of data subjects and this specification would also apply should the provisions be extended to implement Article 80(2) GDPR to allow for opt-out representative action. Organisations wishing to represent consumers would have to meet this specified criteria. Only not-for-profit organisations who are acting in the public interest, and who actively work in the area of the protection of data subjects' rights, would qualify to bring a case. Which? considers itself to be such an organisation that meets this criteria and we are well prepared and ready for the practicalities of what these powers would entail.

Which? is the trading and brand name for the Which? Group, wholly owned by the Consumers' Association. The Consumers' Association is a registered charity and its trustees are charity trustees and company law directors. The Council of Trustees of the Consumers' Association is the ultimate governing body of Which? and is responsible for the achievement of our charitable mission and the continued success of Which?.

Which? works in pursuits of its charitable objects for the public benefit. One of which is promoting and improving knowledge and understanding of laws, regulations, public policies and business practices so as to empower consumers in their everyday lives. We also work to promote and improve life skills including those relating to personal finance, digital and technology, horticulture and the home. Another of our objects is to uphold and promote compliance with consumer laws, regulations and public policies in particular through the exercise of its statutory powers for the benefit or protection of the rights of consumers. We work to protect and promote the safety of consumers and to promote the interests of consumers who are restricted from accessing or using goods, services or data because of their youth, age, ill-health, disability, financial hardship or other disadvantage.

[2] Can Travel Websites Keep Your Personal Data Secure?
https://www.which.co.uk/news/2020/09/marriott-british-airways-and-easyjet-fail-on-data-security-with-hundreds-of-security-risks-exposed-by-which/

Which? envisages a proportionate and effective system of collective redress that incorporates appropriate safeguards to ensure the system works in the interests of consumers, companies and the courts alike. Before bringing any action in the data sphere Which? would engage in the necessary due diligence to ensure that the case was of merit, as we currently do with actions in other areas of consumer protection.

Which? has robust governance measures in place for assessing whether to commence a legal action. In particular, Which? operates within a 'legal actions framework' which provides a comprehensive structure for the organisation to follow when considering whether to bring legal actions. It provides a robust and considered checklist of the various issues that need to be taken into account, and requires cross-organisational efforts in order to ensure proper scrutiny of the issues and that the risks of bringing legal actions are balanced against the likely benefits of the action and Which?'s overall organisational priorities.

Questions

In Which?'s capacity as consumer champion we have chosen to answer those questions which allow us to draw on our experience in consumer protection in the data sphere to present views and evidence based on our expertise. We believe that there are other stakeholders and organisations that are well-suited to assess and provide evidence for other questions that we do not answer, particularly those relating specifically to children's needs.

Q1. Are you responding to this consultation as:
– d. A third sector organisation, (e.g. charity, social enterprise)

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers to make change happen. We fund our work mainly through member subscriptions. We're not influenced by third parties – we never take advertising and we buy all the products that we test.

Q2. What is your view on the uptake and operation of representative action provisions to date and what can be done to improve it? Please provide any relevant data and, where possible, make clear its source. For adults and children respectively, please explain what advice and support is currently available in relation to these provisions.

Which? welcomed the introduction of representative action in the data space under Art. 80(1) GDPR in the Data Protection Act 2018 provisions, and strongly agrees that adequate redress mechanisms for the data sphere are needed in an economy and society fueled by data. However, Which? believes that the current representative action mechanism must be extended and the provisions need to go further by implementing representative action without the specific mandate of the data subject as presented in Article 80(2) GDPR. The current provisions are not working sufficiently as is evidenced by the low levels of uptake of currently available representative actions, despite multiple cases of data breaches that have affected millions of consumers since these provisions came into effect[3].

The Government stated in its call for views and evidence that it is not aware of any claims for compensation brought in the courts by non-profit organisations on behalf of individuals. A major barrier to the uptake of the redress mechanism is the requirement for individuals to seek out an organisation and give their authority before an action can be brought. Under the current representative action provisions the burden lies with consumers to seek out an organisation to bring an action on their behalf - at least one data subject must mandate a representative body to bring an action before others could decide to opt-in. The opt-in requirement presents hurdles and is not working to adequately serve consumers, as is shown by the low uptake of the provisions. There are circumstances where data subjects may not necessarily be aware of what data about them is held by organisations or what is being done with it. In such instances data subjects could not be expected to know

[3] Which? articles on data breaches since GDPR https://www.which.co.uk/news/tag/data-breach/

whether and how they could exercise their rights under data protection law.

The current model presupposes that affected consumers are aware their data has been breached, that they know their right to appoint a representative body and that they see the value in expending time on such an appointment in circumstances where the individual harm suffered may seem relatively small and the prospect of tangible redress remote, but where the collective impact could be significant.

Even if individuals were to appoint an organisation to act on their behalf, under the current provisions those organisations would face significant practical and administrative challenges, particularly in getting other individuals who share the same harm to also opt-in. This ultimately results in many data subjects not getting adequate redress for the harm they have suffered as result of data breaches. This is discussed in further detail below.

ICO Complaints

In its call for views and evidence the Government referred to data, provided by the ICO in January 2020, which suggests that the ICO received around 65 complaints from 'organisations on behalf of individuals' since May 2018. During the reporting period of 2018-2019, the ICO received a total of 41,661 complaints.[4]

It is not sufficiently clear what is meant by complaints from organisations on behalf of individuals here, as the characteristics of the organisations are not outlined - these organisations could include law firms who are acting for individuals, rather than representative bodies acting under the provisions under review.

Additionally, the nature of those complaints is also not clear from the information provided. Many complaints may be of significant interest to the complainant but not of wider significance or impact. An example is individuals making complaints for not receiving adequate responses to their data Subject Access Requests (SARs). Data subjects have the right to ask an organisation whether or not they are using or storing their personal information. They can also ask them for copies of their personal information, verbally or in writing[5]. Data SARs are often used as a first step to a complaint or litigation against an employer, education provider etc.

The data controller may be taking too long or may not have disclosed all the information that is being sought. It is not possible to tell from the data whether significant areas of consumer harm, of the sort that could be addressed through an opt-out representative action system, are going unreported.

Questions for non-profit organisations who have represented individuals

Q5. Do you offer a service to act on behalf of individuals to make a complaint to the ICO or represent them in courts with respect to breaches of data protection legislation? What challenges did you face in doing so?

We provide resources that inform consumers what their options are in cases of data breaches. This includes how to make a complaint to the ICO and how to bring a claim in a small claims court. Although Which? is one of the organisations that falls in the category of being able to bring representative actions with the authority of individuals, to date we have not been mandated to do so. As previously stated, the key challenge to the uptake of the provisions and our representation of data subjects is the opt-in requirement which puts the onus on the individuals to give authority and thereby mandate an organisation such as Which? to act on their behalf.

As a charity, the Consumers' Association must be mindful that it is delivering a public benefit and that its resources are targeted towards maximising impact for UK consumers. An opt-out regime would allow the charity to tackle issues that were causing significant consumer harm; and to ensure that all those individuals who had lost out were represented. Under the current provisions it would be difficult to achieve this aim because of the difficulties associated with encouraging consumers to opt-in. An example of the risks of a low opt-in rate for data claims is the Morrisons data case brought under a Group Litigation Order (GLO) (*WM Morrisons Supermarket*

[4] The ICO's Annual Report and Financial Statements 2018-2019
https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
[5] https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/

PLC v Various Claimants [2018] EWCA Civ 2339[6]), which was concluded in April this year and was ultimately unsuccessful. Which? understands that 99,998 Morrisons' employees were affected in the data breach but only 5,518 of the affected employees initially joined the group litigation. Which? understands that as the litigation progressed the group expanded to 9,263 - a group still less than 10% of the affected group. This was despite all members of the "class" sharing an employer, which could have made them easier to target and sign up.

In October 2019, a GLO was granted in respect of the British Airways data breach that compromised the personal and financial details of over half a million consumers[7]. The court has granted a 15-month window for potential claimants to join the action and reports indicate that around 6,000 claimants have joined to date in spite of the level of press attention the breach attracted.

Which? has experience of opt-in representative action. Which? was designated to bring opt-in claims under the Competition Act 1998. Using its designation, Which? only brought one collective action against JJB Sports for their role in fixing the price of replica football shirts (*JJB Sports PLC v Office of Fair Trading and Allsports Limited v Office of Fair Trading [2004]*[8]*).* The opt-in model presented significant administrative and evidential difficulties which resulted in fewer than 1,000 consumers being compensated, despite millions having been harmed by the infringing practice.

Q8. For adults and children respectively, what, if any, further support should be made available to ensure these complaints or redress mechanisms are exercised properly and effectively? Please explain whether and how the different needs of children at development stages of development affects your view.

Which? is answering this question in relation to adult consumers.

The complex nature of data rights and data protection means that we do not believe that simply making small adjustments to the existing representative action mechanism, or providing additional support, will ever be truly effective in delivering the adequate and appropriate redress consumers critically need, and as a consequence will not be sufficient to drive real change in the behavior of businesses who are not doing enough to protect consumers' data.

Relating to representative action without the authority of individuals

Which? is aware that the questions are each to be considered in relation to adults and children respectively. As Which? is answering the question in its capacity as a consumer champion, the answers pertain to all consumers.

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.

Which? strongly believes that Article 80(2) GDPR should be implemented and that the legislation (Data Protection Act 2018) should be changed to allow non-profit organisations to act on behalf of individuals who have not given express authorisation. There are several reasons for this, which we expand on below:

1. The current 'opt-in' system is not working to adequately serve consumers who suffer at the hand of data breaches, as the onus is placed on consumers, failing to acknowledge many hurdles.
2. Data breaches and data processing practices that infringe data subjects' rights have and are continuing to happen, with consumers suffering real harm as a consequence without having access to the redress they deserve.
3. More needs to be done to hold businesses to account when they do not adequately protect consumers' data and incentivise them to improve their practices.

[6] https://www.supremecourt.uk/cases/uksc-2018-0213.html
[7] https://www.judiciary.uk/wp-content/uploads/2019/10/Weaver-ors-v-British-Airways-PLC-sealed-order.pdf
[8] https://www.catribunal.org.uk/cases/10221103-jjb-sports-plc

Before we expand on these elements it is to be clarified that:

- Which? is aware that Article 80(2) GDPR does not refer to Article 82 GDPR and the compensation rights associated with it. However it does mention Art. 77 (the right to lodge a complaint with a supervisory authority), Art. 78 (the right to an effective judicial remedy against a supervisory authority) and Art. 79 (the right to an effective judicial remedy against a controller or processor).
- Which?'s understanding is that bringing such an action on behalf of data subjects in pursuit of an effective judicial remedy against a data controller or processor without first being mandated by the data subjects would also constitute a form of collective redress (albeit not necessarily in the form of damages) on an opt-out basis. However, in our view, an effective judicial remedy should also include compensation.
- Which?'s reference to redress does not exclusively refer to a judicial remedy in the form of compensation - it includes the regulator taking action in respect of a complaint, seeking a court order requiring a data controller or processor to comply with data protection legislation, compelling measures for companies to assist with future breach/scam protection, and financial compensation.
- Additionally, the Call for Views and Evidence from the UK Government that Which? is responding to is for a statutory review of the Data Protection Act 2018, which transcribed GDPR into UK legislation. The Data Protection Act 2018 requires the government to have specific regard to the merits of extending the provisions to compensation cases. The Call for views and evidence expressly asks for views on not only introducing the opt-out element to representative actions as prescribed under Art. 80(2) GDPR but also to extend this opt-out element to compensation claims.

1. Downsides to an Opt-in System

There are several elements of the current opt-in system that result in harm suffered as a result of breaches of the data protection principles often going without redress, which could be addressed by the extension of the provisions.

Although consumers care about data breaches and business practices which are not compatible with data protection law, they struggle to identify and quantify such harm. Which? conducted deliberative workshops in which participants were given the opportunity to use the tool 'Have I Been Pwned?' to see if their data had been breached[9]. Despite their sense of fatalism and growing awareness of high-profile data breaches, most consumers found that they had under-estimated the amount of information about them that had been breached. In particular, consumers were surprised to find that:

- Information had been stolen from 'reputable' providers who hadn't told their customers that they had suffered a breach (either directly, or indirectly, through the media): for example, there was some surprise in seeing references to accounts held with organisations such as LinkedIn and Yahoo being compromised.
- Information about them had been stolen from unfamiliar organisations that they had not heard of before and who they had not consented to hold their data: this included data brokers, organisations which had only become known to the majority of consumers over the course of the workshop.
- Information beyond email addresses and passwords had been stolen: including home addresses and IP addresses, and in some cases, all of the above.

However, while exposure to this information in the setting of a deliberative workshop increased concern for consumers, it rarely spurred them into action and instead appeared to reinforce a sense of resignation about the security of their data. Many believed that once their information was 'out there' (through cyber crime, but also legal practices such as data sharing) there was very little they could do to protect it[10].

[9] Control,Alt, Delete? The Future of Consumer Data report by Which?
https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report
[10] Control, Alt, Delete? Consumer research on attitudes to data collection and use
https://www.which.co.uk/policy/digitisation/2707/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use

In Which?'s Consumer Insight Tracker we ask consumers about their worries on a quarterly basis, with August 2020 being the source of our most recent data. 66% of consumers asked said they were worried about the security of the data they share (up from 64% in February 2020), making it the biggest consumer worry this year[11].

There is growing fatalism among consumers and a perception that securing their data is beyond their control. These elements of consumer behaviour paired with the onus being on data subjects to seek out representative action means that harm suffered as a result of data breaches often goes without redress. In order to provide consumers with adequate redress and in turn give them confidence in the way that organisations are using their data the representative action provisions need to be extended to allow not-for-profit organisations to bring actions on behalf of data subjects without their express mandate.

There are different behavioural biases affecting consumers that result in a lower likelihood of them seeking redress of their own accord. Bounded rationality results in consumers being unable to process and act optimally on large amounts of data, this often means that they cannot contemplate the multitude of consequences that could result from a situation. Consumers think of immediate impact and struggle to see how a data breach may cause them further harm beyond what they can see in the immediate aftermath. This is amplified by individual harm appearing relatively small at an individual level whilst having a much larger collective impact - something which is prevalent in data breach cases.

Incomplete and asymmetric information also decreases the likelihood of consumers taking up representative action available under the current provisions. Consumers often know less than businesses and organisations about how their data may be used and by whom, and the associated consequences. It is unrealistic to assume knowledge of probabilities of all possible outcomes and for consumers to be able to evaluate these against each other to decide whether to take action. Not-for-profit representative bodies are in a better position to be better informed, due to greater available resources and a smaller opportunity cost of investigating.

2. Breaches of Data Protection Principles Continue to Happen and Consumers Suffer Harm as a Result

There have been significant Data Breaches since GDPR and the Data Protection Act 2018 came into effect, with varying outcomes. Which? has reported on several large-scale major breaches since the introduction of the legislation. Certain businesses have even faced two major breaches in that time despite proposed fines by the Information Commissioner's Office (ICO)[12].

Consumers suffer real harm as a result of these breaches and business practices, despite often not seeking redress due to the hurdles of the current systems we have outlined. Which? recently published an investigation into the human cost of data breaches[13], looking at what happens when personal details fall into the hands of criminals and why the consequences for victims can be far greater than for the companies responsible.

We found that 23% of Which? members have fallen victim to a data breach, according to our survey of 1,369 people in July 2020. Of those members 46% later experienced fraudulent activity. This is just those members who were aware that their data had been compromised. Which? also had 515 members take part in submitting their email address to see if it could be linked to a breach, submitting a total of 610 email addresses. It was revealed that 79% had experienced at least one breach. Of those, the average number of breaches per email address was 3.7. One address had been in 19 breaches.

The investigation also contains personal accounts of consumers, such as an individual who was in the British Airways data breach and had scammers attempt to take £15,000 from his bank account. His account was suspended and he was stranded abroad with no access to funds. He detailed having numerous panic attacks.

[11] *Data from the August wave of Which?'s Consumer Insight tracker, conducted by Populus on behalf of Which? from 12th-14th August 2020. A sample of 2,083 consumers was surveyed and weighted to be nationally representative according to a range of demographic characteristics.*

[12] https://www.which.co.uk/news/tag/data-breach/

[13] The Human Cost of Data Breaches
https://www.which.co.uk/news/2020/09/data-breaches-how-your-personal-details-end-up-in-the-hands-of-criminals/

The data protection principles according to GDPR stipulate that both pecuniary and non-pecuniary loss resulting from infringement of data protection law are within scope.

3. More needs to be done to incentivise businesses to improve their security

An extension of the provisions to introduce representative action without the specific mandate of data subjects is necessary as businesses continue to fail to put adequate measures in place to prevent data breaches and alter their business practices. In September 2020 Which? published an investigation which exposed hundreds of serious data security vulnerabilities on major travel firm websites[14].

Which?, working in collaboration with security experts 6point6, assessed the security of websites operated by 98 travel industry companies, including airlines, tour operators, hotel chains, cruise lines and booking sites, in June 2020. Which? did not just look at the main website of each firm, but also related domains and subdomains – including promotional sites and employee login portals.

Any vulnerability in these websites could be an opportunity for a malicious hacker to target users and their data. We didn't engage in complex hacking to find this information, but rather used publicly available, lawful online tools that anyone can access.

Certain businesses in the travel industry have already had their details and those of their customers stolen in major data breaches yet our experts found dozens of critical hacking risks on their websites. British Airways, easyJet and Marriott Hotels have had breaches affecting nearly 350 million customers combined in the past few years, incurring £283m in proposed fines from regulators. Yet, when our experts tested the security of nearly 100 travel websites, all were in the bottom five.

Our experts identified 834 suspected vulnerabilities, including 32 deemed as critical risks. In 2018, hotel chain Marriott reported that records of 339 million guests had been maliciously accessed. Despite a proposed fine of £99.2m by the ICO, Marriott reported a further breach in May 2020 involving 5.2 million guests. Despite this our researchers found Marriott not only had the most vulnerabilities of nearly 100 websites we investigated, but also the most critical issues.

We reported our findings directly to Marriott, which stated that it had 'no reason to believe' that its customer systems or data had been compromised. It also claimed that some findings were 'not attributable to Marriott', while others 'could not be validated'. It did not supply any specific examples of mitigations, but said that it would be 'taking a closer look at and addressing Which?'s findings'.

These suspected vulnerabilities were found despite the large fines proposed by the ICO. In July 2019 the ICO announced its intention to fine British Airways £183.39 million[15]. In October the ICO fined British Airways for a revised amount of £20 million[16]. The opt-out collective redress mechanism is needed as an additional method to hold data controllers to account when they breach data protection law but also to incentivise data controllers to improve their data security and data processing mechanisms, as data breaches put consumers at considerable risk.

Breached data, consumer detriment and scams

In October 2020 Red Maple Technologies prepared a research report delving into what happens to consumer's personal data exposed in a data breach to paint a clearer image of what risks consumers are then additionally

[14] Can Travel Websites Keep Your Personal Data Secure?
https://www.which.co.uk/news/2020/09/marriott-british-airways-and-easyjet-fail-on-data-security-with-hundreds-of-security-risks-exposed-by-which/

[15] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

[16] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

exposed to. There is extensive information detailing how breached data can expose consumers to further attacks and scams. No personal data was processed on behalf of Which? during this research.

A data breach of a company typically leaks personal information that includes the email addresses of account holders as well as other personal information. It is rare for breaches to include passwords in a usable form (*plaintext passwords*), as industry standard protections for securely storing passwords (*password hashing*) are almost ubiquitous.

However, given a dump of protected passwords it is normally possible to recover a proportion of the passwords into their readable (*plaintext*) form, using password recovery (*cracking*) techniques that typically require lots of computation and lists of dictionary words and example passwords. Lists of email addresses are used, in conjunction with confirmed and possible passwords, to mount attacks such as *phishing*, *brute-forcing*, and *credential stuffing*.

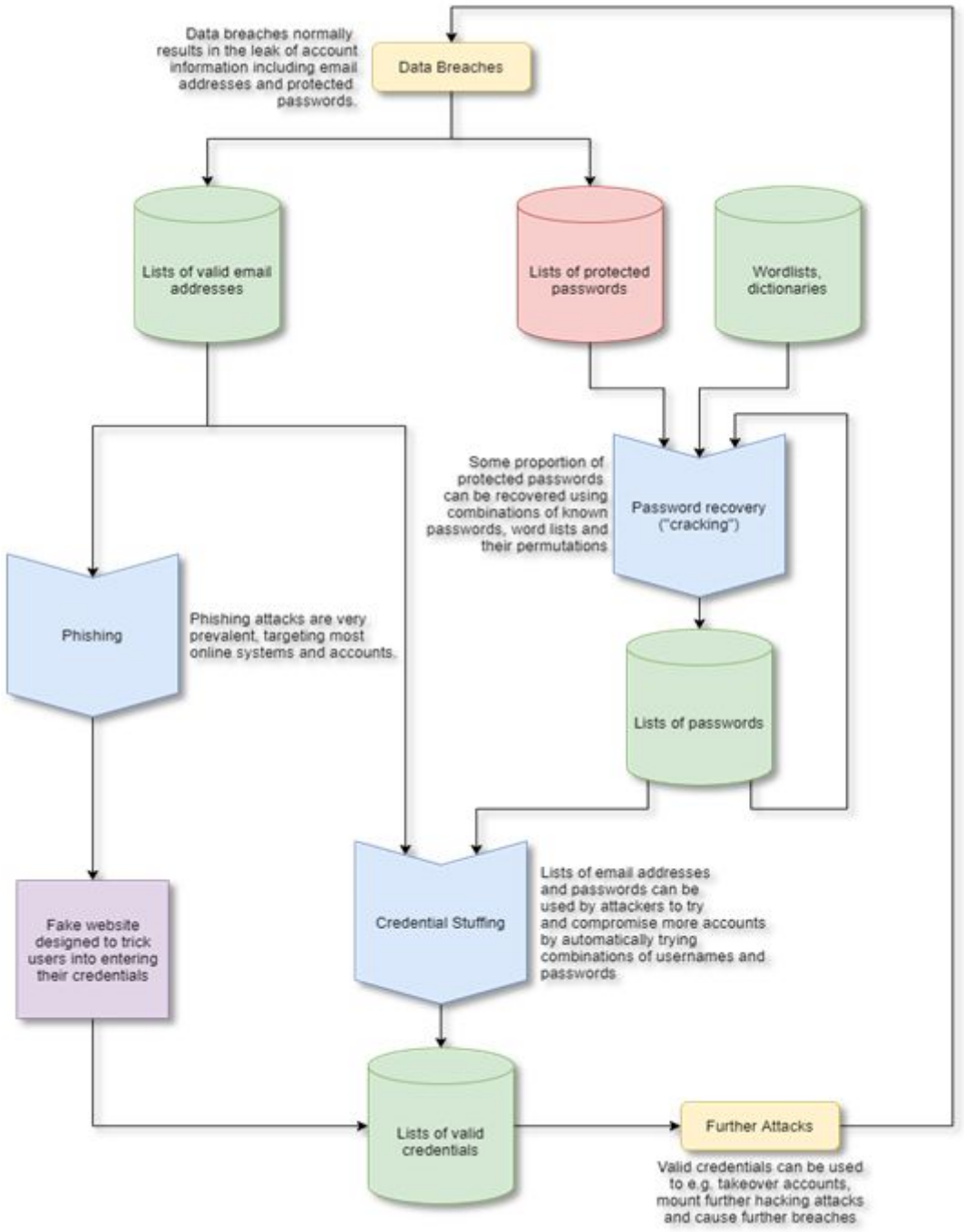
Phishing involves sending emails containing malicious content to target addresses. Of late this most often consists of a link to a malicious website designed to trick the victim into entering their credentials (username/email address and password).

Brute-forcing and credential stuffing are both ways of trying to break into online accounts by testing lots of combinations of possible usernames and passwords. Brute forcing involves trying systematically generated passwords, whereas credential stuffing involves trying known passwords.

The sheer scale of such continuous attacks is detailed by Akamai, a global content delivery network, cybersecurity and cloud service company providing web and Internet security services. From July 2018 through to June 2020 Akamai observed 100 billion credential stuffing attacks across all industries[17].

The diagram below, created by Red Maple Technologies in its research for Which?, illustrates how data breaches, recovered passwords, phishing and common attacks feed into each other, creating ever-increasing public and private repositories of known email addresses, passwords, and compromised accounts:

[17] https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/soti-security-gaming-you-cant-solo-security-report-2020.pdf



Whilst the aim of hackers used to focus predominantly on gaining access to systems and data, now the focus is often solely on stealing credentials. This may be to sell them into the large market for credentials, to use them in further attacks, or both. The use of stolen account credentials is the most common action in large surveys of data breaches[18].

The market for stolen credentials is well established, and largely relies on the Dark Web for hiding the identity of the buyers and sellers, and cryptocurrencies like BitCoin for anonymous transactions. The Dark Web is a parallel version of the Internet that can be accessed by anyone using specific applications. These applications provide encryption and anonymisation of the users' traffic and their location. There are a lot of anecdotal examples of

[18] Verizon Data Breach Investigations Report 2020 https://enterprise.verizon.com/en-gb/resources/reports/dbir/

such transactions, which range in price from a few dollars for small numbers of accounts, to hundreds or thousands of dollars for large sets of credentials.

Red Maple Technologies in its research for Which? safely captured screenshots of Dark Web sites that are either open or require simple registration to access, without any sharing of data or purchases. These screenshots showed large data dumps for sale on sites aimed at selling stolen data. Data dumps of various sizes were presented, each of which affected over a million customers, with prices for the dumps ranging from $200 to $10,000.

We have seen the human cost of credentials falling into the wrong hands - consumers suffer real harm as a result of breaches and inadequate business practices, despite often not seeking redress due to the hurdles of the current systems we have outlined.

Consumer detriment: emotional distress

Research shows that there is a considerable emotional and mental toll that accompanies having one's personal information misused or falling victim to a scam or fraudulent activity.

The vast majority of scam victims experience some emotional harm - a large survey from the European Commission published in January 2020 showed that 8 out of 10 people who experienced a scam suffered some emotional detriment[19]. This increased to 95% among those who suffered a financial loss. The survey was conducted in the 28 EU Member States (at the time including the UK), Iceland and Norway. In total 28,239 interviews were completed across all countries, with the fieldwork conducted between August and October 2019. Those who experienced scams and fraud most often reported to have experienced the scam or fraud by means of online communication channels, including via email (43%) and online advertisements (11%)[20].

Scams can be a source of emotional turmoil for consumers, particularly where financial harm has been suffered. Stress resulting from falling victim to a scam can lead to further emotional detriment, ranging from anger to depression. Consumers report suffering feelings of embarrassment, anxiety, shame, vulnerability and fear[21]. The National Trading Standards Scams Team has previously reported cases where a scam has led victims to feel suicidal[22].

Consumers do not only suffer emotional harm when a scam succeeds. In Which?'s investigation looking at the human cost of data breaches, consumers expressed worry at their data being 'out there' following a data breach[23] . These worries are not unfounded as data breaches, recovered passwords, phishing and common attacks feed into each other, creating ever-increasing public and private repositories of known email addresses, passwords, and compromised accounts used by scammers. As previously mentioned, the data protection principles according to GDPR stipulate that both pecuniary and non-pecuniary loss resulting from infringement of data protection law are within scope.

Given the considerable harms that consumers are exposed to through data breaches, inadequate security measures that put their personal data at risk, and data processing practices that violate data protection principles, more needs to be done to hold data controllers to account when they do not adequately protect consumers' data and incentivise them to improve their practices.

---

19 https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

20 https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

21 https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Scams%20report%20-%20final.pdf

22 https://www.nationaltradingstandards.uk/site_assets/files/NTS%20Consumer%20Harm%20Report%202016.pdf

23 The Human Cost of Data Breaches https://www.which.co.uk/news/2020/09/data-breaches-how-your-personal-details-end-up-in-the-hands-of-criminals/

Q15. What safeguards, if any, should operate to avoid the speculative or vexatious use of any new powers for non-profit organisations to act without the consent of individuals and avoid a disproportionate administrative burden on either the regulatory or courts systems?

Which? recognises that careful thought must be given to the way the new collective redress mechanism is structured. Which? envisages a proportionate and effective system of collective redress that incorporates appropriate safeguards to ensure the system works in the interests of consumers, companies and the courts alike. An opt-out scheme for data breaches could introduce additional procedural safeguards against abuse, such as those that govern the opt-out competition law regime. In addition to ensuring that it is "just and reasonable" for the applicant to act as a class representative, the Court must also consider whether the proposed representative would in all the circumstances fairly and adequately act in the interests of class members, and if she is suitable to manage the proceedings; if the representative is not a member of the class, the court will consider whether the representative is a pre-existing body and its nature and functions; the court will also consider if there is a satisfactory plan for conducting the collective proceedings which includes notifying the class members, governance of the claim and budgeting.

The GDPR is also specific about the type of organisations able to to bring actions on behalf of consumers through both Article 80(1) and Article 80(2). Organisations wishing to represent consumers must meet the criteria as set out by the Data Protection Act 2018. Only not for profit organisations who are acting in the public interest, and who actively work in the area of the protection of data subjects' rights, would qualify to bring an action. The action itself would have to have prima facie merit, namely where a data breach has occurred and the company responsible for protecting consumers' data has not offered appropriate redress. Any organisation wishing to take action would therefore have to demonstrate that not only did it meet the criteria to act on consumers' behalf but that they had an appropriate case.

Q16. What conditions, limitations or safeguards should apply if non-profit organisations act on behalf of individuals who have not authorised them to do so? For example, should individuals be given the right to object to a non-profit organisation taking action on their behalf without their consent? Please explain.

The extension of the provisions should not dictate compulsory representation. The introduction of an opt-out element to representation without the specific authority of data subjects would, by its very definition, allow individuals of a class/group who wish to not be represented in the action to opt-out of the action.

One of the reasons for the strict interpretation of Civil Procedure Rule 19.6, in representative actions brought using them, which we expand on in Q.19, is that an order or judgment in a representative action is binding on all persons who are represented, even if they are unaware that the proceedings were underway. Safeguards, such as those introduced in respect of the competition law collective proceedings regime, can address concerns that individuals will be bound by a decision, which they did not choose to participate in, in circumstances where they may wish to pursue their own claim. It could allow the court to approve a litigation plan, which sets out the publicity efforts to allow individuals the greatest opportunity to be informed about the claim; as well as specifying the period in which members of the class will be able to opt-out.

The GDPR already includes safeguards, for example, requiring the action to be brought by a non-profit, which ensures an additional safeguard of impartiality against abuse as well as placing the responsibility for such actions with organisations that already have significant expertise in the field of data protection and objectives that are focused on providing public benefit.

Q17. If the new provisions discussed in this chapter were adopted, what impacts do you anticipate on data controllers which might be the subject of a complaint or legal claim, particularly businesses, including any increased costs or risks?

The underlying data protection principles would not change. Data controllers handling data subjects' data in a GDPR compliant manner with adequate safeguards in place should not incur additional costs and risks from the extension of the provisions alone.

The extension of the provisions would not mean that every data breach resulted in an action by not-for-profit

organisations. Introducing a representative action mechanism under Article 80(2) GDPR would not stop responsible data controllers from taking timely actions to put things right following a data breach and would not additionally impact those businesses who have adequate data protection measures in place in order to prevent breaches. The new provisions would however give consumers the assurances that those data controllers that have vulnerabilities in regards to how they handle consumers' personal data will be held to account if they do not improve their data processing mechanisms and consumers suffer harm.

Data controllers that conduct themselves appropriately and meet their data protection obligations, including by treating consumers fairly when things go wrong, have nothing to fear and much to gain from an effective redress regime. An example of this are the potential efficiency gains of all related claims being dealt with together, rather than many individuals claims.

Q18. If the new provisions discussed in this chapter were adopted, what are the likely impacts on the ICO or the judicial system, which will be required to consider representations made by non-profit organisations? What is their capacity to handle new claims brought under any new provisions, and how might the design of any new provisions help to manage pressures?

It is critical that the ICO is adequately resourced to effectively deal with an ever-increasingly data-driven society. An increase in cases is to be expected, however this does not have to mean an overwhelming influx. As previously outlined, stringent criteria and safeguards would also be in place to prevent speculative or vexatious use of any new powers relating to compensation claims. This would ensure that actions would be brought with the intention of remedying consumer detriment and incentivising improvement of inadequate data processing practices.

Concerns about a "class action" regime that is vulnerable to abuse are ill founded:

- The introduction of opt-out collective redress in the competition sphere has not led to a deluge of claims – far from it.
- The "loser pays" principle and the very considerable financial challenges associated with pursuing significant opt-out compensation claims ensure that, should an opt-out regime be introduced, organisations and particularly not-for-profit organisations would exercise considerable restraint in pursuing only those claims which have caused significant losses to consumers and which have good prospects of success i.e. meritorious claims.
- As GDPR has specific criteria regarding the types of organisations that can bring representative actions, these types of organisations would not be willing to risk their reputation by bringing a series of unfounded, vexatious or frivolous claims. The reputational consequences would impede the pursuits of their organisational goals.
- Unlike the US, punitive (exemplary) damages are only available in England and Wales in very rare circumstances in cases involving deliberate torts.
- Opt-out regimes in other European jurisdictions, such as Portugal have increased access to justice without creating a system of abusive claims.

By comparison, there is compelling evidence in the data protection sphere, as well as in other sectors, that the opt-in regime is not serving consumers well and is not suitable for pursuing defendants who have caused significant consumer detriment as a result of an alleged breach of the data protection principles.

Case Study: The Netherlands

In March 2019, the Dutch legislators approved the legislation introducing collective damages actions in the Netherlands. In January 2020, the Dutch Act on the Resolution of Mass Claims in Collective Action (*Wet afwikkeling massaschade in collectieve actie*) (Dutch acronym: WAMCA) entered into effect, introducing the possibility of claiming damages on a collective basis under an opt-out regime for Dutch residents and an opt-in

regime for parties residing abroad[24]. The legislation introduced an option to claim monetary damages on an opt-out basis for a variety of claims, including claims relating to violations of the GDPR[25].

Safeguards accompany the legislation as it includes enhanced standing and admissibility requirements for organisations bringing collective actions, which will be assessed at an early stage of the proceedings. These relate to elements such as the governance of the organisation, funding, representation, previous experience and track record.

One admissibility requirement is that the action must have a sufficiently close connection with the Dutch jurisdiction. When this is applied to GDPR this means a sufficiently close connection is deemed to exist:

- If most of the affected individuals for whom the collective action is initiated reside in the Netherlands.
- If the controller or processor is established in the Netherlands, provided that other circumstances also point to a connection with the Dutch legal sphere.
- If the processing that resulted in the violation of the GDPR took place in the Netherlands[26].

Although it is an early assessment due to the legislation only entering into force at the beginning of this year, it does not appear to have brought an overwhelming influx of cases. In August 2020 the first case applying the legislation to infringement of GDPR was brought by The Privacy Collective, an organisation that acts against the violation of privacy rights[27].

Q19. What are the alternative means or mechanisms by which non-profit organisations are currently able to bring complaints to the ICO or to court using existing Civil Procedure Rules? Please provide any evidence of their use or operation to date.

With the exception of the collective proceedings regime for competition law actions, consumers across the United Kingdom do not currently have the benefit of an opt-out collective redress mechanism, which will compensate them for losses suffered in all circumstances, including for losses (whether pecuniary or loss of control) associated with breaches of the data protection principles.

The existing mechanisms are not well suited to tackle consumer detriment in data-cases, where the individual losses may be small, but the collective detriment could be significant. For defendants, the individual defence of numerous low value claims by all those consumers who have suffered a loss as a result of an infringing practice or event are inefficient and burdensome.

Group Litigation Order

Group litigation orders (commonly referred to as GLOs) can be made under the Civil Procedure Rules (CPR 19.11) where there *"are or are likely to be a number of claims giving rise to […] "common or related issues of fact or law"*. Whether or not a GLO is granted is a matter for the court and it is necessary for individual claims to be issued so the amount of unfamiliar and potentially burdensome administration for a consumer, especially one who has suffered a small loss, is considerable and will represent a disproportionate deterrent for many, as will the potential costs risk.

A GLO was used in the previously mentioned *Morrisons* data case, which was heard in the Supreme Court earlier this year and the case shows how difficult it can be to address mass harm situations for all of those who have suffered detriment through a GLO. In that case, the almost 100,000 prospective claimants were colleagues and it ought to have been easier to draw the claim to their attention. In spite of this, Which? understands that less than 10% of the prospective claimants joined the GLO.

---

24 https://www.natlawreview.com/article/new-dutch-act-collective-damages-class-actions-effective-1-january-2020#:~:text=On%201%20January%202020%2C%20the,and%20an%20opt%2Din%20regime

25 https://www.hoganlovells.com/en/publications/a-collective-action-for-damages-in-the-netherlands-is-a-fact

26 http://documents.jdsupra.com/22b85b47-3735-4dee-a6ad-1efbbf04cd9c.pdf

27 https://www.privacyfirst.eu/focus-areas/online-privacy/689-the-privacy-collective-takes-oracle-and-salesforce-to-court.html

In October 2019, a GLO was granted in respect of the British Airways data breach that compromised the personal and financial details of approximately half a million of consumers[28]. The court has granted a 15-month window for potential claimants to join the action and Which? understands that around 6,000 claimants had joined around that time in spite of the level of press attention the breach attracted[29].

"Representative Actions"

A "representative action" is a claim brought by one or more claimants, on their own behalf and on behalf of others under Civil Procedure Rule (CPR 19.6). It can be used when others have the same interest in the claim as the representative claimant. The "class" will have the "same" interest in the claim as the representative and will be bound by the judgment. The courts have historically interpreted the "representative action" test strictly. This means that it has not been an effective tool to address harms suffered by groups of claimants who have been affected by a similar or related loss, which is not identical.

This mechanism is being used by Richard Lloyd in his action against Google, concerning iPhone users' cookies being sold to advertisers without their knowledge or consent. Whilst the claim was unsuccessful at the first instance, the Court of Appeal adopted a more liberal interpretation of the test – indicating that representative action for damages on behalf of a class having suffered a core of the same loss as a result of the defendant's action may be sufficient. The case is due to be heard by the Supreme Court next year.

Q20. In what ways would the potential measures outlined in Chapter 3 either complement or duplicate these alternative mechanisms?

Which? believes that a bespoke scheme for data protection claims (as envisaged by this call for views and evidence) is preferable for the reasons set out below.

Need for a new regime

Model

There is already an opt-out regime benefitting UK consumers who have suffered losses as a result of a breach of competition law. Further to amendments introduced by the Consumer Rights Act 2015, the Competition Act 1998 now provides a mechanism for opt-out claims to be brought in competition cases. It is not essential for a claim to follow-on from a regulatory decision that the defendant has infringed competition law, as stand-alone claims are also possible. To date consumer-focussed applications for a Collective Proceedings Order (the first stage in such a claim) have been made in respect of both follow-on (*Merricks v Mastercard*) and stand-alone (*Gutmann v London & South Eastern Railway Limited*) claims. Whilst no claim has yet progressed beyond the stage of a Collective Proceedings Order, Which? is keen to see the new regime function effectively and recently intervened in the Supreme Court's consideration of Walter Merricks' claim, which has been brought on behalf of approximately 46.2 million UK consumers who suffered loss as a result of MasterCard's anti-competitive conduct.

Developments

Whilst the UK has previously exercised caution in respect of the introduction of opt-out collective redress schemes, the last decade has seen significant developments in this sphere. Namely:

- In 2015, the Consumer Rights Act 2015 introduced an opt-out collective redress procedure for competition claims.

- The scandal associated with "Dieselgate" led to the realisation that the EU should establish a collective redress procedure for all consumers to provide victims of mass harm events with a realistic opportunity

[28] https://www.judiciary.uk/wp-content/uploads/2019/10/Weaver-ors-v-British-Airways-PLC-sealed-order.pdf

[29] https://pgmbm.com/high-court-in-london-granted-a-group-litigation-order-following-september-2018-british-airways-data-breach/

to address breaches of their legal rights. In April 2018, the European Commission adopted a "New Deal for Consumers". The collective actions file has since progressed and will include collective redress provisions for data protection breaches. In June 2020 an EU deal was agreed on a draft directive on representative actions for the protection of the collective interests of consumers[30]. The directive will cover actions for both injunctions and redress measures. It will empower designated qualified entities to seek injunctions and/or redress, including compensation or replacement, on behalf of a group of consumers that has been harmed by a trader who has allegedly infringed one of the EU legal acts set out in the annex to the directive. These legal acts cover data protection[31].

- Following significant consultation, the possibility of opt-out collective redress for Scottish consumers was expressly included in the Civil Litigation (Expenses and Group Proceedings) Act 2018, alongside opt-in collective redress. The Group Proceedings Working Group established by the Scottish Civil Justice Council ("SCJC") in March 2020, conducted an informal consultation process for implementing the new mechanism[32]. In the consultation the SCJC expressed a preference for introducing the new mechanism on an opt-in basis initially, with the consideration of an opt-out mechanism to follow later[33]. The relevant court rules have now been published and entered into force 31 July 2020[34].

In light of the above developments in Scotland and Europe, English and Welsh consumers may be left at a distinct disadvantage in the future as compared to their near neighbours and therefore in a position where they are ultimately less safe online, in stark contrast to the Government's stated aims.

Conclusion

Which? urges the Government to extend the Data Protection Act 2018 provisions and introduce representative action without the specific authority of data subjects as outlined in Article 80(2) GDPR, allowing not-for-profit organisations to bring actions on behalf of consumers on an opt-out basis. If the Government seeks to achieve its objectives of making the UK the safest place to be online, the best place to start and grow a digital business, trial new technology and undertake advanced research, then it is imperative that consumers have access to adequate redress.

Consumers must have confidence in the way that organisations are using their data and must be assured that there are well-functioning and accessible mechanisms in place for instances where their data rights infringed. Adequate redress mechanisms for data breaches, inadequate data processing practices and business practices that violate data protection principles are critically needed in an economy and society fueled by data.

In the call for views and evidence it is outlined that the representative action provisions are 'designed to help individuals who may not have the capabilities or resources to exercise their rights effectively on their own'. Evidence shows that this is not happening effectively with the current provisions.

The current system is not working to adequately serve consumers, as evidenced by the low uptake of the current provisions. The introduction of the opt-out collective redress mechanism is necessary to combat the presuppositions of the current model that affected consumers are aware that their data has been breached, that they know their right to appoint a representative body, and that they see the value in expending time on such an appointment in circumstances where the individual harm suffered may seem relatively small even though it may have had a much greater collective impact. Evidence shows that this is often not the case.

[30] https://www.consilium.europa.eu/en/press/press-releases/2020/06/30/eu-consumers-obtain-access-to-collective-redress/
[31] https://www.consilium.europa.eu/en/press/press-releases/2020/06/30/eu-consumers-obtain-access-to-collective-redress/
[32] https://www.cms-lawnow.com/ealerts/2020/06/scottish-class-action-procedure-to-come-into-force-on-31-july-2020
[33] https://www.scottishciviljusticecouncil.gov.uk/news/2020/07/09/group-proceedings-actions-now-available-in-scotland-s-highest-civil-court
[34] https://www.dlapiper.com/en/uk/insights/publications/2020/07/class-actions-easier-to-seek-redress

Data breaches and business practices that put consumers' data at considerable risk are continuing to happen, resulting in consumer detriment ranging from distress to financial losses. The collective impact of these continued breaches and infringement is a system that is not functioning as data protection principles stipulate. There is growing fatalism among consumers and a perception that securing their data is beyond their control. This must be combated in order to facilitate an environment where consumers have confidence in their engagement with businesses. The continued success of e-commerce depends on the active engagement of consumers, which is dependent on their trust[35].

Besides giving consumers better access to the redress they are entitled to according to data protection law, more needs to be done to hold businesses to account who do not adequately protect consumers data or engage in business practices which contravene data protection principles. The underlying data protection principles would not change. Facilitating redress through an opt-out mechanism would be a complementary method to incentivising good practice alongside existing measures.

We have seen the introduction of opt-out mechanisms in other areas of consumer protection in the UK, and the benefits of opt-out systems have also been recognised in other jurisdictions without waves of 'spurious' claims. The developments in Europe show that there is a trend in acknowledging the need for properly functioning collective redress mechanisms. Examples from other areas of consumer protection and other jurisdictions show that a proportionate and effective system of opt-out collective redress system is possible, a mechanism that incorporates appropriate safeguards to ensure the system works in the interests of data subjects, businesses and the courts alike. We urge the Government to do the same and introduce the representative action regime without the specific authority of data subjects so that UK consumers are not left at a distinct disadvantage as compared to their neighbours and are not left in a position where they are ultimately less safe online, in stark contrast to the Government's stated aims.

Which? is the UK's consumer champion. As an organisation, we're not for profit and all for protecting consumers – a powerful force for good, here to make life simpler, fairer and safer for everyone.

We stand up for what's right for consumers, their experiences drive us to make things better. Our research gets to the heart of the consumer issues that matter, and our expert advice is completely impartial. Same goes for our product reviews – our rigorous tests and expert recommendations help consumers to make better decisions. We investigate and make change happen - from tackling online scams to campaigning for safer products, we're the independent consumer voice that influences politicians and lawmakers and holds businesses to account.

We fund our work mainly through member subscriptions. Businesses whose products or services earn our endorsements can, for a fee, use our name to promote them, and we get commission from some retailer websites where consumers can buy products or services that we feature on our site. We are not influenced by third parties - we never take advertising or accept freebies from manufacturers.

Everything we do is about championing consumers. We'll always be on their side, fighting their corner and working to make them more powerful.

For more information, please contact Vera Opoku, Policy Adviser, Which? at vera.opoku@which.co.uk

[35] https://www.consumersinternational.org/media/155222/consumerchecklistforinternationale-commercedeal.pdf