CLIFFORD
CHANCE

DATA LITIGATION: A TOOLKIT FOR DEFENDANTS

— THOUGHT LEADERSHIP

OCTOBER 2020

DATA LITIGATION:
A TOOLKIT FOR DEFENDANTS

The rise of data litigation

The risks to businesses of civil claims arising out of data breaches have been underplayed. Data litigation is on the rise and the exposures are potentially significant. In this briefing, we explore the key defences to such claims and the arguments available - in light of the emerging case law - to challenge the large amounts being claimed by data subjects in damages.

2020 has seen a significant number of data claims being issued in the English courts. Following British Airways' announcement in 2018 that there had been a breach of its security systems leading to more than 500,000 customers' data being leaked, claimants have issued claims which could be worth up to £3 billion. The ICO penalty notice handed down this month, for £20 million, is comparatively small. In Lloyd v Google LLC [2019] EWCA Civ 1599, a representative action on behalf of an estimated 4.4 million individuals (at £750 per individual), Google's potential liability is for £3.3 billion, excluding costs. And after a data breach affecting Starwood Hotels' guest reservation database led to the loss of 300 million individuals' data, an action has been commenced against Marriott International which could cost it £1.7 billion.

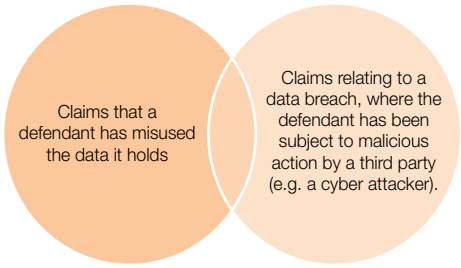
Dealing with data claims

Businesses facing claims need to give serious thought to how they will defend their position. Data breaches take many forms, and understanding the factual issues (including steps needed to comply with the GDPR) is key. Businesses should seek expert legal advice at an early stage, and before responding to claims for compensation.

However, in our experience, four key lessons should form the basis for any business's litigation defence toolkit.

Litigation Defence Toolkit – Lesson 1: be mindful of civil litigation exposure

In broad terms, data claims can be split into two categories:



Upon receipt of a claim or complaint, or in the event of a data breach, businesses need to be mindful of their civil litigation exposure. They should take early action to:

- identify the scope of the data held;
- investigate what went wrong and the damage that was caused;
- identify the contracts (e.g. terms and conditions) on the basis of which the relevant data was held; and
- notify relevant regulatory authorities where appropriate.

They should also ensure they have a communication protocol in place to ensure that they benefit from legal professional privilege, where appropriate.

Litigation Defence Toolkit – Lesson 2: consider your factual defences against claims for loss of control over data

Businesses should be aware that, in the event of a data breach, there are defences available to them. In our experience, defendants to data claims generally seek to rely on the following broad categories of defence to adverse allegations:

Type of Allegation	Basis for Allegation	Potential Defence
Allegations as to the quantity and significance of the data released / misused	In a claim for breach of confidence, the confidential information must have been disclosed in circumstances of confidentiality, and there must be a threatened or actual disclosure of the information.	There was no relationship of confidence between the claimant and the defendant. The law is instead targeted at the use of information by its recipient (and the defendant did not misuse it).
		The information disclosed was not confidential, or did not belong exclusively to the claimant, or was already in the public domain.
		The claimant did not exert any meaningful control over the data in the first place.
	A claim for misuse of private information requires a "*reasonable expectation of privacy*" in the information.	The data was not such as to create a reasonable expectation of privacy. For example, in its defence to a representative action brought by Atkinson, Equifax argued that a name, date of birth and telephone number were in any event publicly available. That case has recently been withdrawn. However, similar arguments have been raised in British Airways' defence.
Breach of contract	A claimant may argue that the defendant has held the claimant's data in a manner inconsistent with its obligations under a contract between them, or is otherwise in breach of contract.	Defending such a claim will require a detailed analysis of the relevant contract by expert legal advisers.
Allegations as to the events that took place	A claimant will make a range of factual allegations which need to be individually considered and addressed. In some circumstances, the ICO may have chosen to investigate an information breach and may have issued a notice or penalty. Firms need to review such notices carefully, as they may be relied on by potential claimants.	Defendants will need to consider any ICO notices closely with expert legal counsel. There may be areas that the ICO has not explored.
Allegations as to the duties of care owed to the claimant	A claim for misuse of private information requires that the defendant owed the claimant a tortious duty to keep his / her data secure or reasonably secure.	Defendants may be able to argue that the law doesn't recognise any such duty in the relevant context – in claims brought for breaches of statutory duty (e.g. under the Data Protection Act ("DPA") 1998 or 2018, or the GDPR), the courts have previously held that it is inappropriate to superimpose a duty of care in tort (Smeaton v Equifax [2013] EWCA Civ 108).
		Defendants may be able to argue that they did not receive information they knew or ought to have known was fairly and reasonably to be regarded as confidential.

Type of Allegation	Basis for Allegation	Potential Defence
Inadequate systems or supervision, or failure to mitigate	A claimant may argue that the defendant has breached standards of good practice, such as the data protection principles set out in the DPA 1998 / 2018 and GDPR, which relate to, among other things, audits, checks and retention practices. Notably, claimants have raised such concerns even where a data breach did not affect certain customers (e.g. where data breach notifications were sent to those whose personal data was not actually affected).	Defendants will need to take early technical advice and consider these allegations closely with expert legal counsel, who can assist in analysing the reasonableness of any processing of data and / or mitigation strategies the defendant has in place. However, a defendant might argue that it is for the claimant to demonstrate a failure to comply with relevant standards / the GDPR – this is an argument made by British Airways in the significant data breach litigation it is currently defending.

Litigation Defence Toolkit – Lesson 3: employ applicable causation arguments

Causation is an important area which has yet to be significantly explored by the English courts in relation to data litigation. Defendants should focus on such arguments because they have the potential significantly to reduce the level of damages a court awards against a defendant, or bar a claim from proceeding entirely.

Internal investigations, data collection and expert economic analysis can give businesses an important head start. A basic causation argument in a cyber-attack scenario might be that a malicious third party was ultimately responsible for a data breach, and not the mitigation systems in place to fend off such attacks. However, we advise our clients to look at causation more deeply. If a defendant can show through economic analysis that the harm did not stem from the data breach, or that an intervening event broke the "chain of causation", the required causal nexus may not be established.

Where a factual and legal causal link has been found, businesses seeking to reduce the amount of damages payable should consider whether the claimant took adequate action to mitigate their loss (e.g. by changing passwords and immediately alerting relevant stakeholders, such as their bank).

Where credit card data has been compromised, detailed analysis could be undertaken as to whether the harm in question stemmed from a fraudulent use of the particular information released in the data breach or whether the fraud occurred as a result of another instance in which that financial data had been exposed (e.g. a prior cyber-attack).

Litigation Defence Toolkit – Lesson 4: explore applicable quantum arguments

The quantum of damages to be awarded in the event of a data breach is largely untested in the English courts. As a result, businesses have a variety of novel arguments (some drawn from US jurisprudence) at their disposal.

What damages can you claim for?

The forms of compensation sought by claimants tend to vary in line with (i) the type of data which is the subject of the action – commercial data or personal data – and (ii) the arrangements that were in place between the claimant and defendant in relation to the data in question.

The **traditional forms of direct compensation** sought by claimants fall into the following categories:

Form of Compensation	Explanation
Damages in contract: the "expectation" measure	An unauthorised processing or release of data may breach contractual arrangements between the claimant and defendant. Such arrangements could include online terms and conditions governing the use of personal information provided via a website, or a confidentiality agreement between businesses seeking to protect a class of confidential information. Where parties to a contract have negotiated and agreed the terms governing how confidential information may be used, their respective rights and obligations are then governed by the contract and in the ordinary case there is no wider set of obligations imposed by the general law of confidence.
Damage in tort: the "reliance" measure	The basic principle underpinning an award for damages in tort (e.g. for breach of confidence or misuse of private information) is that the defendant should compensate the claimant for the loss the defendant has caused the claimant. So, for example: • If the claimant would have used the information to earn profits, the correct measure of damages is fair compensation for what was lost (see, for example, *Universal Thermosensors Ltd v Hibben* [1992] 1 WLR 840 – though see *damages to account for profits* below). • If the claimant would have licensed or sold the information to others, the correct measure of damages is the market value of the confidential information on a sale or licence between a willing seller and a willing buyer (*Seager v Copydex (No 2)* [1969] 1 WLR 809). • In *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch), a misuse of private information case, loss of control over data was found to be compensable, as the court recognised that data had value and so it followed that damage had actually been suffered.
Damages to account for profits	Claimants may seek to be compensated in the amount of any gain / profit that has been made by the defendant through the unauthorised use of confidential data. This measure of damages is, in practice, oft-sought and rarely awarded. The courts' view (*see Vercoe & others v Rutland Fund Management Ltd & others* [2010] EWHC 424 (Ch), for example) is, in general, that where the data is not clearly proprietary in nature (such as intellectual property in the form of a patent) and there is nothing exceptional to indicate that the defendant should never have been entitled to seek to make money from it, the appropriate remedy is likely to be an award of damages (assessed by reference to a reasonable buy out fee) rather than an account of profits.
"Damage" under section 13 of the DPA 1998	Historically, the English courts held that "*damage*" for the purposes of section 13(1) of the DPA 1998 did not go beyond "*its root meaning of pecuniary loss*", i.e. monetary or other material loss (such as physical damage). Further compensation for "*distress*" under section 13(2) of the DPA 1998 was, on that view, only available where monetary or material loss had resulted from the data breach. The case of *Vidal-Hall v Google, Inc.* [2015] EWCA Civ 311 changed the legal landscape. In that case, the Court of Appeal found that this approach was incompatible with the EU Charter of Fundamental Rights. It found that "*damage*" for the purposes of section 13 of the DPA 1998 could encompass a range of material and non-material damage, including any damage suffered as a result of contravention by a data controller of any of the requirements of the DPA 1998. Given the interpretation given by the courts to the requirements of the GDPR and DPA 2018 (see below), this could include a broad scope of damage. In the recent case of *Aven, Fridman & Khan v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) the High Court followed the example set by the Court of Appeal in *Vidal-Hall* in awarding damages for distress but in this instance the award was also for reputational damage and loss of autonomy. The prospect of considering reputational loss (generally seen in defamation cases) within the scope of "damage" under section 13 of the DPA 1998 will, we suspect, add further breadth to the type of damage in respect of which claimants can seek compensation.

Form of Compensation	Explanation
Loss of control damages under section 13 of the DPA 1998	The judgment of the Court of Appeal in *Lloyd* extended *Gulati* to include "*loss of control*" as a head of damages available under section 13 of the DPA 1998. Importantly, the court confirmed that claimants did not need to show that they had actually suffered any loss because of the breach. It was not relevant that a claimant may not have objected to the loss of control. Businesses now therefore face the possibility of classes of claimants seeking relatively small amounts for data breaches which they do not need to show caused them damage. As in *Lloyd*, small amounts can add up.
Damages under Article 82 of the GDPR and the DPA 2018	Article 82.1 of the GDPR provides that a person who has suffered "*material or non-material damage as a result of an infringement of this Regulation*" should have the right to receive compensation for the damage suffered. Section 169(5) of the DPA 2018, implementing the GDPR, also provides that "*damage*" includes financial loss and damage not involving financial loss, such as distress. The scope of these provisions led the Court of Appeal in Lloyd to conclude that they allowed for claims for the same "*damage*" provided for under the DPA 1998 (above). Indeed, Recital 85 to the GDPR refers to "*physical, material or non-material damage*" to a person as including "*loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*". This effectively opens up businesses to damages claims of a range of kinds and types.
Wrotham Park damages (otherwise known as "negotiating damages" or "user damages")	It was left open in *Lloyd* whether in due course the English courts would consider a separate category of compensation in the form of "user damages", assessed on a hypothetical basis by reference to the amount that the claimant would have, in theory, gained for releasing the defendant from its obligations to prevent the relevant data misuse. Looking forward, this may be a further avenue for compensation that the English courts may explore in data litigation cases.

Claimants can and do claim a variety of other **indirect forms of loss:**

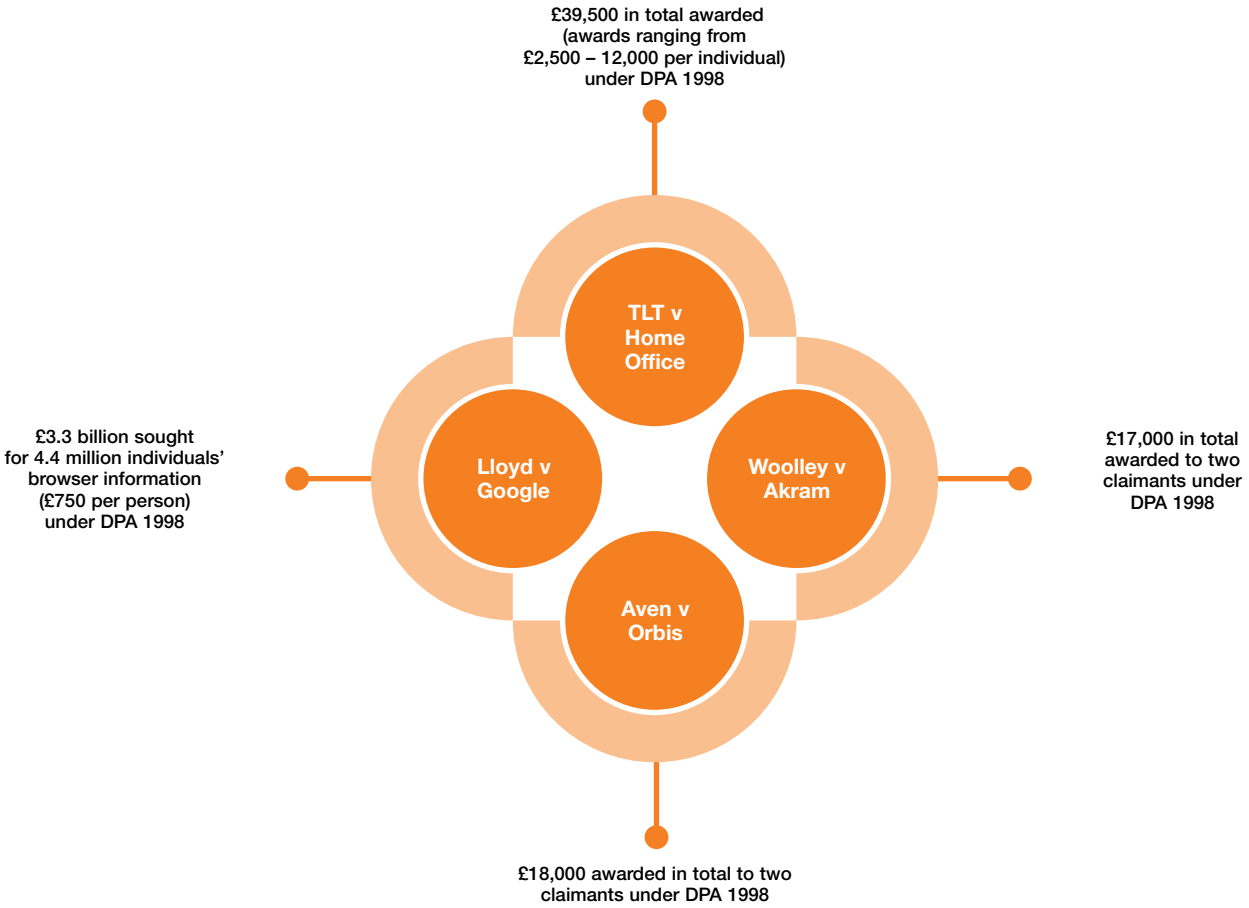
Form of Compensation	Explanation
Loss of option to use data	Owner of data has lost the ability to do with it what he / she chose with the data.
Prospect of later damage	The prospect that the misuse or breach has increased the likelihood of future data theft or misuse, which may cause loss.
Loss of option to negotiate	By losing control over relevant information, the data owner has been deprived of the opportunity of haggling a lower price for the service which has led to the loss of data.
Diminished value of information	The extent to which the information has lost its value now it is in the public domain, or because of the misuse.

Indirect Claims

Can defendants exploit data valuation economics?

Where the valuation of data does not rely on a set tariff or uncontroversial calculation method, it is often open to challenge by defendants. Empirically calculating the damage caused by the loss of control over information is difficult: in each instance it must take into account, among other things, the nature of the information, the confidentiality attached to it and the preferences of the holder.

Claimants for loss of control over data have sought varying (and potentially inconsistent) amounts of compensation, demonstrating precisely how difficult it can be to value data.



Consumer valuations of data can differ significantly from commercial valuations, and indeed can vary hugely as between different individuals. These variations do not necessarily correlate with the sensitivity of the data – for example, consumers may not value sensitive personal data (as defined in the GDPR) more highly than other forms of personal data.

A well-advised defendant will therefore seek to draw to the Court's attention any weaknesses in the way a claimant has sought to attribute value to his / her data.

a) Fragments of data may have little value by themselves, and it may not be possible to attribute significant value to data which was only disclosed in part.

b) In relation to personal data, one of the key difficulties with identifying an uncontroversial value is the "*privacy paradox*" – the often-substantial divergence between consumers' stated preferences for privacy and their behaviours with respect to the disclosure of information. A claimant may value his / her data highly in the event of a claim, but otherwise have freely published it on social media. There can also be a significant divergence in the value attributed to the same data by different people, and so sample size is key where valuation relies on survey-based techniques.

c) The claimant's valuation of the relevant data may reference its market value where in fact there is no market (e.g. for sale of the data to an advertising company). This is particularly important in cases (such as the *Lloyd* case) involving the loss of personal information – it is unlikely that the claimants in those cases would have sought to sell the information that is alleged to have been lost.

d) The claimant may have ignored any benefits accruing to him / her because of the loss of that control. For example, the unauthorised use by an online search engine of personal data may lead to consumers being given targeted discounts on purchases, or advertisements that are better tailored to their requirements,

A well-advised defendant will therefore seek to draw to the Court's attention any weaknesses in the way a claimant has sought to attribute value to his / her data.

and improvements to their online experience.

e) Where the claimant calculates a premium for data privacy, that may assume that he / she would have paid to keep data private. Many products, such as Google and Facebook, are free to use, and so the court will be unable properly to conceive the value of information as a premium attached to the use of such products, which ought to be refunded in the event that control over data is lost.

f) Where an award of damages is ordered to compensate the claimant for distress there could be an argument, based on Warby J's comments in Orbis, that the amount awarded is dependent on the claimant's character. In his judgment, Warby J accepted that the claimants had suffered distress as a result of the disclosures complained of but, in his assessment, each claimant was of a "*robust character, not given to undue self-pity*" and counsel for the defendants were right to request only "*modest*" damages for distress [199].[1]

Quantifying Data

Using quantum arguments in litigation

Where there is controversy with respect to the valuation of data, defendants ought to put their own views to the court as to what the relevant data was actually worth. They would generally do this by obtaining the evidence of an expert on the valuation of data, and placing the expert's report before the court.

Experts employ a range of techniques to value data, comprising behavioural economics, consumer survey and industry behaviour analyses. Assistance from data valuation experts is likely to be critical. Each of these should be considered carefully to determine whether it may be relevant on the particular facts of a case:

Policy appraisal-
Where a valuation is determined using techniques seeking to value lost time and / or inconvenience caused by data loss.

Consumer surveys-
Surveys of this kind focus on what the consumer would have done and analyse the historic behaviour of the consumer to build a model of preferences. More sophisticated consumer surveys, such as conduit surveys, allow experts to infer how much the loss of private information might be worth to an individual.

Market-based techniques-
There are several options for identifying the market value of data. For example, one could analyse the amount an advertiser is willing to pay for information sold to it or the value placed on data when it is sold from one organisation to another.

Cost-based techniques-
The method which takes into account market costs for consumers. For example, what is the value of the consumer's lost time resulting from the breach?

Econometric analysis-
The analysis of large datasets and use of statistical and mathematical modeling can provide insight into human behaviour around data.

Dark-web-
Though potentially unreliable, reviewing the value of data on the dark web may provide an insight into how data can be valued and monetised.

Insurance bench markers-
The analysis of how much an individual would be willing to pay to protect their information is another method for placing an economic value on data.

Risk simulation-
A combination of other techniques (including insurance benchmarks, market-based techniques etc.) to compare the estimate of damages with the likelihood in any case that damage will occur, to reach an overall valuation.

Natural experiments-
A method whereby consumer behaviour is reviewed in set scenarios. For example, if there has been a disclosure of consumer information to third parties, has there been any change in the consumer's behaviour as a result? If the consumer behaviour doesn't change this might show that the data wasn't highly valued.

1. For a useful exploration of some of these points, see Altuglu, Hitt, Hussain and Bergolis (2019), *"Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions"*.

Where one or more of these techniques values the relevant data at less than might have been alleged by a claimant, defendants have a range of options:

- Where the overall quantum of a claim is relatively low, they may seek to settle it to avoid incurring further cost.
- Where it is high overall, but each individual claimant in a representative group is only seeking a small amount, a defendant may seek to argue, pursuant to the principles in *Jameel v Dow Jones* [2005] EWCA Civ 75, that the claim ought to be struck out or summarily dismissed on the basis that it is "not worth the candle".
- Defendants may also argue that the costs of pursuing the claim would be disproportionate to its value, or that the losses were trivial and the action served only to enhance the financial interests of the claimant's lawyers and / or litigation funders.
- It may be possible to argue that the claim did not meet the threshold of seriousness applicable under Article 8 of the European Convention on Human Rights and in the DPA 2018.

Conclusion

Whilst each case involving the loss of control over data will stand or fall on its own facts, defendants to such claims typically have, in our view, a range of options for defending them. These include arguments about causation or evidence of the facts alleged.

Prudent defendants would do well to add quantum arguments to their armoury. Such arguments may show that the economic value of lost data is not as significant as might otherwise have been claimed.

Far from the current "*finger in the air*" exercise used by the courts, we consider that the valuation of data will become a hotly contested area of expert debate in the coming years. We would advise that businesses seek expert guidance from counsel who have experience of making such arguments so that they can make the best possible use of all options open to them in defence of claims to which they are subject.

CLIFFORD

CHANCE

CONTACTS

AUTHOR

Haafiz Suleman
Senior Associate
London
T: +44 207006 4348
E: haafiz.suleman@
cliffordchance.com

Kate Scott
Partner
London
T: +44 20 7006 4442
E: kate.scott@
cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ