Milestone UK court ruling on data protection liability

Date : June 26, 2015

Executive Summary

The UK's Court of Appeal gave a very important judgment in March in a case concerning Google's internet behaviour tracking through a browser where it found that:

- Misuse of private information is now classified as a tort, thereby in this case enabling proceedings to be issued against a party outside the jurisdiction of the UK;
- Financial compensation for distress caused by breaches of the Data Protection Act 1998 ("the DPA 1998") may now be claimed, despite there being no monetary loss, the UK legal provision which had to date prevented this having now been disapplied;
- It is arguable that browser-generated information can be used to identify an individual (i.e even without the ability to identify an individual by name) and therefore constitutes personal data under the DPA 1998, thereby in this case also enabling proceedings to be issued against a party outside the jurisdiction of the UK; and,
- The prospect of more compensation claims for distress is likely - good compliance to prevent breaches of the DPA 1998 can help minimise the potential for claims.

This case is particularly important because litigation for data protection infringements is rising steadily. We reported previously on privacy class actions here concerning the Schrems case, and here concerning consumer associations in Germany, and we also talked about it in one of our Cordery TV YouTube videos.

Following this ruling (Google -v- Vidal-Hall/Hann/Bradshaw, 27 March 2015), the legal footing upon which to obtain compensation in court claims for data protection infringements has moved forward significantly and may pave the way in general for class actions.

Whilst last year's privacy legal headache for Google was the Right To Be Forgotten, this year's headache for them is the Right To Compensation For Distress!

Background - General

Three individuals who used the Apple Safari internet browser brought court claims in the UK in 2013 against Google after discovering that between 2011 and February 2012 Google had circumvented the browser's default security settings and collected private information about these individuals' internet usage without their knowledge or consent, referred to as the so-called "Safari workaround".

Background - Technical

Since the summer of 2011, all versions of Safari have had their default security settings set to block third-party cookies, mainly to prevent advertising-related tracking without the knowledge/consent of the user. The default setting ensures that cookies from third-party advertisers are not placed in users' browsers unless the user actively chooses to change their security settings and enable them.

Google however bypassed the default privacy settings by implementing the Safari workaround, under which temporary third party cookies could be installed on users' systems and for browser-generated information ("**BGI**") to be collected from the cookies. The cookies were applied to track users' online activities and this information was then used to group individual users into categories. The information was used by Google's "doubleclick" advertising service, allowing advertisers to target advertisements based on the interests of the three individual claimants. Google's publicly stated position was that BGI tracking could not be conducted for Safari users unless they had opted to enable cookies.

Background - Legal

The claimants each brought claims against Google for: breach of confidence; misuse of private information; and, breach of statutory duty under the **DPA 1998**, for the tracking and collating of information relating to the claimants' online behaviour without their knowledge or consent. In respect of their claims for misuse of private information and/or breach of confidence, the claimants alleged that their personal dignity, autonomy and integrity were damaged, for which they were claiming damages (i.e financial compensation) for anxiety and distress. In respect of their claims under the DPA 1998, they were claiming compensation under the DPA 1998 for damage and distress.

In neither case was there a claim for so-called pecuniary loss (generally-speaking a pecuniary loss is one that can be measured in money terms) - and not even a nominal loss could be identified, as has been in previous cases. Plus, the claimants were also claiming so-called "aggravated damages" (generally-speaking this is additional compensation where damage has been increased by the manner in which the wrong was committed) on the basis that, either, Google ought to have been aware of the operation of the Safari workaround, or, Google was aware of the operation but chose to do nothing about it.

In bringing these claims the claimants faced, amongst others, two main legal hurdles:

- First, because the entity they needed to sue (Google Inc) is outside the jurisdiction of the UK, the claimants could only proceed with the UK High Court's permission to serve proceedings abroad. Under UK civil rules of procedure, a claim can only be served outside the jurisdiction if, amongst other things (including whether there is a serious issue to be tried - see later below on this), it falls within a limited number of so-called "jurisdictional gateways". Put very simply, in this case the claimants had to persuade the court that misuse of personal information should be classified as a tort (i.e a civil wrong) in order to get through one of these gateways;
- Second, because the claimants were claiming for compensation that was not pecuniary loss, there was an issue of interpretation of the term "damage" under the DPA 1998, where the question was whether there can be a claim for compensation under the DPA 1998 without pecuniary loss.

The High Court ruled in favour of the claimants, allowing proceedings to be served abroad. Google then appealed against this ruling, with the Information Commissioner's Office (the UK data protection regulator, the ICO) acting as an intervening party.

The Court of Appeal Ruling - General

The Court of Appeal (the Court) made very significant determinations not only with regard to these two main issues (whether misuse of personal information is a tort, and whether there can be a claim for compensation without pecuniary loss), but also as regards the issue of whether BGI could be considered as "personal data" under the DPA 1998.

The Court of Appeal Ruling - Misuse of Private Information as a Tort

Significantly, for the purposes of data protection rights, the Court held that the misuse of private information is a tort.

Through a complex analysis of the history and evolution of common law and equitable remedies, the (UK) Human Rights Act 1988 (in particular Article 8 on the respect for private and family life, and, Article 10, on the freedom of expression), and, private international law, with detailed reference to recent UK case-law, the Court arrived at the conclusion that causes of action before the courts for breach of confidence and actions for misuse of private information are clearly distinguishable because they are based on different legal foundations and protect different legal interests.

In essence, according to the Court, legal redress for misuse of private information is to be considered a tort even though it grew out of the law of the breach of confidence, whereas a claim for breach of confidence is not a tort because of its particular history. The Court was at pains however to say that this reading of the law "does not create a new cause of action. In our view, it simply gives the correct legal label to one that already exists"

According to the Court, “with [one] possible exception […] this is the first case in which the 'classification' question has made a difference.” The “difference” here, which is the key significance for the purposes of litigation for data protection infringements, and despite the Court’s downplaying of this as a matter of simply correct legal labelling, is that in such cases service can now be effected against non-UK defendants out of the jurisdiction. Casting the litigation net out can now therefore be done far more widely.

The Court of Appeal Ruling - Damage and Compensation

Also very significantly, and arguably the most important part of the ruling for the purposes of data protection rights, the Court held that compensation can be awarded even where there is *no* pecuniary loss. To achieve that result, in a bold move and legally complex manner, the Court *disapplied* the relevant section of the DPA 1998 in order to address what the Court saw as a legal incompatibility between UK law and EU law so as to give full application to EU law.

As explained above, the claimants did not suffer any pecuniary loss. Instead, they alleged that they had (mainly) suffered “distress” due to the tracking and collating of information relating to their online behaviour without their knowledge or consent, for which they sought (financial) compensation. The problem for them was how to be able to legally claim this because the DPA 1998 requires that damage is suffered for compensation to be payable, which in effect limits any right to claim non-pecuniary damages.

This triggered the issue of whether the UK had properly implemented Article 23 of EU Data Protection Directive 95/46 (the Directive) into UK law, i.e into Article 13(2) of the DPA 1998. That meant deciding the following in turn:

- Whether Article 23 included non-pecuniary loss (i.e compensation for “distress”) within the term “damage”; and,
- If the UK had not properly implemented Article 23, the next issue was whether Section 13(2) should be disapplied in so far as it is incompatible with the Directive non-pecuniary loss obligation.

Implementation of Article 23

Article 23(1) of the Directive requires EU Member States to provide for individuals “to receive compensation from the [data] controller for the damage suffered” due to a breach of the Directive. Section 13(2) of the DPA 1998 implements this article by providing an entitlement to compensation from a data controller for “distress” suffered due to a breach of the data protection rules, if, under Section 13(2)(a), “the individual also suffers damage by reason of the contravention […]” or, under Section 13(2)(b) “the contravention relates to the processing of personal data for the special purposes”. Therefore, under Section 13(2)(a), damage has to be suffered as a pre-requisite in order to get compensation, which broadly speaking has been the approach of the UK (and Irish) courts to date in litigation in this field.

According to the Court’s interpretation, “damage” in Article 23 of the Directive must be given a wide meaning, i.e Article 23 of the Directive does not distinguish between pecuniary and non-pecuniary loss. The Court reached this conclusion on the basis that what the Directive purports to protect is privacy rather than economic rights and that it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded so as to cause them emotional distress but not pecuniary damage.

Construction of Section 13(2) DPA

This then led to the issue of whether Section 13(2) of the DPA 1998 could be construed consistently with the meaning of Article 23. The Court found that this was not possible and reasoned that this was because section 13(2) specifically prescribed the circumstances in which an individual who suffers distress by reason of a contravention of the requirements of the DPA 1998 by a data controller is entitled to compensation. Parliament (in the UK) had deliberately decided *not* to permit compensation for distress in all cases, albeit for reasons that were indiscernible to the Court. Instead, Parliament had permitted compensation for distress only in certain carefully defined circumstances (i.e 13(2)(a) and 13(2)(b)). Accordingly, the Court ruled that it should not, under the guise of interpretation, subvert Parliament's clear intention to provide section 13 of the DPA 1998 with a different meaning

to that of Article 23.

Disapplication of Section 13(2) DPA

Because the Court could not reach a consistent construction between Section 13(2) of the DPA 1998 and Article 23 of the Directive, it had to consider whether section 13(2) should instead be disapplied in so far as it was incompatible with Article 23. The Court referred to the principles established under recent UK case law on disapplication which were as follows:

- *Where there is a breach of a right afforded under EU law, Article 47 of the EU Charter of Fundamental Rights (the Charter) is engaged, namely the right to an effective remedy and to a fair trial;*
- *The right to an effective remedy for breach of EU law rights provided for by Article 47 embodies a general principle of EU law, and, subject to exceptions, that general principle has so-called "horizontal effect";*
- *In so far as a provision of national law conflicts with the requirement for an effective remedy in Article 47, the domestic courts can and indeed must disapply the conflicting provision; and,*
- *The only exception to the foregoing is that the court may be required to apply a conflicting domestic provision where the court would otherwise have to redesign the fabric of the legislative scheme (which is a task for Parliament).*

The Court of Appeal considered the present case fell squarely within these principles. Article 47 was engaged as a result of the claimants' claims that their rights under the Charter had been infringed, namely Article 7 (the respect for private and family life) and Article 8 (protection of personal data). And so, according to the Court, all that was required in order to make section 13 of the DPA 1998 compatible with EU law was the disapplication of section 13(2). This did not mean that the Court had redesigned the fabric of the legislative scheme, nor did this approach permit the Court to subvert Parliament's desired interpretation of section 13(2).

The upshot is that, because the Court considered that there is no requirement under Section 13 for financial loss to be suffered before a claim can be made, accordingly, from now, if an individual can demonstrate that a breach of the DPA 1998 has caused them distress, they will be entitled to bring a claim under Section 13. The removal of the requirement for pecuniary loss therefore significantly widens the potential number of individuals who might be entitled to bring a claim.

The Court of Appeal Ruling - Serious Issue To Be Tried: Is BGI Personal Data (Direct and Indirect Identification)?

As referred to earlier, because the entity they needed to sue is outside the jurisdiction of the UK, the claimants could only proceed with the UK High Court's permission to serve proceedings abroad. Under UK civil rules of procedure, a claim can only be served outside the jurisdiction if, amongst other things (included the abovementioned tort classification issue), there is a serious issue to be tried on the merits of the claim, which means that claims must raise substantial issues of fact or law or both.

In this matter a serious issue to be tried was raised, which had two aspects: firstly, whether the BGI was to be considered as "personal data" under Section 1(1)(a) of the DPA 1998 when looked at in isolation; and, secondly, if the answer to that question was negative, whether the BGI amounted to "personal data" under Section 1(1)(b) of the DPA 1998, at least in so far as the data concerns users in respect of whom Google also held account data, e.g because the user holds a Gmail account.

For the sake of clarity, the Court did not have to answer these two questions for the purpose of deciding whether proceedings could be served abroad or not, but instead, it simply had to decide whether there was a serious issue to be tried that BGI is "personal data" under the DPA 1998. In the event, the Court decided that this was indeed a serious triable issue.

Section 1(1) of the DPA 1998 provides that personal data "means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller." Therefore, there are two forms of identification of an

individual, i.e direct and indirect.

As regards direct identification, citing both the regulatory guidance (Opinion) of the EU's Article 29 Data Protection Working Party and European Court of Justice case law, the Court ruled that the claimants' case that the BGI data on its own identifies the claimants (and so constitutes "personal data") was certainly arguable. The Court's summary of the claimants' argument was that identification for the purposes of data protection is about data that "individuates" the individual in the sense that they are singled out and distinguished from all others. It is immaterial that the BGI does not name the user - the BGI's technical elements (browsing histories and information derived from the "doubleclick" cookies) singles out the users and therefore directly identifies them to Google.

As regards indirect identification, two aspects were addressed:

- The wording of Section 1(1)(b) of the DPA 1998 where the Court interpreted this as appearing to only be concerned with whether data "can be used" to identify an individual user, i.e what matters is whether Google has other information actually in its possession which it could use to identify the subject of the BGI, regardless of whether it does so or not; and,
- The potential identification of the claimants as persons having the characteristics to be inferred from the targeted advertisements by third parties viewing the claimants' screens. Google argued that the knowledge of a third-party was not likely to come into Google's possession and so this information could not fall within the Section 1(1)(b) DPA 1998 definition of data. Against this the claimants argued that the knowledge of third parties cannot be excluded from the issue of identification under Section 1(1) of the DPA 1998. Both sides relied on a UK House of Lords case to support their arguments. Here the Court didn't really tackle the issue head-on, possibly because of the difficulties in correctly interpreting the UK House of Lords case in question, and stated that the issues were "neither clear-cut nor straightforward". Because the Court had already concluded that there were serious issues to be tried in relation to Section 1(1)(a)&(b) it did not see that it was necessary to say more than it was not persuaded that the issue was not arguable and that the issue was best left to be determined after the facts have been found and after full argument at a trial.

The upshot was that, because the Court concluded that it was clearly arguable that the BGI was personal data under Section 1(1)(a)&(b) of the DPA 1998, the claimants could proceed with the UK High Court's permission to serve proceedings abroad.

Commentary

In terms of next steps this judgment allows the claimants to serve proceedings against Google in the US to be followed by a trial in England where the claimants may now go ahead and claim for their alleged non-pecuniary losses. Important issues like whether the BGI constitute "personal data" will also be determined at that trial. And any such trial could of course itself be subject to appeal on any number of issues. Quite when that trial will take place is anybody's guess for the moment.

One big question is whether this will lead to a substantial class-action case against Google. There are many Safari users in the UK. One major upshot in any event is that, because of the disappearance of the pecuniary loss requirement, there could well be an upturn in litigation in general for infringements of the DPA 1998, especially in cases where a data breach involving many thousand individuals occurs, which could go the route of a class-action or which could end up as thousands of small claims.

The news regularly reports on data breaches, for example, one such matter that has been in the news earlier in the year concerns private pension data that has allegedly been passed on by data firms without their customers' knowledge and which ended up in fraudsters' hands who then used it to target people. This is a case that the ICO is currently investigating, and, if it finds that there has been a breach is the kind of case that could typically then yield a court case for compensation for distress caused even if no money was lost.

In terms of so-called limitation periods, it should be noted that it will be possible to bring claims for data breaches up to six years - tens of thousands of people in the UK are estimated to have used Safari in the relevant period of September 2011 to February 2012.

This also means that data controllers processing sensitive personal data will need to be more careful than ever as they will be at risk in particular due to the nature of the data that they hold and the likelihood of distress that might be caused in the event of an infringement of the DPA 1998. Sectors such as the health sector that have been in the ICO's particular spotlight for data breaches, where the nature of the data is of an especially sensitive type, will need to be very vigilant otherwise they might be the subject of the double ignominy of an ICO fine (which can now also be higher in the magistrates' courts) and a consequent lawsuit seeking damages.

It should also be noted that the right to compensation and liability as set out under Article 77 of the proposed EU Data Protection Regulation amends Article 23 of the existing EU Directive by making specific reference to "material or immaterial" damage, and, this right now also incorporates damage caused by processors - the latest version of the proposed Regulation, for which there has been "general approach" agreement by the (EU) Council, can be found here.

There will also no doubt be some issues for which judicial guidance and clarity need to be sought. The Court itself recognized this concerning its labelling of misuse of private information as a tort, and the judges remarked that they were conscious of the fact that there may be broader implications arising out of their categorization as regards limitation periods and vicarious liability.

Other parts of the DPA 1998 have been persuasively argued by some to not be in conformity with the existing Directive, so could the Court's use of disapplication in this case point the way to its use again in other cases on related issues ?

Finally, the current government is examining the issue of repealing the Human Rights Act with a view to replacing it with a British Bill of Rights. Because no detailed plan has been set out yet speculation can be wide. So, for example, if a British Bill of Rights doesn't contain rights that are equivalent in part or whole to Article 8 (respect for private and family life) and Article 10 (freedom of expression), what would be the impact of this on the newly labelled tort of misuse of private information ?

The message of this judgment from a compliance perspective is in any event clear - data protection compliance is now even more of a priority in light of the extra risk that a breach may now entail. Organisations are therefore encouraged to do the maximum to minimize the potential for damages claims - it is worth a reminder here that the DPA 1998 does allow for a defence where it can be shown that reasonable care was taken to comply with the DPA 1998 - and it might be worth checking insurance policies too.

For more information contact André Bywater or Gayle McFarlane with Cordery in London where their focus is on compliance issues.

André Bywater, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Gayle McFarlane, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 118 2700