Misuse of information — the floodgates open

Stephanie Pritchett and Ben Wootton, Data Protection and Technology Lawyers, Pritchetts Law, examine the issues raised by the landmark ruling in* Vidal-Hall and Ors v Google*, and advise on the measures to take to account for the increased risk of claims

The global shift in business towards ever increasing levels of data analytics carries certain compliance risks — as Google has recently discovered.

In *Vidal Hall & Ors v Google Inc*, the company faced allegations of misuse of data — specifically, it was said to have extrapolated certain personal data for data analytics use without the prior consent of its users.

The Court of Appeal's decision — to find in the claimants' favour — has wide implications, and is likely to lead to a greater number of compensation claims for breach of the UK Data Protection Act 1998 ('DPA').

Earlier at the High Court

In *Vidal-Hall and Ors v Google Inc* [2014] EWHC 13 (QB) (January 2014), the UK High Court heard claims against US-based Google, by three users of Apple's Safari browser. The individuals claimed that between mid-2011 and February 2012, Google had used internet cookies to collect private information about their web browsing history without their knowledge and without first gaining their consent.

Such information is usually known as 'browser generated information' ('BGI') and is gathered by organisations like Google for the purposes of:

- allowing a website to be tweaked to improve a user's experience, for example to adjust a site to a mobile user or for a foreign user;
- providing information in aggregated form to its advertisers (e.g. via Google's 'DoubleClick' advertising service, which reportedly holds as much as 77% of market share); and
- better understanding user browsing habits in order to more effectively target advertising at website users.

The website tracking and collection of BGI was in breach of Google's publicly stated privacy policy at that time.

The claimants issued claims against Google for misuse of their private information, breach of confidence and breach of the DPA and sought a damages award under the DPA.

In a landmark ruling, the High Court decided that the three claimants, resident in England, could bring claims against US-based Google Inc for misuse of private information and breach of the DPA.

Google appealed the case arguing that, as a corporation registered in Delaware, and with its principal place of business in California, the UK courts did not have jurisdiction to hear the claims made against it.

What data were at issue?

Once set on a user's device, Google's 'DoubleClick ID' cookie allowed the company to know when the particular browser visited a site displaying an advert from Google's advertising network. It was then possible for that user specific browser to be correlated with the BGI.

This correlated data revealed various pieces of information: the site and the pages of the site visited, the date, time and duration of the visit, the time spent on each page, the adverts viewed and where they were placed, and the IP address which often indicates the town or city in which the device is located. Google could therefore, over time, establish the order in which websites were visited and the frequency of those visits.

Google was able to obtain information relating to people's internet surfing habits, interests, hobbies and pastimes, news reading habits, shopping habits, social class, racial or ethnic origin, political affiliation or opinion, religious beliefs, trade union membership, physical health, mental health, sexuality, sexual interests, age, gender, financial situation, and geographical location.

It was reported that Google also aggregated browsers displaying

(Continued on page 12)

(Continued from page 11)

sufficiently similar patterns into groups, enabling advertisers to select which groups they wanted to direct their advertisements to.

Both the High Court and later the Court of Appeal considered that this information could be personal data, and therefore, if Google could not demonstrate they had consent to process that data, there was a potential for there to be a breach of the DPA.

The Court of Appeal case

In *Vidal-Hall et al v Google Inc* [2015] EWCA Civ 311 (27th March 2015) (copy available at: www.pdpjournals.com/docs/88447), the Court dismissed Google's appeal.

The Court found that the claimants had established that there was a serious issue to be tried on the merits of the claim. The Court also said there was a good case that their claims came within one of the jurisdictional 'gateways' under the UK Civil Procedure Rules (CPR 6.36 and Practice Direction 6B) on the grounds that misuse of private information could be classified as a tort for the purpose of service out of the jurisdiction. In all the circumstances of the case, England was the most appropriate forum for the dispute and the Court should exercise its discretion to permit service out.

The Court upheld the previous judgment of Mr Justice Tugendhat in the earlier High Court case, which had created a tort of misuse of private information.

Additionally and worthy of note, the Court found that the claimants could make a claim for compensation under the DPA where distress has been caused without any pecuniary loss — and that BGI constituted 'personal data' for the purposes of DPA claims.

Impact on the definition of 'personal data'

A person's online activity as captured via cookies creates a basic set of characteristics of their online browsing behaviour and basically identifies their PC, or mobile handset. At first glance, these BGI data are relatively unsophisticated, designed purely to enhance the user experience. However when analysed, and particularly if combined with other types of data held by a business, the level of personal data revealed can easily discern a personal fingerprint.

The UK DPA states 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[…]'.

The Court decided that in basic terms, anonymised and/or aggregated data could still be 'personal data' within the meaning of the DPA if a person's identity can be extrapolated from that data when combined with other data within the data controller's possession.

It was 'clearly arguable', said the Court, that the BGI could constitute personal data under section 1(1)(a) of the DPA, because although Google could not identify a particular user by name, it could identify particular browsers. The Court said (at paragraph 115 of the judgment):

'*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 singles them out and therefore directly identifies them for the purposes of section 1(1)(a) of the DPA'.*

However, it was not so clear whether the BGI constituted personal data under section 1(1)(b) of the DPA. The Court examined:

- whether the BGI combined with the Gmail email account data held by Google enabled identification of an individual; and
- whether individual users could be identified by third parties who accessed their device and could then learn something about them as a result of the targeted advertising.

Google argued that it had no intention of amalgamating the information to identify individuals, but the Court of Appeal rejected this argument, taking a purposive interpretation of the legislation and on the basis that the DPA does not require identification to actually take place. As to the second issue, the Court viewed it to be difficult and deferred it to a further trial.

As the Court of Appeal had already found that there was a serious issue to be tried in relation to section 1(1)(a) DPA, it decided that the section 1(1)(b) arguments should be determined at trial (at paragraph 133).

There could be some very interesting further findings in relation to the identification issue. Until then, much remains uncertain.

Damages — the issues

Data controllers will want to know whether there is a greater chance of compensation claims from individuals following this case.

Section 13(1) DPA states that an individual who suffers damage by reason of any contravention of the DPA by a data controller is entitled to compensation for that damage. Section 13(2) DPA states that an individual who suffers distress by reason of any contravention of the DPA by a data controller is entitled to compensation from the data controller for that distress if: (a) the individual also suffers damage, or (b) the contravention relates to the processing of personal data for the purposes of journalism, literature or art ('special purposes').

The Court of Appeal was required to consider whether damages under Section 13(2) of the DPA could be awarded in circumstances where the claimants had not suffered any actual financial harm. It found that they could.

The Court was also required to consider submissions from the Information Commissioner's Office ('ICO'). The ICO said that its previous guidance on Section 13 of the DPA, which suggested that damages should not be available unless financial harm existed, was incorrect.

The ICO believed that damages should be available in this case.

The Court accepted the ICO's argument, but said that on a literal interpretation, Section 13(2) DPA did not allow damages where there was no financial harm. Despite this, the Courts found that Section 13(2) of the DPA could be ignored as it was incompatible with the equivalent EU requirement under Article 23 of the Data Protection Directive (95/46/EC).

Does 'damage' in Section 13(1) DPA mean financial loss, except for the circumstances set out in Section 13(2)?

In seeking to answer this question, the Court referred to *Johnson v. Medical Defence* Union [2007] EWCA Civ 262 which established that damage in section 13(1) DPA referred to 'pecuniary loss' except in the two instances set out in section 13(2). The Court said it was not bound by *Johnson,* because the corresponding reference to 'damage' in Article 23 of the Directive (on which Section 13 of the DPA is based) could be interpreted as meaning 'distress'. The Courts took a 'purposive interpretation approach', saying that the legislation was designed to protect privacy rights not economic rights.

If 'damage' in Article 23 of the Directive includes non-financial loss, should Section 13 of the DPA be struck down?

The Court considered whether Section 13(2) of the DPA should be struck down as being incompatible with Article 23, in accordance with the principles set out by the Court in the previous case of *Benkharbouche and Janah v. Embassy of Sudan and others* [2015] EWCA Civ 33.

Controversially, it held that it could, because the Section conflicted with the rights guaranteed by Articles 7 (right to respect of private and family life, home and communications) and 8(1) (right to protection of personal data) of the European Convention of Human Rights ('ECHR').

Effectively the Court said that Section 13(2) of the DPA breaches Articles 7 and 8(1), and consequently the claimants in the *Vidal-Hall* case were denied an effective remedy for such breaches.

> ***"Effectively the Court said that Section 13(2) of the DPA breaches Articles 7 and 8(1) and as a result, it denied the claimants in the Vidal-Hall case an effective remedy for such breaches."***

Misuse of private information now a 'tort' under UK law?

In order to be able to serve proceedings on Google in California, the *Vidal-Hall* claimants needed to satisfy a relevant 'gateway' — i.e. to show that their claims related to an actionable tort.

Previous case law (*Wainwright v Home Office* [2003] UKHL 53, [2004] 2 AC 406) had established that there was no general tort of invasion of privacy, so at the High Court the *Vidal-Hall* claimants argued (and the Court of Appeal agreed) that there should be a tort of misuse of private information.

The Court of Appeal upheld the decision in part on the basis that:

- misuse of private information should be recognised as a tort for the purposes of service out of the jurisdiction;
- this was not a new cause of action, it simply gave the correct legal label to one that already existed;
- while the finding may have broader implications in relation to (for example) remedies, limitation and vicarious liability, these were not the subject of the submissions in the case and such points would need to be considered as they arise; and
- although the classification of the misuse of private information has been the subject of discussion in previous cases, this was the first scenario in which the outcome made a difference. Without the classification, the claimants in this case could not have remedied the civil wrong in the UK courts.

This finding by the Court will of course have an impact on all organisations based outside the UK, opening them up to claims from UK data subjects for breach of the DPA.

What does *Vidal-Hall* mean for our organisation?

Google has confirmed that it will appeal the *Vidal-Hall* case to the Supreme Court. Further, there are numerous legal and factual issues that have been left unresolved by the Court of Appeal's decision.

That said, the case has already caused quite a stir and potentially has far reaching repercussions that all organisations should be aware of.

The impact for Google is that claims can now be brought against the company directly in the UK. Pending the outcome of the appeal, the advent of a lower threshold for compensation claims might create a greater incentive for all data subjects in the UK to bring DPA breach claims against UK data controller organisations of all kinds.

To date, DPA claims have been used more commonly as an add-on to other claims, such as Employment Tribunal cases. The decision means we are likely to see a marked increase in stand-alone DP cases.

Further, such claims are likely to have a greater chance of success, especially where individuals present reasonable arguments that anxiety or distress exist, even if they have not suffered any direct financial loss.

(Continued on page 14)

(Continued from page 13)

In reality, the level of any damages awarded might be small.

What should we do about increased risks?

Risk registers — As it currently stands, there is a greater likelihood of small (and large) claims being brought against organisations, and also of increased legal costs in defending those claims. Internal risk registers should be adapted to reflect this increased risk.

Review how data are segregated within the organisation — If policy has simply been to segregate data internally, this is no longer likely to be sufficient.

If policy is to anonymise all data before supplying it to a third party (in accordance with the ICO's Anonymisation Code of Practice), then organisations must carefully consider whether that third party has its own data that, when combined with the organisation's own, would allow it to re-identify particular individuals. If it can, then there is a risk that the third party is handling 'personal data', and as such needs to meet the requirements of the DPA.

Review staff-facing and public-facing data protection policies — The potential for claims exists where organisations fail to comply with the DPA as well as their own data protection policies. Organisations are therefore advised to regularly review and revise policies.

Review data collection forms — Following this decision, there is a much greater need to focus on fair collection of personal data, including situations where that collection is only for data analytics purposes.

Collecting and analysing personal information can create exceptional market knowledge and be very valuable for organisations trying to better understand customer behaviour. This collection must be underpinned by fair collection processes, adequate collection of consents and proper provision of fair processing information.

Cookie dropping — When using cookies and similar technologies, data controllers must focus on compliant collection and use of personal data.

Conclusion

Some commentators have suggested that the Court of Appeal has simply cleared the path for the case to be tried all over again in full.

Whatever the future holds, it seems clear that the judgment is likely to pave the way for an increasing number of privacy claims relating to online activities.

Those operating a business that relies on personal data gathered from customers' online activities should therefore adopt a cautious approach going forwards.

Stephanie Pritchett leads PDP's training course, Data Protection Essential Knowledge Level 2.

For more details, see www.pdptraining.com

Stephanie Pritchett and Ben Wootton
Pritchett's Law
ben.wootton@pritchettslaw.com
stephanie.pritchett@pritchettslaw.com