# Data privacy: new ruling may change the game for companies' cyber exposures

**A ground-breaking ruling by the Court of Appeal of England and Wales in March 2015 might usher in a new era of data privacy litigation across Europe - with the potential to dramatically increase the level of liability for companies collecting private data.**

## Google v. Vidal-Hall case – a new cookie monster

On March 27th, the Court of Appeal of England and Wales issued a ruling in the case of Google v. Vidal-Hall. The case examined Google's alleged use and sale of browser-generated information (BGI), collected through cookies without the claimant's knowledge or permission. In 2012 and 2013 Google had settled similar allegations in the U.S. for close to USD 40 million. However, until the Vidal-Hall claim, Google had not faced any sanction in Europe.

Highlighting inconsistencies in current international legislation, the Court of Appeal of England and Wales strongly backed the privacy rights of consumers and - for the first time - clearly indicated that financial loss is no longer the threshold necessary for a privacy claim to proceed.

There were four significant issues raised in Google's appeal, each of which was decided in favour of the claimants:

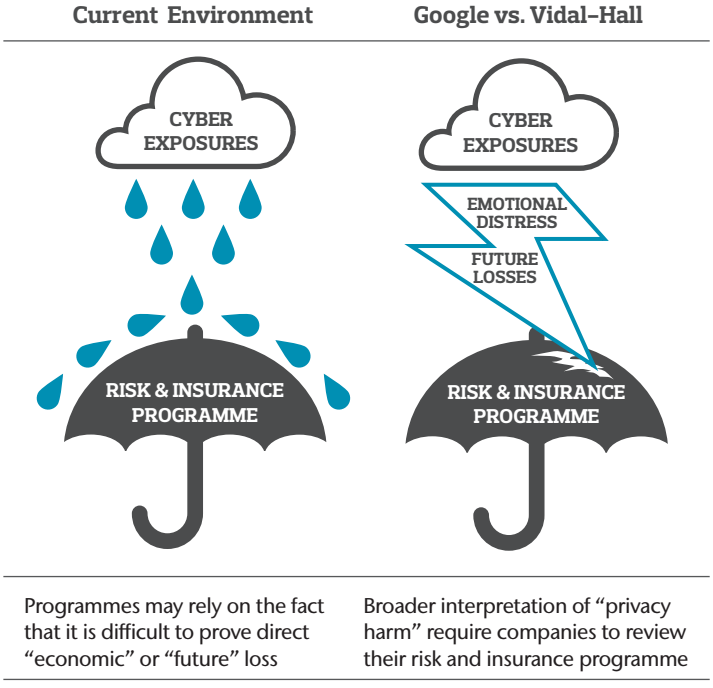
1. The misuse of private information is a tort in and of itself;
2. There can be a claim for compensation without economic loss;
3. Browser-generated information constitutes personal data; and
4. The misuse of such private information can form the basis of legal action.

## Google ruling threatens a wave of privacy litigation: are you exposed?

Prior to this case, European courts tended to mirror the U.S. precedent that "potential future harm" and "emotional pain and suffering" are not actionable damages in privacy litigation without proof of actual economic loss. This ruling has the potential to change that interpretation and opens up consideration of non-financial loss in future privacy litigation cases.

As Jonathan Upshall, Cyber Broking Director for Aon explains, "The ruling offers a much broader interpretation as to what might constitute damage resulting from a breach of privacy and this decision could therefore have significant implications for any company that collects and stores large scale private information from users or customers".

It is important to note that this ruling allows the matter to proceed and be decided upon, as opposed to being an outright dismissal of Google's appeal. Although the final outcome on this particular case is still to be decided, the mere fact that the Court of Appeal has recognised the claimants' right to bring such a claim is a fundamental legal change and may open the floodgates to similar claims.



# Data privacy: new ruling may change the game for companies' cyber exposures

## Implications to reach far and wide

The implications for UK and European companies could be significant, particularly considering the amount of data that is captured by companies online and/or stored digitally.

While presently confined to England and Wales, the ruling also establishes precedent in the E.U.

Upshall suggests that "companies in Europe and worldwide will need to consider even more closely how they collect, use and store private information, and what risk management controls are in place to protect them against potentially costly litigation".

## A looming threat to be managed by business

Upshall cautions that "the current ruling has broadened the definition of what constitutes harm resulting from a breach of privacy and may negatively affect the inherent protection afforded to data controllers. If the new threshold for damages becomes emotional distress and future loss, the impact will likely be far-reaching and costly".

Additional significant scrutiny will be placed on companies' use of online data, while available insurance capacity could also become severely curtailed. It is therefore worth planning ahead for an environment in which regulators will pay far closer attention to the sign-posting, capture and use of private data.

For further details from the Aon team, contact:

**Jonathan Upshall**
Cyber Insurance Broking Director
+44 (0)20 7086 1897
jonathan.upshall@aon.co.uk

**Alistair Clarke**
Cyber Insurance Broking Director
+44 (0)20 7086 7357
alistair.clarke@aon.co.uk

## Aon recommends that risk managers work with their Information Security, Legal as well as Sales and Marketing leaders to review the following aspects of their Cyber risk management programme

### Plan
Review existing data practices and breach plans, and conduct a data skills audit

### Prevent
Work with your cyber insurance broker to review the appropriateness of your existing coverages

### Communicate
Explain data capture and protocols to customers and the market in clear, transparent language