RPC

Technology and cyber risk update

July 2015 edition

Drones – issues for casualty insurers

Public liability, professional liability and commercial combined policies will only cover drone-related risks to the extent that they fall within wording of existing policies which, at risk of stating the obvious, were not developed with drones in mind. more›

Court of Appeal opens door to "distress-only" claims where no financial loss

In an important ruling, the Court of Appeal confirmed that misuse of private information is a tort and rules on the meaning of "damage" under s13 of the Data Protection Act (DPA), allowing claimants to recover compensation for "distress" resulting from a breach of the Act without also having to prove pecuniary losses. more›

AFD Software Limited v DCML

A licensee of postcode look up software was found not to have been in breach of a licence which restricted the use of the software to a "public internet website" when its use of the software was via a password and login protected section of a website. more›

EU general data protection regulation – late, better than never?

Reports of the potential demise of the General Data Protection Regulation following the departure of Justice Commissioner Vivienne Reding appear to have been exaggerated. more›

PNI security breach – aggregation issues

At the time of writing, it appears that a serious data security breach has occurred at PNI Digital Media which provides payment services for online photo processing companies including CVS Photo, Walmart Canada, Tesco and Costco in the US and Canada. more›

Any comments or queries?

Philip Tansley
Senior Associate
+44 203 060 6561
philip.tansley@rpc.co.uk

Christopher Neilson
Senior Associate
+44 203 060 6567
christopher.neilson@rpc.co.uk

Robert Johnson
Senior Associate
+44 203 060 6620
robert.johnson@rpc.co.uk

Alex Hamer
Partner
+44 203 060 6449
alex.hamer@rpc.co.uk

Drones – issues for casualty insurers

Drones – or Unmanned Aerial Vehicles to give them their proper title – continue to be a hot topic in technology circles. If the commercial drone industry fulfils even a fraction of analysts' growth predictions it will become a multi-billion dollar industry in the next 5 to 10 years.

Public Liability, Professional Liability and Commercial Combined policies will only cover drone-related risks to the extent that they fall within wording of existing policies which, at risk of stating the obvious, were not developed with drones in mind. This gives rise to interesting questions (from a lawyer's perspective at least) about the extent to which resulting liabilities will be covered.

Use of drones is being championed in a multitude of industries such as agriculture, infrastructure maintenance, surveying, transport, oil & gas, journalism, and film-making or simply as a "must have" toy. The scalable nature of drone technology means that it can be utilised across a spectrum of businesses, from small "disruptive" technology start-ups to large corporations (such as Amazon's much-heralded plans for drone deliveries).

Whilst dedicated drone insurance policies remain in their infancy, the question arises how traditional liability policies respond to the issues raised by drones. Commercial drones are typically small inexpensive devices under 20kg so do not give rise to significant first party exposures. The main exposures arising from drones are:

- **Liability for personal injury and damage to third party property:** The most obvious area of liability is plainly the risk that the operation (or sudden failure to operate) of a drone will injure people or damage property. Whilst the majority of reported incidents have been minor ones resulting in property damage, instances of unauthorised use near airports and in commercial airspace show that drones can potentially give rise to very significant liabilities. Typically, claims will be brought in negligence and involve the establishment of liability in a similar way to any other tort claim. However, the burden of care on a drone operator will be high so, unless there are unusual circumstances or the injured party is at fault, liability is likely following an incident. Primary liability will typically be on the part of the drone operator (both the individual operator and his employer). However, depending on the nature of the incident, other parties are potentially at risk of liability, such as a third party who has hired the drone
- **Product liability:** Incidents arising from defective drones clearly also give rise to potential liabilities on the part of various entities in the supply chain such as the manufacturers of the platform itself and of components of the system such as the autopilot manufacturer, payload systems and the software/firmware developer
- **Trespass:** Overflight of property will not in itself give rise to a liability in trespass (although it might give rise to a liability in the tort of nuisance or privacy issues). However, the take-off and the landing (particularly where unplanned) do potentially give rise to liability issues arising from access to property

- **Privacy:** The use of drones by journalists leads to obvious privacy concerns but the use of drones in mundane applications, such as surveying can also lead to potential issues. Gathering images in public places or on third party private property potentially constitutes the processing of personal data for regulatory purposes. Unless policies contain specific exclusions of these exposures, this is increasingly an issue for casualty insurers following the recent Google v Vidal Hall decision (see below) which indicated both that breach of privacy is a tort in itself and that the requirement of "damage" for liability claims under Section 13 of the Data Protection Act, does not require the claimant to show physical harm or financial loss
- **Regulatory/criminal investigations:** To the extent that coverage is available for the costs of responding to regulatory investigations, operating drones gives rise to a number of potential exposures:
  - *Health and Safety Executive (HSE):* an incident involving a drone may well give rise to a HSE investigation
  - *Information Commissioner's Office (ISO):* as indicated above, gathering images may involve processing personal data for the purpose of the Data Protection Act and bring the activities within the regulatory ambit of the ICO, which has issued guidance regarding the operation of drones
  - *Civil Aviation Authority (CAA):* drones larger than 7kg are subject to regulation by the CAA. The regulations limit the extent to which commercial drones can fly in congested areas, close to people or property or beyond the line of sight of the operator. Tighter restrictions apply to unmanned aircraft used for surveillance purposes imposing minimum distances from which the drone can approach properties. These regulations will impose liability on the operator of the drone together with additional liability on the "remote pilot" of the drone to satisfy himself that the flight can be conducted safely. To date, at least two drone pilots have been prosecuted by the CAA (for flying a quad-copter drone over busy rides at Alton Towers and loss of control of a drone near an MOD facility, narrowly missing a public bridge)
  - *Police:* misuse of drones can also lead to criminal prosecution under the Air Navigation Order 2009. A recent case involved prosecution of an individual for filming a number of public buildings in London and premiership football matches in breach of the regulatory requirements not to fly over congested areas and/or without line of sight to the drone.

What is clear however is that there are gaps in many of the existing coverages, particularly for the significant liabilities which may arise from the considerable regulation imposed on drone operators (which is likely to increase with the introduction of further EU regulation in 2016). If the market for drones grows as predicted we therefore expect to see an increase in bespoke wordings specifically covering risks such as operator's regulatory exposures, costs of the loss or disappearance of the drone itself and third party contractual liabilities arising from the loss of or defect in a drone.

Back to contents>

Court of Appeal opens door to "distress-only" claims where no financial loss

In an important ruling, the Court of Appeal confirmed that misuse of private information is a tort and rules on the meaning of "damage" under s13 of the Data Protection Act (DPA), allowing claimants to recover compensation for "distress" resulting from a breach of the Act without also having to prove pecuniary losses.

Vidal-Hall and others v Google Inc
The Court of Appeal has handed down a judgment confirming that:

- misuse of private information is a tort
- claimants may recover damages section 13 of under the DPA for non-pecuniary losses
- it is strongly arguable that "browser generated information" collected via cookies may be "personal data" for DPA purposes.

The effect of this case is that individual data subjects may now seek compensation for breaches of the DPA purely by asserting that they have suffered "distress", despite not suffering financial loss.

We expect that this judgment will result in a significant increase in the volume of civil actions brought by individuals under the DPA, either on an individual basis, or as a group (as in *Vidal-Hall*). Distress claims also might be added to wider claims such as defamation and employment disputes.

Additional background and detail:

The facts
Essentially the claim in *Vidal-Hall* stems from the revelation that Google used cookies to collect "browser generated information" (BGI) from users of Apple's Safari web browser. By collecting BGI, Google was able to track Safari users' internet usage in order to target advertising at those users more effectively. For example, Google might direct adverts for a hotel or airline to a user who had been researching a holiday. Safari users had not consented to Google's collection of information generated by their browsers. Alongside claims for misuse of private information and breach of confidence, the claimants sought compensation under the DPA, on the basis that Google's activities had breached the Act. The claimants did not, however, disclose any financial loss.

Legal background
Article 23 of the current EU Data Protection Directive required member states to implement provisions allowing a person who has "suffered damage" as a result of a data protection offence to obtain compensation from a responsible data controller. The UK implemented this requirement through section 13 of the DPA.

DPA section 13 draws a distinction between damage and distress. An individual suffering "damage" may recover compensation for that damage; by contrast an individual suffering "distress" may generally only recover compensation for where he or she also suffers financial damage. In almost all cases, a claimant must therefore show pecuniary loss to recover compensation under section 13.

In J*ohnson v MDU* the High Court rejected the argument that the term "damage" as used in the Directive was not restricted to pecuniary loss, since it referred to any sort of damage recognised

by member states' domestic laws. It found that there was no compelling reason for the term "damage" to be extended beyond pecuniary loss.

The *Vidal-Hall* judgment

The present judgment relates to the claimants' application to serve proceedings on Google outside the jurisdiction. Since the claimants had disclosed no pecuniary loss for Google's alleged breaches of the DPA, (it is not the final judgment on the issues in question) the Court of Appeal was required to revisit the recoverability of non-pecuniary losses under the DPA to decide whether they had an arguable loss.

The court found for the claimants. Since the primary aim of the European data protection regime was to safeguard privacy, rather than economic rights, it would be odd if a data subject could not recover compensation for an invasion of his or her privacy purely because there was no pecuniary loss. Accordingly the term "damage" as used in the Directive should be construed to include non-pecuniary losses.

The court also ruled that it was clearly arguable that the BGI did constitute personal data on the basis that it "individuates", or singles out the individual, and distinguish him from others. This was regardless of the fact that: i) the BGI did not name the individual and ii) Google asserted that it had no intention of linking the BGI with other data that Google held and which could lead to the individual being identified. The court did not have to determine the issue finally – only establish that there was a clearly arguable case. If the case does go to a full trial for resolution, then data practitioners can look forward to some valuable guidance on this issue and questions on "identification" more generally.

Back to contents>

AFD Software Limited v DCML

Introduction

A licensee of postcode look up software was found not to have been in breach of a licence which restricted the use of the software to a "public internet website" when its use of the software was via a password and login protected section of a website. In reaching that decision, the court held that the term "public internet website" did not have any recognised meaning and, as the licensor had not explained what that term meant in the context of the licensee's use, it was for the licensee to conclude that its use was permitted under the terms of the licence.

In addition, the court found that, as the licensee had provided all the relevant facts regarding the use to which it would put the software and, in circumstances where, the licensor's representative had recommended the software, the licensor was estopped from contending that the licensee was not able to use the software as it had done.

The facts

The claimant's postcode lookup software enabled users to enter a postcode into an address form on, for example, a company's website and the software would then autocomplete the rest of the address. The defendant, DCML, licensed the software from the claimant for use on its website and in various call centres for car dealerships.

Prior to DCML purchasing AFD's software, it licensed equivalent software from an alternative provider for a fee of approximately £2,500 per year. When that provider informed DCML that it would no longer be providing the software, DCML undertook research to locate an alternative product. As a result of its research DCML understood AFD's product to be the cheapest and subsequently discussed the product with AFD to find out what it would be used for. AFD informed DCML that the product identified would be suitable for DCML's use and sent an evaluation copy of the software.

DCML decided to purchase a licence for the software. AFD sent an invoice to DCML containing its standard terms, which was duly paid and DCML started using AFD's product in its business. Prior to installing the software, DCML also had to accept AFD terms via a click through text box. DCML continued to licence the software for five years DCML paying AFD a total of £7,475.

In December 2010, AFD contacted DCML to inform them that the costs of their licence would increase as a result of changes to AFD's licensing of the underlying Royal Mail post code data. At that point there were further discussions between DCML and AFD regarding the use to which the software was put. AFD considered that DCML's use was outside the terms of the licence. On 23 December 2010, AFD issued an invoice for retrospective licence fees in the sum of £12m plus VAT. By the time the case came to trial that figure was reduced to £2.5m.

AFD's case was that the Licence Certificate provided that the product was only to be used on "public internet websites" and that DCML's website did not fall within that description because, although the website could be accessed by anyone with an internet connection, the content

could only be accessed by car dealerships via login and password. AFD also alleged that, in the course of DCML's initial enquiries in January 2006, DCML deliberately misdescribed the use that DCML would make of the software.

The judgment

The judge rejected the allegation that DCML had misled AFD in January 2006 and found, on the evidence, that DCML had properly described to AFD the use to which the software would be put and that AFD had recommended the product to DCML on the basis of that description.

The court held that AFD was estopped from contending that DCML was not properly licensed to use the software in the way that it had done. DCML had properly explained what it wanted the software for; DCML had reasonably relied on the recommendations as to the licence terms; DCML had changed its position in reliance on the recommendation made by AFD by licensing AFD's product as opposed to a cheaper alternative; and that reliance was to its detriment if the use amounted to a breach of contract of infringement of copyright.

Further, the use of the phrase "public internet website" was in AFD's terms "not unambiguous" and it was not unreasonable for DCML to conclude its intended use was licensed by it. There was therefore no clause in the licence which forbids the use to which DCML made of the software so the breach of contract claim also failed.

Comment

This case came down to the evidence regarding the conversation between DCML and AFD in January 2006. In particular, the judge found elements of AFD's evidence as to that conversation inconsistent and unreliable. In addition, the judge considered the sums claimed by AFD's were grossly inflated which seems unlikely to have helped AFD.

Although DCML was able to establish a defence of estoppel and that was based on pre-contractual recommendations to DCML by a salesperson, the court did not make any finding that DCML was in breach of the terms of the licence and considered that it was reasonable for DCML to conclude its use was within the terms of the contract.

RPC acted for DCML and its insurers in this case. DCML was awarded a substantial part of its costs on an indemnity basis.

Back to contents>

EU general data protection regulation – late, better than never?

Reports of the potential demise of the General Data Protection Regulation following the departure of Justice Commissioner Vivienne Reding appear to have been exaggerated. Over three-and-a-half years since the process started, it seems like the General Data Protection Regulation may become law as early as December this year.

The Regulation is now in the Trialogue stage where representatives of the European Commission, Council and Parliament will try to agree a final text. Substantial differences still exist between the Parliament's position (which essentially seeks to maximise the protection available for individuals data) and the Council (which has adopted a more business friendly approach). Of interest from a cyber insurance perspective, the Council is proposing the compulsorily notification of breaches within 72 hrs (rather than 24), limit the obligation to notify to "serious" breaches, suggests that compulsory appointment of a data protection officer should be a matter for local regulators and rejects the fines of up to €100m or 5% global turnover suggested by the Parliament (although it has not made a firm counter-proposal on this question).

Given the significant areas of difference and the time taken for the Regulation to reach this stage it remains to be seen whether a final text can be agreed by December. However, it now seems to be only a matter of time before the Regulation becomes law. Attention is now turning to how the "one stop shop" regulatory regime imposed by the Regulation will affect regulators' behaviour. On the one hand will regulators funded by a levy on data subjects attempt to adopt a "light touch" approach in an effort to attract large data processors to their jurisdiction. Conversely, regulators reliant on the income from fines for funding may be encouraged to take a more aggressive approach.

Back to contents>

PNI security breach – aggregation issues

At the time of writing, it appears that a serious data security breach has occurred at PNI Digital Media which provides payment services for online photo processing companies including CVS Photo, Walmart Canada, Tesco and Costco in the US and Canada.

This is a salutary reminder of the potential aggregations risk for cyber insurers if shared platforms such as payment service providers are compromised, as the insurance policies of, not just PNI but its customers are likely to respond to this large breach.

Back to contents>

About RPC

RPC is a modern, progressive and commercially focused City law firm. We have 77 partners and 560 employees based in London, Hong Kong, Singapore and Bristol.

"... the client-centred modern City legal services business."

At RPC we put our clients and our people at the heart of what we do:

- **Best Legal Adviser status every year since 2009**
- **Best Legal Employer status every year since 2009**
- **Shortlisted for Law Firm of the Year for two consecutive years**
- **Top 30 Most Innovative Law Firms in Europe**

We have also been shortlisted and won a number of industry awards, including:

- **Winner – Law Firm of the Year – The Lawyer Awards 2014**
- **Winner – Law Firm of the Year – Halsbury Legal Awards 2014**
- **Winner – Commercial Team of the Year – The British Legal Awards 2014**
- **Winner – Competition Team of the Year – Legal Business Awards 2014**
- **Winner – Best Corporate Social Responsibility Initiative – British Insurance Awards 2014**
- **Highly commended – Law Firm of the Year at The Legal Business Awards 2013**
- **Highly commended – Law firm of the Year at the Lawyer Awards 2013**
- **Highly commended – Real Estate Team of the Year at the Legal Business Awards 2013**

Areas of expertise

- Banking
- Commercial
- Commercial Litigation
- Competition
- Construction
- Corporate
- Employment
- Insurance
- Intellectual Property
- Media
- Outsourcing
- Pensions
- Private Equity
- Real Estate
- Regulatory
- Reinsurance
- Tax
- Technology

14946

Tower Bridge House
St Katharine's Way
London E1W 1AA
T +44 20 3060 6000

Temple Circus
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000

11/F Three Exchange Square
8 Connaught Place
Central Hong Kong
T +852 2216 7000

8 Marina View #34-02A
Asia Square Tower 1
Singapore 018960
T +65 6818 5695