Rising tide of cyber risks could swamp the market

Published 1 September 2015

Growing privacy and cyber liability in the UK will boost the cyber insurance market, but liability insurers will need to examine their exposures if they are to avoid a flood of unexpected claims.

With new technologies, personal data is becoming integral to modern-day life. But attitudes to privacy are changing, and regulatory and legal trends are likely to result in more successful claims for damages following a data breach. For liability insurers this has important consequences. As currently drafted, insurance contracts – ranging from professional indemnity (PI) and directors' and officers' (D&O) to commercial combined policies – are exposed to privacy liability claims. Insurers need to give careful thought to what this emerging class of liability means to them and what action they must take to avoid unintended consequences.

Personal data is becoming more valuable and its usage more complex – big data and new technology will see more and more personal data collected and shared with increasing sophistication. As we increasingly move into the digital age, data protection laws will no doubt evolve. Even now, the EU is considering a new data protection regime, while many aspects of existing data protection law are being tested in the courts.

One important area in which the law is being tested is around the damages a data breach victim is able to claim. Until recently, the Data Protection Act 1998 (the Act) required a claimant to demonstrate a financial loss first before they were able to seek damages for distress. This has proved a significant hurdle preventing many claims for breach of the Act.

However, in recent years the courts have shown an increased willingness to find ways to award damages for breaches of privacy. For example, there have been a number of cases where courts have awarded nominal damages for financial loss in order to award more substantial damages for distress. The Court of Appeal's decision in *Vidal-Hall and others v Google Inc* (*Vidal-Hall v Google*), however, simply cuts through this hurdle and the need for judicial workarounds.

Landmark case

On 27 March 2015, in a landmark decision, the Court of Appeal granted three claimants permission to pursue Google for compensation for distress caused by breaches of the Act. In doing so the court confirmed a new tort of the misuse of private information.

Vidal-Hall v Google concerns Google's allegedly secret collection of the internet usage of Apple Safari users through the use of cookies that circumvented Safari's privacy settings. The claimants claim Google's actions damaged their personal dignity, autonomy and integrity and caused them anxiety and distress. Crucially, they do not claim to have suffered any financial damage.

"What we are now seeing is the emergence of a new class of privacy liability," says Hans Allnutt, Partner at DAC Beachcroft. "*The Vidal-Hall v Google* judgment recognises that individuals should be compensated, even where they have not suffered a financial loss. As a result, organisations now face an increased risk of claims for compensation following a breach of privacy or the Act," he says.

The desire of the courts to compensate individuals for breaches of privacy is shared by the regulator. In *Vidal-Hall v Google*, the Information Commissioner's Office intervened in the proceedings and stated that compensation must be available to people for their moral damage caused by companies' data protection breaches. UK data protection law is also set to change under the proposed EU Data Protection Regulation, which is likely to clarify the situation for damages.

"While still under negotiation, the proposed EU Data Protection Regulation should be much clearer on the type of compensation that can be sought, and I expect the right to claim damages for emotional distress alone will be included. The courts are already moving in this direction with the support of the regulator," says Allnutt.

Many liability insurance policies will indemnify privacy claims under general insurance clauses, cyber extensions or specific wordings relating to data protection or privacy.

"Cyber insurance gets all the attention, but a wide range of traditional insurance policies do provide some cover for data protection and privacy liabilities. There is now a potentially significant exposure under data protection and 'invasion of privacy' clauses for insurers, clauses that have not yet been fully tested in the face of such claims," says Allnutt. "All liability underwriters need to look at how their policies would respond to such claims and whether wordings meet their intentions. They should consider whether they need to amend wordings and ask more questions around privacy, cyber security and the

use of people's private information," he says.

Professional indemnity

The *Vidal-Hall v Google* decision is potentially very significant for professional services firms, many of whom hold large amounts of confidential and privileged client data, as well as data belonging to third parties. For example, a law firm handling a high-net-worth divorce case would hold highly private information relating to their client's spouse, which could potentially expose them to a third-party claim should there be a privacy breach, notwithstanding the spouse not being a client of the firm.

"Solicitors' PI insurers are potentially exposed to data breach or privacy claims through the main insuring clause for losses arising from private legal practice," explains Clare Hughes-Williams, Partner at DAC Beachcroft. "There will be a debate as to whether this exposure is covered by the main insuring clause, and insurers may try to formulate an argument that data breaches do not arise from the normal course of business. However, this is unlikely to be a straightforward argument and it therefore may not be possible to avoid privacy exposures.

"The question will be whether to cover privacy exposures under a standalone cyber insurance policy and exclude them from PI insurance, if this is indeed possible."

Minimum standards of indemnity cover are typically set by professional bodies, which regulate professions like law and accountancy. So any attempt to exclude privacy-related exposures from PI policies would have to be agreed by the relevant professional body, explains Hughes-Williams. PI underwriters should look to understand more about their data and privacy exposures and what risk management procedures insureds have in place, she advises. "Proposal forms could be amended to ask questions around the IT systems, business processes and training, which should make it easier to assess the exposures and rate the risk."

Directors' and officers'

Growing privacy liability also has implications for directors and officers and their insurers. *Vidal-Hall v Google* could give rise to new grounds for a company to sue its directors if they fail to take reasonable steps to prevent a breach, or unlawful use, of personal data, according to Karen Boto, Associate at DAC Beachcroft.

"It is too early to say for certain that we will see a surge of claims, but there is an increased risk. There are potential scenarios that could lead to more claims being pursued against directors and officers, as well as claims for costs associated with regulatory investigations," says Boto. "For example, companies may more readily sue the former board in the event of an insolvency or if the board has been replaced, as a result of public demand, following a major data breach."

D&O insurance typically provides broad cover for losses sustained for claims arising from a 'wrongful act'. So if a director neglects to prevent a data breach, the loss is likely to be indemnified under Side A and B cover. Loss suffered by the company itself could also potentially fall under Side C entity cover, if it is not restricted to security class actions.

"Insurers should look at Side C cover to ensure that it is not so wide as to respond to the company's losses relating to a data breach or misuse of information unintentionally. These could potentially exhaust the policy limit of indemnity leaving nothing for the directors and officers," advises Boto.

"D&O policies do not typically expressly refer to privacy risks – the cover offered is usually so broad that it is not strictly necessary. Nevertheless, brokers and insureds are pushing for specific cyber extensions to obtain clarification of coverage. While new, these extensions will probably evolve over time and may feature breach of privacy and information misuse in due course."

Commercial combined

Commercial combined insurers could also face unexpected claims associated with a privacy breach or misuse of personal data through public liability and, to a lesser extent, employers' liability coverages. The principal exposure arises through the main public liability insuring clause – to indemnify the insured for legal liability to pay compensation for damages that may arise from personal injury, property damage or nuisance and trespass.

"The emerging privacy liability tort could provide a new line of cases relating to personal injury. Underwriters typically think of personal injury in terms of physical harm, like slips and trips, and few would contemplate a person suffering injury through a breach of privacy or misuse of information," says David Bear, Partner at DAC Beachcroft.

To claim compensation for personal injury, a claimant would typically have to suffer a recognised medical condition. However, it is possible to imagine scenarios where a data breach could trigger or contribute to a psychological condition, such as reactive depression or anxiety neurosis where the claimant would be regarded as the primary victim. For example, the release of information relating to a person's sexuality, lifestyle, medical conditions or personal views could give rise to significant distress, triggering depression or severe stress.

"Underwriters of both public liability and employers' liability need to give thought to potential personal injury for moral damage and distress arising from the misuse or release of personal data," says Bear. "There are already cases that set the bar

for personal injury for mental conditions, and stress or reactive depression, supported by proper medical evidence, can get over the line for the purposes of a personal injury compensation claim. This is definitely one to watch and one for underwriters to think about.

“Extensions to public liability policies, some of which relate to data protection law, may also give rise to exposure. Such extensions were not written with moral damage and distress without financial damage in mind. However, they could potentially give rise to claims where anxiety or distress falls short of what is needed for personal injury,” adds Bear.

“Underwriters need to decide whether they are prepared to write and accept liability for this new tort, and whether they want to amend policy wordings as a result,” he says.

It is possible to take steps to limit exposure to data protection claims in public liability policies. However, employers’ liability insurance is compulsory and must meet minimum standards of cover. “Underwriters need to ask questions about data protection, and give some careful thought to extensions and exclusions as this is a new class of tort in today’s data-intensive world,” says Bear.

Trend toward notification

Data breaches continue to hit the headlines. And while data protection laws are evolving, the general direction of travel suggests that companies will increasingly be required to notify regulators and individuals when there has been a breach of data security.

Under current UK data protection law, most companies are not legally required to notify the regulator or individuals following a data breach. However, current regulatory guidance is that serious breaches should be notified to the regulator and consideration given to notifying affected data subjects. If companies do not, they could face higher sanctions.

Corporate social responsibility is also resulting in an increasing number of companies voluntarily notifying data breaches. A long-touted revamp of the EU data protection regime is currently being negotiated in Brussels, and current drafts of the legislation suggest some form of compulsory notification regime will be included.

“The general consensus is that compulsory notification of regulators and data subjects will be introduced, although the finer details of any such requirements are still being negotiated by European lawmakers,” says Allnutt.

First-party costs associated with a data breach and subsequent notification can be expensive. Such costs are not typically picked up by third-party liability policies, justifying the need for specialist cyber covers that indemnify a range of breach-related costs, including legal, forensic, notification and crisis management services.

Standalone cyber

Standalone cyber insurers will also face a growing exposure to privacy liability. However, on balance they should benefit from increased awareness and demand for their product. As discussed, the cover under traditional liability policies could be said to be limited, unclear and untested. As liability insurers assess their exposure, they may, where allowed, limit their liability and introduce exclusions.

Standalone cyber insurance, in contrast, is specifically designed to cover data and privacy claims and will offer clear cover for both liability and first-party costs. In addition, cyber underwriters are best placed to assess the risk and price their policies based on clients’ data and cyber security profile.

“Cyber underwriters should consider the implications of an increase in privacy-related claims, but with their expertise they are much better positioned to assess the exposures and should benefit from increased awareness and demand for cover,” says Allnutt. "It is too early to say for certain that we will see a surge of claims, but there is an increased risk."

Authors

Hans Allnutt
London - Walbrook
+44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com

David Bear
London - Walbrook
+44 (0) 20 7894 6140
dbear@dacbeachcroft.com