DAC BEACHCROFT

LEGALIGN GLOBAL

INFORMED INSURANCE 2021/2022

Privacy, data breaches and class actions: the next scandal is just around the corner

Privacy, data breaches and class actions: the next scandal is just around the corner

Data-gathering, in the age of smart phones and seemingly limitless online connectivity, is unrelenting and goes well beyond the ability or desire of most ordinary people to comprehend it. We know we are being asked to surrender our data, but we often have only the vaguest idea how much our privacy is being compromised in the process.

A data security breach might occur where someone forgets to change their password. Or it might be the result of poor coding on an AI algorithm, or it could be a decision to hack user information on a website for financial gain. The challenge of safeguarding people's privacy can be extremely complicated and challenging.

And that was before COVID-19. In the past 18 months, as physical movement has been severely curtailed by the global pandemic and pushed more of our lives online, a lack of privacy and the potential for security breaches has become an even greater concern to many people, heightened by requests for individuals to share personal health and location data with third parties.

Fortunately, regulators and policymakers around the world have not been idle in getting to grips with the issue of data privacy. If anything, COVID-19 has emphasised the need to place privacy much higher up the regulatory agenda. Greater privacy protections can also be seen in a growing number of class actions around the world.

PRIVACY CASE STUDY: NEW ZEALAND

New Zealand has been lauded for the way it managed to avoid the worst of the pandemic. Its handling of the data privacy issue was an integral part of that, according to Joseph Fitzgerald, Senior Associate at Wotton + Kearney in Wellington.

"Privacy is important to ensure trust and there were a lot of questions asked about how the public could be reassured that their information would be kept safe and wouldn't be used for other purposes."

In New Zealand (and Australia), governments used the available technology to track the spread of the COVID-19 virus. In New Zealand, the early adoption of the track and trace app and the Ministry of Health's development of a comprehensive contact tracing database involved an amalgamation of a massive amount of public information.

"The New Zealand government took a real 'privacy first' response," said Fitzgerald. "For example, the COVID-19 tracing app does not store data in a centralised repository. It retains the information on your phone and if it is necessary to pull that information from your phone for contact tracing purposes, you receive a notification."

By making a conscious effort to address the privacy issues raised by the app, the government was able to increase the level of trust. "It was intrinsic to how the whole country responded. We were willing to go into an extended period of lockdown because people had trust in what the government was doing and a big part of that was showing the location and medical information they were gathering was being dealt with in a responsible way."

The pandemic has definitely highlighted the legal and regulatory challenge around data ownership and third party usage, said Hans Allnutt, UK lead Partner on Cyber and Data Risk at DAC Beachcroft.

There's always a tension between handing over information for the greater good and at the same time having concerns about where that data is going. That perception is further skewed by a natural suspicion of Big Tech, in the form of Facebook and Google, both of whom have faced accusations over the misuse of data on many occasions.

"There is so much information out there, the only way that you can filter it is to use an algorithm," said Allnutt. "Those algorithms are designed to be helpful, but it comes down to who is controlling them and what their motivation is: profit, or something worse?"

Allnutt said any company using automation and failing to understand the inherent flaws in its underlying systems needs to put processes and governance structures in place to deal with it. Or it will be in the regulators' and class action lawyers' firing line.

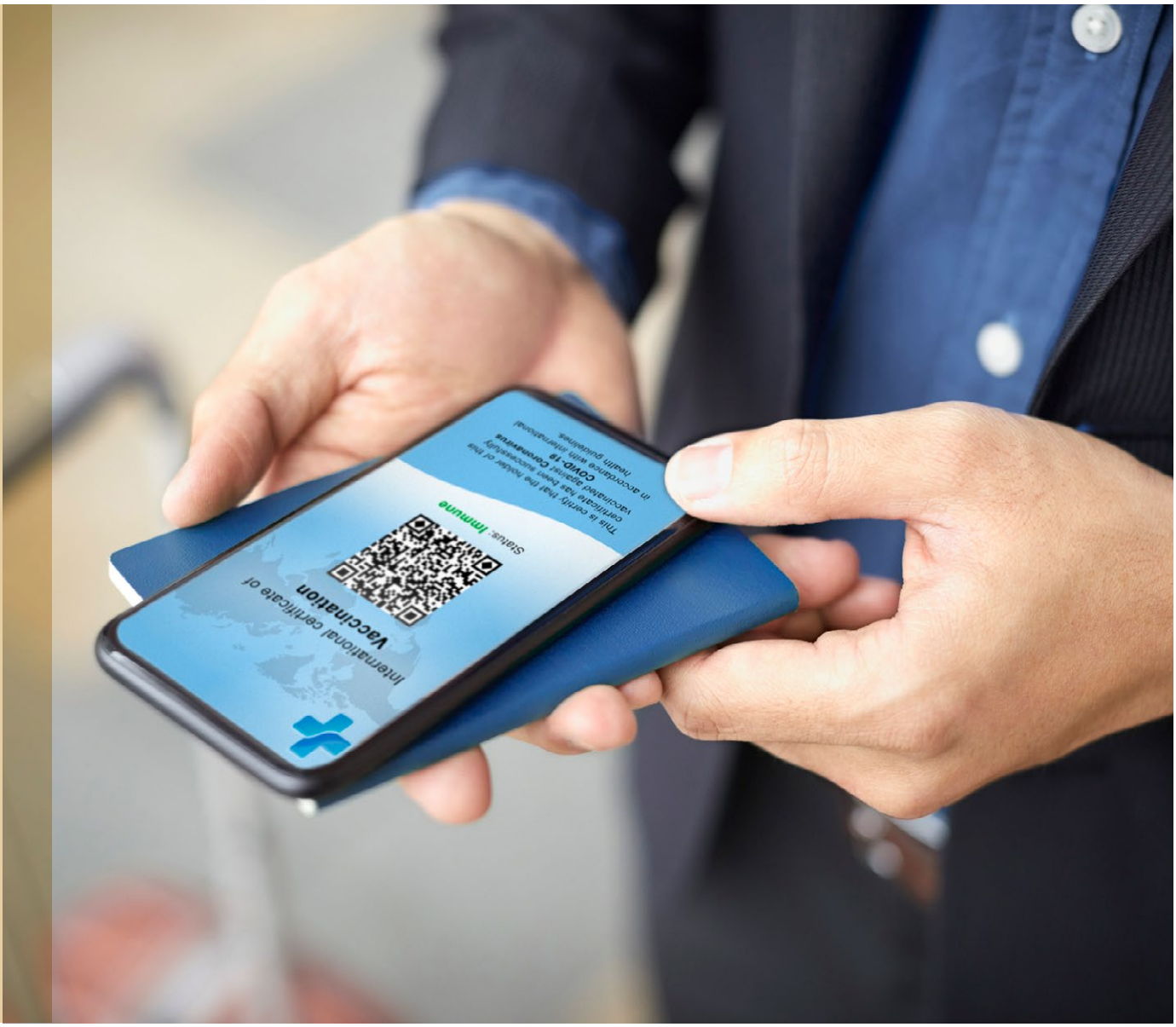
VACCINE PASSPORTS

While there is general agreement that vaccine passports are useful, questions have been raised as to how much information should be collected. There's also an understandable sense of trepidation about whether vaccine passports will get the balance right between individual privacy and public health. Again, it comes down to trust.

"Unfortunately, it seems that the automatic starting point is one of mistrust on anything to do with personal data and vaccine passports," said Allnutt.

Without even considering the natural reluctance of a significant proportion of the population to the very idea of vaccine passports, there are so many ways in which their use could go wrong. "For example, if they were used in a way that results in prejudice, which you can see happening pretty easily, that would be a problem," said Fitzgerald.

"How do we ensure that the entity collecting the data doesn't then use them for other more sinister reasons? If you don't get the rules around vaccine passports right, then you end up with people not taking them up."



A notable addition to New Zealand's recently updated Privacy Act is the mandatory breach notification, requiring that particular privacy breaches, if they are deemed likely to cause harm to an individual, must be notified to the Office of the Privacy Commissioner. The Commissioner now has fining powers, limited to NZD$10,000, but also has the power to issue compliance notices and compel agencies to comply with access requests.

However, the new Privacy Act is notable for what it doesn't contain: in many ways it is already outdated. It was based on recommendations made in a report by New Zealand's Law Commission released in 2011. In comparison, the EU's General Data Protection Regulation (GDPR) was finalised in 2016, so there is plenty still for New Zealand to do to catch up with Europe.

"There's a lot missing from our Privacy Act that we see in other jurisdictions," said Fitzgerald. "Things like the right to data portability; the right to be forgotten; substantial fines; rights around algorithmic transparency; the right to know how that decision was arrived at."

Australia's Privacy Act is also under review and could potentially be turned into a much more GDPR-style code of requirements, according to Kieran Doyle, Partner at Wotton + Kearney in Sydney.

"One thing of note is a potential statutory right of action for individuals. Currently there is no tort of privacy in Australia. That doesn't stop the Privacy Commissioner hearing complaints in her own jurisdiction, but in terms of bringing an action to court there is no basis as it stands. So that would be a game-changer. It would also give a boost to class actions, depending on how the government deals with regulating class actions in this space."

INFLUENCE OF THE GDPR

The transfer of data across borders, the ability of entities to have establishments in multiple jurisdictions and the ease of data trading are some of the great challenges to privacy regulation in the modern era.

The GDPR has led the global charge in setting the standard for data protection. The European Union regime allows other jurisdictions to attain "adequacy" status and exchange personal data much more easily. This has triggered a wave of updated privacy legislation around the world. There's a genuine incentive for other countries to match those European standards and to maintain or attain adequacy status.

"Some of the provisions of the GDPR are quite forward thinking, around the control of data," said Allnutt. The regulation around disclosure of security breaches is also making it easier for individuals to bring claims and class actions. "The biggest change to data security in the last 10 years is the greater number of compulsory breach notification laws around the world. People have always had their data hacked or stolen, and it was happening 20 years ago, but back then companies didn't have to tell anyone about it."

For a company concerned about the protection of customer and personal data, the breach may nowadays just as easily occur at one of their suppliers as within their own systems. For example, Blackbaud is a large cloud-based data provider to schools, universities and charities around the world. They were the target for a ransomware attack in 2020, had data stolen from their charities and foundations and then went and told their donors.

"I strongly suspect that if you tell the average donor to a UK charity that their data had been impacted by a cyber incident at a company called Blackbaud in the US, they would say "I've never heard of the company. How on earth did my data end up there?" This happens much more frequently than you might think," said Allnutt.

"Under the GDPR, you ought to be informed about where your data is going. The reality is that it's not until your data has been hacked that you find out where some of your data has gone."

CLASS ACTIONS ON THE RISE

The UK has a long history of group litigation, mostly around financial services. The recent proliferation of data movement is the key reason for the rise in privacy breach collective actions.

Kieran Doyle in Sydney sees a greater shift towards compensation claims that is likely to escalate further, whether by firms or individuals: "It's an unstoppable trend."

The vast cross-border data transfers are causing a higher level of system inefficiencies and costs, which is bad for the insured and bad for the insurer, said Doyle.

"If you've got a multi-party data breach, there will be issues around the different treatment of transfers around the world and different thresholds for data retention for a multi-jurisdictional entity. That's a huge investment in time and cost, pre- and post-incident."

Australia loves a good class action, he added. "We are starting to see litigation funders turning their minds to data breach class actions and so far we've had one go through a court process and another two were recently filed. It's only a matter of time, because we know there are a number under investigation by litigation funders."

In New Zealand, the situation is a little different. There is a tradition of privacy litigation but as Fitzgerald explains, when it comes to class actions they are at the other end of the spectrum.

"Our entire class action regime has so far been developed piecemeal. We have one section in the High Court rules which opens the door to class actions, but doesn't provide any of the surrounding mechanisms that you would find in a more mature regime such as in Australia or the UK. The courts are currently doing their best to deal with a regime that is entirely devoid of detail."

The New Zealand Law Commission is now accepting submissions, so with the mandatory breach notification rules in place, New Zealand can expect to see the structure around class actions mature quite quickly once the Law Commission makes its final recommendations to the Minister of Justice in May 2022.

BIG TECH IN THE CROSSHAIRS

It's a challenging environment for the big tech companies in Australia. The consumer watchdog, the Australian Competition and Consumer Commission (ACCC), is going after Facebook and Google in particular. The action against Google relates to deceptive and misleading conduct on the basis that people couldn't turn off the location tracking on their Android phones - even when they had turned it off, it was still on.

The Privacy Commissioner has also issued proceedings against Facebook arising from a Cambridge Analytica data breach which happened five years ago.

These are regulatory actions, but Doyle said there is no reason why a class action couldn't spin off the back of one of them. "In fact it makes it much easier for the class. While we haven't seen anything announced yet, I wouldn't be surprised if there are litigation funders looking to piggy-back off the ACCC."

Allnutt believes the changes taking place at a regulatory level could well pave the way for more class actions against the tech giants. "There will always be grey areas and ancillary uses for data: cookie tracking and online monitoring. It will be a constant theme in years to come. The threats to privacy won't be solved by a single class action. Just like financial services, the next scandal is just around the corner."

Richard Lloyd v Google LLC

In a landmark decision given in October 2019, the Court of Appeal gave permission for Mr Lloyd, a consumer protection champion, to proceed with his "opt-out" representative action against Google. His claim alleges that Google breached its duties as a data controller under the Data Protection Act 1998 (DPA) when it collected and used the browser-generated information of 4.4 million Apple iPhone users during the period 2011-2012.

The Court of Appeal was satisfied the requirements for granting permission in representative claims (as set out in CPR 19.6) were met. It held the Claimants are all victims of the same alleged wrong and have all sustained the same alleged loss - namely, loss of control of their data in breach of s13 of the DPA 1998. The Court also accepted that damages could be calculated as a uniform amount for each person within the defined class, and there is no need to prove they have suffered pecuniary loss or any distress due to the infringement of their rights.

Google appealed the decision. This was heard by the Supreme Court in April 2021 and judgment is expected in late 2021.

There are widespread concerns that, if the Supreme Court were to find in Mr Lloyd's favour and grant permission for the claim to proceed, it would open the floodgates to similar US-style class actions in data breach claims. There are a number of such claims that have already been filed and their progress will depend on the outcome of this case.

Some have questioned the appropriateness of claimants being automatically joined to litigation without giving their express consent. This raises issues including whether they ought to be awarded damages where they have shown no interest in pursuing a claim or, if they have, whether this effectively stops them from pursuing their own separate claims. There are also the implications of awarding eye-watering levels of damages - £3bn is collectively claimed against Google - without the need for claimants to prove loss. It goes without saying that all eyes are on this eagerly-awaited decision.

Contributors:

Hans Allnutt
DAC Beachcroft, London
hallnutt@dacbeachcroft.com

Kieran Doyle
Wotton + Kearney, Sydney
kieran.doyle@wottonkearney.com.au

Joseph Fitzgerald
Wotton + Kearney, Wellington
joseph.fitzgerald@wottonkearney.com

Click below to read our whole suite of new thought leadership:

- Interconnectivity of solutions
- Brexit
- Climate change
- Privacy, data breaches and class actions
- Social unrest

KEY CONTACTS

David Pollitt
Managing Partner
DAC Beachcroft
T: +44 (0) 117 918 2226
M: +44 (0) 7909 928 330
dpollitt@dacbeachcroft.com

Todd R Davies
Lead Partner
Alexander Holburn
T: +1 604 484 1799
M: +1 604 506 8294
tdavies@ahbl.ca

Helen Faulkner
Head of Insurance
DAC Beachcroft
T: +44 (0) 117 918 2225
M: +44 (0) 7841 322 480
hfaulkner@dacbeachcroft.com

Bastian Finkel
Partner
BLD Bach Langheid Dallmayr
T: +49 221 944027 893
M: +49 163 2829 330
bastian.finkel@bld.de

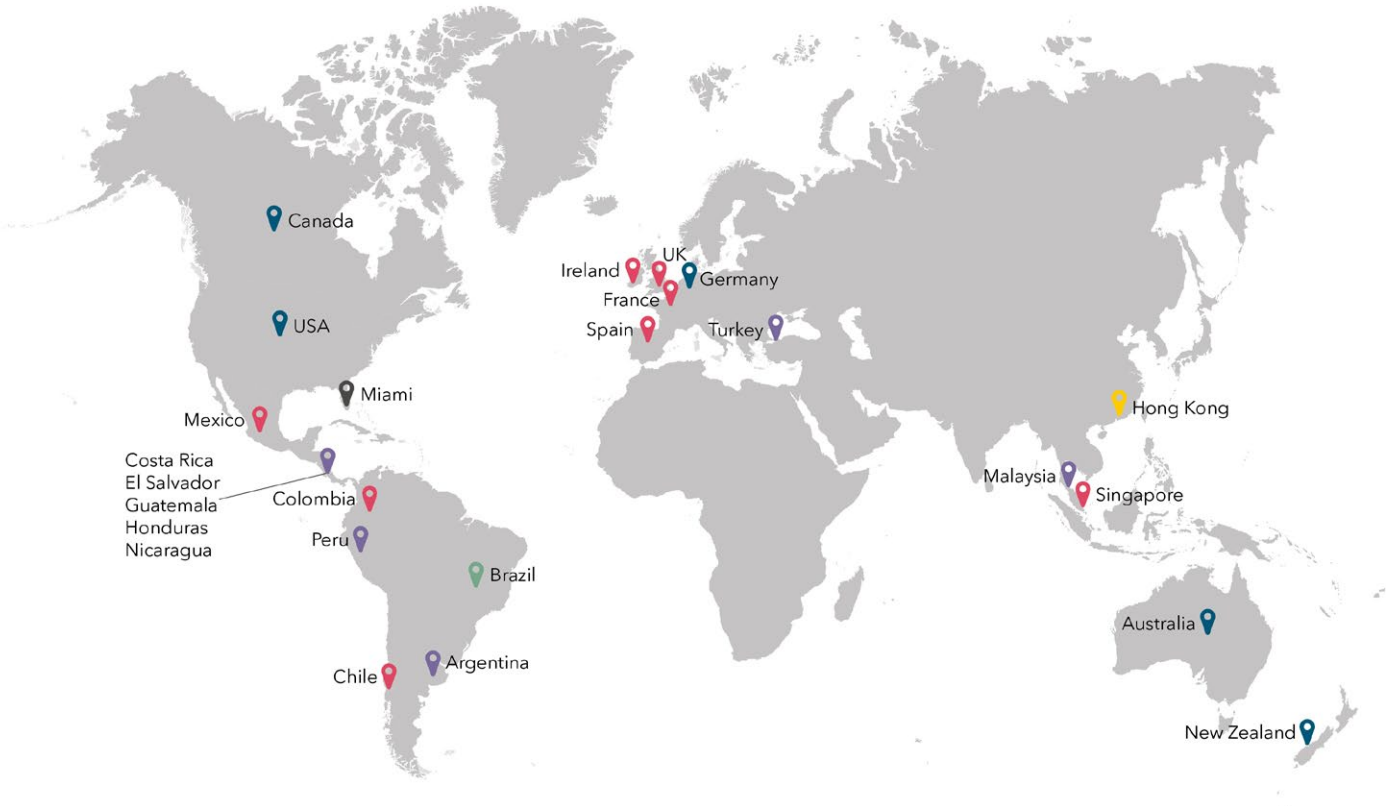
Craig Dickson
CEO
Claims Solutions Group
T: +44 (0) 121 698 5270
M: +44 (0) 7834 308 472
cdickson@dacbeachcroft.com

Daniel J McMahon
Chairman
Wilson Elser
T: +1 312.821.6147
M: +1 312.339.3895
daniel.mcmahon@wilsonelser.com

Charlotte Shakespeare
Senior PSL/ Editor
DAC Beachcroft
T: +44 (0) 207 894 6816
M: +44 (0) 7921 890842
cshakespeare@dacbeachcroft.com

David Kearney
Chief Executive Partner
Wotton+Kearney
T: +61 2 8273 9916
M: +61 4 1873 6196
david.kearney@wottonkearney.com.au

OUR GLOBAL REACH



insurance.dacbeachcroft.com

dacbeachcroft.com

Follow us: @DACBeachcroft

Connect with us: DAC Beachcroft LLP