Data Points is Chapman Tripp's new regular publication tracking relevant developments in the privacy sphere in New Zealand and internationally.

Privacy is an evolving area of law as regulators try to keep up with fast-developing technologies, the rapid accumulation of private data and increasingly sophisticated cyber-criminals.

It is important to stay on top of these developments. The risk for organisations getting it wrong can be very high – both when the organisation is a victim and when the organisation fails to maintain expected standards of confidentiality and data integrity.

We hope you find our insights within this publication useful. Do get in touch if you would like to discuss any topic in more detail.

Contents

MAY 2020

New Zealand

Legislation/regulation

Privacy and COVID-19 guidance

The Privacy Commissioner has published a series of guidance notes on privacy issues relating to COVID-19. Specific privacy advice is provided for hospitality businesses, employers and employees, landlord and tenants, and healthcare professionals.

To read more, visit the website

COVID-19 and location tracking

Countries around the world are using digital tracking methods as part of their COVID-19 response. These range from directly requiring individuals to install specific tracking apps on their devices to ascertaining general movement trends using anonymised location data from millions of cell phones.

In New Zealand, the Privacy Commissioner has given health authorities the green light to track coronavirus-infected persons via data collected by their mobile phone companies. Both the Privacy Act and the Telecommunications Information Privacy Code allow telcos to disclose information if they believe, on reasonable grounds, the disclosure is necessary to prevent or lessen a serious threat to public health.

To read more, view the article

Privacy Bill update

We now have a firmer idea of the detail of the new privacy regime to be created by the Privacy Bill through a series of late changes introduced by the Government last month through a Supplementary Order Paper (*SOP*).

The Bill has had a famously long gestation – around 456 weeks at the end of April, taking conception from the Law Commission report of June 2011 on which the Bill is based. It had been scheduled to come into force on 1 March 2020 but has now been extended to 1 November.

The amendments contained in the SOP are technical in nature and do not, nor were intended to, align New Zealand with the requirements of the EU General Data Protection Regulation (*GDPR*). This means that the new Act will require almost immediate amendment. Indeed, officials are already looking at what this will entail.

We are one of only 12 countries in the world to have EU 'adequacy status' but that was granted before the GDPR came into force, and the status is due for review before 25 May 2020.

For more detail read Chapman Tripp's commentary on the SOP, and earlier commentary on the Bill

Open banking increases risks around data security

The impending introduction of open banking into New Zealand is creating new imperatives around data security for New Zealand banks.

Open banking refers to a standardised and secure framework for sharing bank customer data with trusted financial service providers, such as fintech and other technology companies. The idea is that it will enable a wide range of new financial products and better ways to aggregate and present data that will be timely and personalised to the consumer.

This has the potential to deliver significant economic and social benefits for both consumers and businesses. But the downside from a privacy perspective is that expanding the access to sensitive consumer information will create new opportunities for hacking and fraud and increase the potential for unintended disclosure.

For more detail read Chapman Tripp's *Finance trends and insights* commentary

Court and Office decisions

Peters loses invasion of privacy claim

The High Court has rejected Winston Peters' invasion of privacy claim against two former National Ministers and two senior public servants, finding that they had a proper interest in or a genuine need to know the facts relating to the overpayment of his superannuation.

For more detail, here is the Chapman Tripp commentary

The scope of "personal information" and mixed information

In *Taylor v Department of Corrections*, former inmate Arthur Taylor challenged the redaction under the Privacy Act of Corrections staff names and details in its response to an official information request from Taylor.

Taylor had requested all file notes, incident reports, email traffic and other documentation by any Corrections employees which related to him or mentioned him "in any way, shape or form" over the period 1 August to 5 September 2014, when he was in Auckland Prison.

Both the Privacy Commissioner and the Director of Human Rights Proceedings intervened to argue, in support of Taylor, that "personal information" should be defined broadly to act as a 'jurisdictional filter'.

But the Court found that the redacted information, "while appearing on the same pages as Mr Taylor's personal information, was not 'about him'. It was essentially administrative…. Nor did its omission render the communication unintelligible".

For more detail, here is the judgment

Invading privacy does not require widespread publicity

In *Henderson v Walker*, the High Court issued a landmark decision greatly expanding the tort of invasion of privacy. At issue were the actions of Mr Walker, who was the liquidator of one of Mr Henderson's companies. After having Police seize a Henderson company laptop, Mr Walker then shared emails and voice recordings contained on it with the IRD, the Official Assignee and third parties.

The High Court was highly critical of Mr Walker's actions, commenting that "he appeared to see himself as something of an avenging angel and … that he went above and beyond what many liquidators might." The Court found that Mr Walker had not only breached confidence but had also invaded Mr Henderson's privacy.

This finding expands the scope of the invasion of privacy tort by finding that widespread publicity is not required and that in the circumstances, simply providing the documents without authorisation was enough. Effectively the Court has merged the invasion of privacy tort with the intrusion into seclusion tort.

For more detail, read the LawTalk article and Stuff article

Employer's failure results in $7,000 payout

A company has been made to pay $7,000 to a former employee who fell victim to identity and credit card fraud after copies of his personal information, including his driver's licence, were stolen from his ex-employer. The employer had kept the documents in a cabinet which, although locked, was accessible by several staff.

For more detail, read the article

Credit checks out unless there is financial risk

A temporary employment agency has been found in breach of information privacy principle 1 for running a credit check on a potential employee for a role involving no financial risk. The Office of the Privacy Commissioner provided the man with a certificate of investigation and told him he

was free to take the matter to the Human Rights Review Tribunal.

The Office did not accept the employment agency's argument that the check was a necessary part of the screening process because the client had asked it to ensure that the contractors hired did not have any credit worthiness issues and because the call centre work at issue involved handling highly sensitive information from the public.

For more detail, here is the case note

Data breaches

Click to consent not enough?

A survey has found that only 2% of New Zealanders read online privacy policies. The main reasons offered were that they were long and confusing. The Privacy Commissioner has already identified "click to consent" formats as an issue, indicating that there may be an emerging legal risk in relying upon them.

For more detail, here is the article

Houseparty privacy concerns

Hundreds of users of the Houseparty app, available on Google's Play store and Apple's app store, have claimed their Spotify, Snapchat other accounts have been hacked after downloading the app.

Popularised during the COVID-19 global lockdowns, Houseparty allows users to join video calls and play games with friends. Users have to manually opt out of the collection of their personal data, and even if they do, Houseparty can still collect and use information is deems to be non-personal.

Epic Games, the owner of Houseparty, has denied the hacking claims, offering a $1m reward to anyone who can prove the hacking reports are in fact part of a commercial smear campaign. No legitimate computer security firms have confirmed a problem with the app.

But the alleged hacks have put the spotlight on Houseparty's privacy policy, which experts consider is probably non-compliant with European privacy laws and with the New Zealand Privacy Bill.

Gehab Gunasekara, an associate professor in commercial law at the University of Auckland, has called Houseparty a "Trojan horse", saying "you're essentially allowing this app to access your smartphone and your smartphone tells a lot about you, your movement, your locations, your contacts, how often you contact people, who you communicate with, and they'll be able to basically track your every move".

For more detail, here is the media item

Warning from the top

The Director-General of the Government Communications Security Bureau (*GCSB*) has warned businesses in sensitive areas of the economy – including operators of critical infrastructure, holders of key intellectual property and major exporters – that they are susceptible to hacking by foreign states and that, the more they protect against this risk, the more resources the GCSB will be able to direct to "high-end threats".

The GCSB worked on about 340 cyber incidents last year, more than a third of which could be linked back to foreign governments (in particular Russia, China and North Korea). Yet fewer than one in five of 250 nationally significant organisations surveyed by the GCSB in 2018 had a dedicated executive to deal with information security and more than 40% were "barely confident they would know if their systems were hacked".

For more detail, here is the article

Cyber sabotage an expensive threat

The Reserve Bank has applied two internationally recognised methods to estimate that the indicative average annual cost of cyber incidents in New Zealand is $104m for the banking sector and $38m for insurance sector – or the equivalent of between 2% and 3% of annual profits.

The modelling also indicates that there is a 5% chance in any given year of the costs exceeding $2.3b. The research was part of the Reserve Bank's programme of work on the risks to the financial system.

For more detail, here is the RBNZ statement

Ministry of Culture and Heritage in damage control mode

The Ministry of Culture and Heritage went into damage control mode after the privacy of the 302 people who applied for its Tuia 250 Voyage Trainee programme was inadvertently breached. At least 370 documents were compromised, including passports, driver's licences, birth certificates and other forms of identification.

The Ministry was alerted to the breach after a fraud attempt using a copy of a driver's licence obtained through the leak. It tried to contact each applicant by phone, set up a support team for those affected and published an information sheet on its website. The Ministry commissioned independent review of its systems, process and circumstances that led to the breach, and accepted all of the report's recommendations.

The Prime Minister announced at her regular post-cabinet press conference the following Monday that it will be mandatory for specific government agencies (to be identified in a list) to work only with approved ICT suppliers and to follow set security standards.

For more detail, click for links to the Ministry media release, website notice, media release, and media release

International

Legislation/regulation and guidance

The importance of getting consent

The UK Information Commissioner's Office (*ICO*) has produced a 25 page report on the way personal data is being used to sell advertisement space on websites. The process – known as real time bidding – relies on the potential advertiser seeing information about the browser (or the potential customer).

The data can be basic – the device you're using, the country you're located in. But it can be more detailed and paint more of a picture of you, including other websites you've visited, or your perceived interests.

The ICO advises that this breaches the GDPR and that consent is the only lawful basis advertisers can rely on for processing the personal data of individuals when engaging in this type of programmatic advertising. It has asked advertisers to obtain consent from individuals, and to demonstrate a greater degree of transparency regarding the use and distribution of personal information, when obtaining such consent.

For more detail, here is the ICO report

Court decisions

Landmark win for Google over right to be forgotten

The European Court of Justice (*ECJ*) has found for Google in a landmark case regarding the application of the right to be forgotten, ruling that there is no obligation under EU law for a search engine operator to apply a de-referencing request beyond the EU.

Google argued that to apply the obligation outside Europe could lead to it being abused by authoritarian regimes to hide human rights abuses. There was also a concern that, had the ruling gone the other way, it might be viewed as an attempt by the EU to police the US tech giants beyond the EU's borders.

Google was supported by Microsoft and Wikipedia.

We note that this decision is at odds with the Canadian Supreme Court's 2017 decision which had ruled Google could be forced to remove content worldwide, not just in Canada.

For more detail, read the article

Class actions for breaches of privacy

The English Supreme Court has agreed to hear a challenge to a Court of Appeal ruling which would allow a class action against Google on behalf of four million iPhone users to go to trial.

At the centre of the class action is the claim that Google used tracking cookies to override privacy settings in the Safari browser. The Court of Appeal's decision is potentially far-reaching.

In permitting the litigation to proceed, it held that an individual's personal information has an economic value such that loss of control over it is a violation of the right to privacy. Accordingly, it followed that:

- the claimants did not need to show they had actually lost money or suffered distress, and
- each had suffered the same loss and therefore shared the same interest (which is a critical component for a class action).

For more detail, read the article

Supermarket not vicariously liable for employee's breach of privacy

The United Kingdom Supreme Court has overturned the Court of Appeal and determined that supermarket giant Morrisons was not liable for an employee leaking the payroll data of about 100,000 staff.

The Court considered that the man was motivated by a grudge against Morrisons and that his actions were not closely connected with his duties at work so there was no basis for imposing vicarious liability on Morrisons.

The decision ended the hopes of employees whose personal details had been posted on the internet that Morrisons would be ordered to pay them compensation.

For more detail, read the Guardian article

International data transfer case breached privacy

The United Kingdom Supreme Court has ruled that the British Government breached the Data Protection Act (UK) by giving the United States information on two suspected Isis terrorists without assurances that they would not get the death penalty.

The ruling confirms that strict compliance with the Data Protection Act is required and that controllers and processors needed to have documented the basis for processing personal data.

For more detail, read the article

Court permits police use of automated facial recognition technology

The High Court of England and Wales has dismissed a judicial review claim arguing that the South Wales Police's use of automated facial recognition at public events contravened the UK's Data Protection Act 2018, Human Rights Act 1998 and the Equality Act 2010.

Police used the technology to scan faces against a watch list of suspected offenders, persons of interest or individuals wanted for arrest, and to act in real-time against potential matches.

The Court found that, while the scans engaged the right to privacy under Art 8 of the European Convention on Human Rights, the Police actions were still in accordance with law and proportionate. The judgment is now being appealed.

For more detail, read the decision

Enforcement

Cathay Pacific pinged £500,000

Cathay Pacific has been fined £500,000 by the UK ICO after an investigation into a privacy spill affecting 111,578 UK residents uncovered "a catalogue of errors", some dating back to October 2014. These included:

- back-up files that were not password protected;
- internet facing servers that didn't have the latest patches;
- operating systems that were no longer supported by the developers; and
- inadequate anti-virus protection.

The airline first became aware of the issue in March 2018 when it suffered a "brute force" password guessing attack. The customer information which had been exposed comprised passport details, dates of birth, phone numbers, addresses and travel histories.

For more detail, read the article

Mega breaches attract mega fines

The ICO has deferred hefty fines issued last year against British Airways and hotel chain Marriott International pending further investigations. They are the largest penalties the ICO has imposed to date under the EU General Data Protection Regulation (*GDPR*), in effect since 25 May 2018.

- British Airways was fined $205.7 million after user traffic to its website was diverted to a fraudulent site where the personal data of approximately half a million customers was harvested by cyber attackers; and
- Marriott International was fined $111.5 million after around 339 million guest records were exposed through a vulnerability in the systems of the Starwood group, which was bought by Marriott in 2018. The ICO said Marriott had failed to take appropriate due diligence when making the acquisition.

For more detail, read the article

Location tracking misleading customers

The Australian Competition and Consumer Commission (*ACCC*) has filed a case in the Federal Court alleging Google misled consumers about location tracking. The ACCC claims that users of Androids phones were misled into thinking they had disabled location tracking by turning off the "Location History" option. But it turned out that Google could still track users' movements unless the "Web & App Activity" setting was also turned off. Google says it intends to defend the claim and earlier this year had added new privacy controls.

For more detail, read the article

Google to move UK data to US

Google is planning to move the data and user accounts of its British users from its European headquarters in Ireland to the US. It is understood the trigger is that it is not clear whether, post-Brexit, Britain will follow the GDPR or adopt different data protection rules.

Google has said it will continue to apply the protections of the GDPR to these users, and that "nothing about our services or our approach to privacy will change, including how we collect or process data, and how we respond to law enforcement demands for users' information". However, the effect is that British authorities wanting access to the personal data of British Google users will need to negotiate with the US rather than the EU – and the US regime is much more accommodating, particularly with the recent passage of the Cloud Act.

For more detail, read the article

Checkers checked

Amazon, Apple, Facebook and Google have all reviewed their processes after they were found to have given third parties access to customer oral communications for the purpose of improving the voice recognition capabilities of their products.

Voice speakers and chat programs give rise to heightened privacy concerns as the information they contain has often been captured accidentally. Google, Apple and Facebook have since stopped audio quality checks for privacy reasons, and all are planning to get users' consent before engaging their communications in the quality assurance process.

Amazon has given users an express right to opt out of having their audio recordings checked.

To read more, view the Facebook article and Google/Apple article

Key contacts

KELLY MCFADZIEN – PARTNER
T:+64 9 357 9278
M:+64 27 473 2230
kelly.mcfadzien@chapmantripp.com

JUSTIN GRAHAM – PARTNER
T:+64 9 357 8997
M:+64 27 209 0807
justin.graham@chapmantripp.com

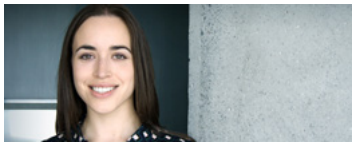
TIM SHERMAN – PARTNER
T:+64 4 498 2400
M:+64 27 345 3250
tim.sherman@chapmantripp.com

NICK LETHAM – PARTNER
T:+64 3 353 0024
M:+64 27 204 7323
nick.letham@chapmantripp.com

FIONA BENNETT – PARTNER
T:+64 3 353 0341
M:+64 27 209 5871
fiona.bennett@chapmantripp.com

TOM CLEARY – SENIOR ASSOCIATE
T:+64 9 357 9889
M:+64 27 722 9430
tom.cleary@chapmantripp.com

EMMA DALE –SENIOR ASSOCIATE
T:+64 9 357 9291
M:+64 27 589 1978
emma.dale@chapmantripp.com



LIORA BERCOVITCH – SENIOR SOLICITOR
T:+64 9 357 9620
M:+64 27 469 9366
liora.bercovitch@chapmantripp.com

STEPHANIE GRAY – SENIOR SOLICITOR
T:+64 9 358 8466
M:+64 27 205 3369
stephanie.gray@chapmantripp.com

DAVID SMITH – SENIOR SOLICITOR
T: +64 4 498 4935
M: +64 27 370 1434
david.smith@chapmantripp.com