

Privacy Foundation NZ Newsletter

No 3 July 2020

Welcome to the third issue of the Foundation's newsletter. The last newsletter was in April near the start of the Covid-19 lockdown. It seems such a long time ago! The Foundation has been busy during the period not only with Covid-19 related matters but also surveillance and the new privacy law.

Committee meeting in June 2020

The Committee met by zoom video conference in June.

Covid-19 focus

The Foundation was well served by the active Health Care and Policy Working Group led by Barbara Robson. The working group identified contact tracing as a key issue. Special attention was paid to the contact tracing audit report and the privacy impact assessment of the Covid-tracer app.

On 18 April the Foundation issued a statement [calling for immediate release of COVID-19 contact tracing audit report](#). We believed the report was needed to understand the current contact tracing process and begin the discussions on the recommendations made to improve it. It is critical the process be fit for purpose to ensure any outbreaks that emerge after this lockdown period are quickly stamped out. An associated [resource document](#) was produced.

On 29 April the Foundation made a public statement on the proposed [COVID-19 smartphone app – Privacy Foundation expects transparency around privacy controls](#). Following the rollout of the app we made a statement [Moving Covid-19 tracking to next level: Privacy remains important in Tracer App and business practice](#). This acknowledged that the Ministry has developed its NZ COVID Tracer app with privacy in mind and undertook a privacy impact assessment but noted that without enhancements the app did not constitute a fully complete or effective contribution to the nation's contact tracing needs and urged further action.

On 7 July the Foundation expressed its [concern at reports of privacy breach of Covid-19 cases](#).

Over the period the Chair, Gehan Gunasekara, fielded many media interviews on privacy aspects of the pandemic.

In addition, to contribute to "informed and fair public comment on privacy" the Foundation published several commentaries. These do not necessarily represent the Foundation's position but are the opinions of the authors. Six commentaries with a bearing on the pandemic had already been published by the time of the April newsletter. Additional ones included:

- Blair Stewart (20 April) [Diaries unite against COVID-19](#)
- Health Care and Policy Working Group (29 April) [Contact Tracing – APPROaching the Future](#)
- Tim McBride (7 May) [The lockdown: a human rights perspective](#)
- Gehan Gunasekara (11 May) [Privacy Act Awareness Essential for Tackling Covid](#)

- Blair Stewart (26 May) [Privacy Impact Assessment in a Pandemic: Don't skip consultation](#)
- Blair Stewart (26 May) [Privacy Impact Assessment in a Pandemic: The Privacy Commissioner has a role](#)

Submissions

On 1 May the Foundation made a substantial submission to the Minister Responsible for the GCSB and the NZSIS on the [Consultation on Intelligence Cooperation Ministerial Policy Statement](#).

In its concluding statement the submission noted:

As has been outlined, Privacy Foundation New Zealand has considerable concerns about intelligence sharing by the New Zealand intelligence and security agencies with their overseas counterparts. At the crux of many of our concerns is the relatively wide statutory purposes governing the functions of the agencies. Where information sharing is concerned, we believe such purposes must be more narrowly defined, subject to a robust necessity assessment and be proportionate to the needs for which they occur. Lastly, the [Ministerial Policy Statement on Intelligence Cooperation] must pay more than lip service to human rights obligations, such as the obligations contained in the Privacy Act, through requirements for ex ante measures such as training and privacy impact assessments as well as ex post accountability through documentation and review.

The submission was prepared by the Foundation's Chair, Gehan Gunasekara, with the assistance and input of members of the Foundation's Working Group on Surveillance.

Privacy Bill update

On 17 March the Minister of Justice released [Supplementary Order Paper 482](#) outlining the Government's intended amendments to the Privacy Bill. A commencement date of 1 November 2020 was signalled which implied completion of parliamentary stages during April. The finishing line appeared close. However, Covid-19 intervened with the Prime Minister's Statement to the Nation on 21 March and the country moving to level 3 on 21 March and level 4 on 25 March. A State of National Emergency was declared on 25 March. Parliament had its last sitting on 25 March and adjourned until 28 April.

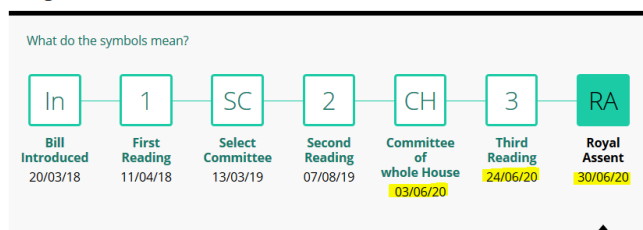
Understandably the bill would be delayed by the pandemic. However, with a General Election set for September there was a real risk that the bill would be delayed until 2021 and the uncertainties of a new government. The Foundation waited until the country moved out of lockdown and wrote to the Minister of Justice on 13 June urging that, subject to higher pandemic priorities, the Privacy Bill complete its final parliamentary stages at the earliest opportunity. The Foundation wrote:

There are of course many reasons in normal times why it is important to replace our aging privacy law with something more effective. The all-party support for the Privacy Bill at each parliamentary stage to date has been evidence of that. However, the Foundation wishes to highlight that there are good reasons to enact the bill to support New Zealand's health and economic response to the pandemic. We wish, in particular, to emphasise that:

- Privacy law underpins trust in government which is vital for New Zealand to effectively respond to the pandemic.
- Modern privacy law is an enabler to e-commerce and e-government which have been central to New Zealand's public health and economic responses and will be increasingly important as we move forward in recovery.

The [Foundation letter](#) and the [Minister's response](#) are available on the website.

Progress of the bill



After a long gestation the Privacy Bill made rapid progress once Parliament reconvened after the lockdown completing Committee of the Whole House stage, Third Reading and receiving Royal Assent.

The [Privacy Act 2020](#) was enacted on 30 June 2020 and commences on 1 December. It appears that the pandemic may have delayed the commencement of new law by a mere single month which is pretty extraordinary give the scale of global disruption.

The Foundation marked the occasion with this [media release welcoming the new privacy law](#):

Privacy Foundation welcomes new privacy law

The Privacy Foundation NZ welcomed the new privacy law just passed by Parliament.

Privacy Foundation NZ Chair, Gehan Gunasekara, said:

“The Foundation congratulates the Minister of Justice, Andrew Little, for finally achieving the replacement of the Privacy Act 1993, a task that had eluded his predecessors in the nine years since the Law Commission’s 2011 report.

“We are particularly pleased that Parliament enacted the new Privacy Act with complete multi-party support continuing a tradition for New Zealand privacy law. All parliamentary parties appreciate the importance of legislating for good information handling practice in both the public and private sectors.

“The testing times we are in, with the Covid-19 pandemic, have highlighted once more how essential it is for individuals and society to have secure means of communication and to be able to have confidence that organisations will protect their personal information.

“The Privacy Act 1993 is more than a quarter of a century old and is showing its age. It is no longer sufficient for our digital age and the new privacy law is well overdue.

“The new Privacy Act will bring benefits for New Zealanders. The law will require serious breaches to be notified to both the individuals at risk and to the regulator. It will give the Privacy Commissioner the necessary powers to act promptly and effectively. It will more effectively address risks in cross-border information transfers.”