JUSTICE COMMITTEE OF PARLIAMENT - PRIVACY BILL

SUBMISSION OF THE PRIVACY FOUNDATION NEW ZEALAND

24 MAY 2018

INTRODUCTION

1. The Privacy Foundation ("the Foundation") warmly welcomes the Privacy Bill and strongly supports its early passage. The existing Act is now 25 years old. The flexibility of its core principles has been an asset; but modern technologies have created revolutionary shifts in how we collect, share, store and use personal information. It is now urgent to update the law to ensure that it empowers action on new threats to privacy, and makes information holders publicly accountable.

2. We support the general shape and direction of the Bill, which is based on the 2011 report of the Law Commission and believe the core concepts are sound. We especially welcome the:

   - retention of the core Information Privacy Principles (IPPs) as a flexible tool for protecting New Zealanders' privacy in a turbulent environment
   - addition of the compliance notice power
   - compulsory breach notification
   - access determination power
   - introduction of additional protections for personal information sent overseas.

3. We need to face the fact that much has changed since the Law Commission issued its report seven years ago. We need to be prepared for the future, not just catching up with the past. The renewal of privacy law in New Zealand takes place against a background of major, repeated invasions of privacy; growing public fears; rising international standards (including from the European General Data Protection Regulation (GDPR) and the updated OECD principles); and huge leaps of technology in exploiting our personal data. Recent events – including the notorious Cambridge Analytica situation – suggest that the use and misuse of personal data has taken an increasingly sinister turn. The law is struggling to keep up.

4. The Foundation therefore makes a number of major proposals for new provisions that would help to bring the Bill more completely up to date. We have also made some suggestions for drafting changes that would improve the workability and effectiveness of the Bill. A particular concern is that over the next few years the GDPR will progressively enforce its new, higher, standards of data protection and business practice. The GDPR's influence in the data protection world will only increase: for many purposes, it may become the default standard. It is also the product of some of the most detailed thinking available about the rights, obligations and enforcement mechanisms that we need if we are to continue to protect privacy in an increasingly complex world. We cannot, and should not, ignore what it has to say.

5. It is especially important that New Zealand does not lose its insider status as one of the few non-European nations whose law is deemed "adequate" – that is, materially similar enough to European data protection law that European information can be exported to, held in and processed in New Zealand. Our law's adequacy is a major benefit to our businesses, including small to medium enterprises. Compliance costs for SMEs of aligning with European law might otherwise prove crippling.

6. The Bill as it stands takes some important steps towards maintaining our adequacy status. But in our view it will not do enough to ensure we keep it. Further amendments to the Bill are needed to align our law better with the GDPR, to better protect individuals' privacy and our businesses.

7. We recognise that further policy work may be necessary before we can decide whether to adopt some potential new rights, new obligations or enforcement policies. We need to make sure that they fit our New Zealand cultural and legal context, and that the legislative drafting is workable in practice. So we appreciate that not everything will be able to be included in this Bill if it is to be passed quickly.

8. It is important to commit to review – and in the near future. Technology is also highly dynamic; further amendments to the law will be needed soon if we are to keep pace.

9 We recommend that the new legislation should **set a firm date** by which the law is to be brought back to Parliament.

10. The Privacy Foundation is an incorporated society of volunteers working to protect New Zealanders' privacy rights. We highlight privacy risks and speak up for fair and practical solutions. Further information is available on our website: privacyfoundation.nz. In preparing our submission, members of the Foundation were asked for ideas. We are grateful in particular to: Associate Professors Gehan Gunasekara (Auckland University) and Nicole Moreham (Victoria University); Rick Shera, Katrine Evans and Kathryn Dalziel (lawyers in private practice), Marcin Betkier (legal researcher); and Marie Shroff (former Privacy Commissioner). We are grateful to a number of other members who have assisted. We have drawn on various members' specialist expertise (eg on the GDPR) and can explain or assist the committee or officials further in certain areas if required.

SUMMARY OF MAIN POINTS

11. The Privacy Foundation supports **early passage** of the Privacy Bill, and if possible would amend or add the following important elements:

- right to **portability** of information
- an obligation to permit people to remain **anonymous** unless the agency cannot fulfil its legitimate aims without identifying them
- protections against **re-identification** of individuals
- stronger protection for **offshore transfers** of personal information
- **increase** the level of **fines**

- require agencies to show **ongoing compliance** with privacy law
- **simplify access** provisions
- add a **reasonable person test for notifiable breaches**

12. In addition, in paragraphs 27-56, we make a number of other suggestions for changes to the content of the Bill that aim to **improve practical protections and workability** of the law. In paragraphs 57 and 58 we look at automated processing (eg profiling and algorithms) and "the right to be forgotten", and also raise these issues for the Committee to consider.

DATA PORTABILITY

13. **Data portability** is a key new right in the GDPR. It requires agencies to provide individuals with the ability to obtain a copy of their information, or get it in a readily usable format and transfer it to a new service provider.

14. Data portability is similar to phone number portability. It provides a practical mechanism so consumers have a real choice to move to new service providers. An example is where a person can uplift the complete contents of their social media profile on one platform and transfer it to a different provider – perhaps one that offers different features, or that provides greater privacy protection. This reduces the risk that large players can effectively hold people captive.

15. Data portability is not explicitly set out in the Bill. The existing right of access to one's own personal information (in Information Privacy Principle 6) goes some way towards enabling individuals to obtain and transfer their information to new providers. But data portability would be an important additional protection for consumers and enhance competition; and a plus in retaining New Zealand's adequacy status.

Recommendation:

16. We therefore **recommend** the following amendment:
Add the core ingredients of the GDPR to clause 62: that "information an individual has herself or himself provided to an agency be made available in machine readable format and be able to be directly transferable to another agency". This could be incorporated in Clause 62(1) by adding a new paragraph (g).

ANONYMITY AND PSEUDONYMITY

17. In its *Review of the Privacy Act*, at recommendation 35 (page 122) the Law Commission recommended that IPP 1 should be amended to require agencies to allow individuals to remain anonymous (or use a pseudonym) unless it was essential to identify them to fulfil the purpose for which the information was being collected. We understand that, in the original Government Response to the Law Commission's report, this recommendation was accepted, but the version of the Bill that has been introduced to the House does not reflect it.

18. We suggest that the Law Commission's recommendation should be added into the Bill. It would be a straightforward amendment (for instance, Australian Privacy Principle 2 could be used as a model).

19. Again, this new obligation would usefully build on an existing right in the Privacy Act. IPP 1 already requires agencies to collect personal information only when this is necessary for the agency's lawful purposes. However, this does not equate to a specific direction that people should be able to remain anonymous or pseudonymous where possible.

20. Such a direction would provide a relatively bright line for agencies to follow. It would also enhance privacy protection significantly; one of the best privacy protections for individuals is where agencies do not collect identifiable information about them at all. Agencies tend to assume that they need to collect identifiable information. It is the norm, and it tends to go unchallenged, in the absence of an express obligation to consider whether collecting non-identifiable information could fulfil the same aims. Adding in this obligation would require agencies to turn their minds to crafting different, more privacy protective ways of operating. It would also better reflect the data minimisation principles of the OECD and the GDPR, and support principles of "privacy by design".

Recommendation:

19. We therefore **recommend** that the Bill be amended to **enact R35 from the Law Commission report.**

REIDENTIFICATION

20. Re-identification has emerged as a concern relatively recently; it was not a topic that the Law Commission considered in its report seven years ago. Now, it is commonly accepted that an individual can be re-identified with relative ease from a dataset even where personal identifiers have been removed. Large datasets are useful for improving delivery of social benefits. But individuals are more likely to share their information where identification is mostly not permitted (see, for instance, the work of the Data Futures Partnership). Our drafting suggestion below ought to strike the right balance by countering the new right with legitimate exceptions, which are currently present in the IPPs.

21. Adding a prohibition on reidentification to the Bill will not solve all the problems. It creates a legal rather than a technical barrier. For instance, it does not guarantee that malicious actors (who are the most likely to deliberately reidentify people from datasets) will be detected or deterred. However, where an agency *is* found to have reidentified someone, it would provide a direct means of holding that agency to account.

22. There are different options for the placement of a prohibition on reidentification. One option is to add it to IPP10 (use of personal information). The option that we suggest is to add it to IPP4 as follows:

Recommendation:

Renumber the first portion of IPP 4 as subclause (1); then add a subclause (2):

"An agency may not collect personal information by re-identifying an individual from information that is held in a form in which the individual concerned is not identified (by for example being aggregated with the personal information of other individuals or rendered anonymous) unless

the agency believes on reasonable grounds" … [add paragraphs (a) - (d) from existing paragraphs (c) - (f) of IPP 10(1)].

APPLICATION OF BILL TO OVERSEAS AGENCIES WITH A LINK TO NZ

23. It is currently unclear whether the Privacy Act applies to collection, storage and disclosure of personal information of those in New Zealand by overseas entities (see for example the recent disagreement between the Privacy Commissioner and Facebook about whether Facebook is subject to the New Zealand Act). The Act is therefore out of alignment with the Fair Trading Act (s 3), the Australian Privacy Act (s 5B) and the GDPR (art3)(2)(a) and (b) all of which regulate those who carry on business or have some other link with their domestic jurisdictions.

24. The wording of our proposed amendment draws on existing formulations in NZ and overseas but has an innovation in clause 8 A(b). It adopts the existing "carrying on business" and information collection tests in place elsewhere, but adds a second alternative limb to the information collection and holding tests. The carrying on business formulation is well understood for example in Australia.

25. The location and processing of data is now almost irrelevant to exercising consumer rights, as shown by recent cases in both Europe and the US. In the era of widespread use of cloud services existing terminology may be out-dated. Our view is that New Zealand law ought to apply where an organisation in another country processes the data of New Zealand consumers, provided the organisation has a business link with New Zealand and the interests of the consumer are prejudiced in New Zealand.

Recommendation:

26. **Amend Clause 8A, adding a subclause as follows:**

Application of Act to conduct outside New Zealand

(1) "This act extends to the engaging of conduct outside New Zealand by an agency where that agency –

(a) Carries on business in New Zealand; and

(b) The personal information was -

(i) collected or held by the agency in New Zealand either before or at the time of engaging in the conduct; or

(ii) the interests of an individual have been or are likely to be prejudiced in New Zealand as a consequence of the manner in which the information was collected, held, disclosed or used, (or alternatively "manner in which the information has been collected, held etc") by the agency."

IMPROVING EFFECTIVENESS AND WORKABILITY OF THE BILL

PURPOSE

27. The purpose clause (clause 3) gives effect to internationally recognised guidelines. We recommend that this be extended to the GDPR (EU 2016/79), which harmonises privacy protections across Europe. This is important to retain our adequacy trading status in Europe. (See paragraphs 4-6 above.)

Recommendation:

28 **We recommend reference to the GDPR should be added to clause 3 (b) but that the list be left open by retaining the existing "including" in order to acknowledge the likelihood of future developments.**

NEWS ACTIVITIES EXEMPTION

29. The Foundation supports broadening of the exception to recognise that the nature of news commentary has changed significantly since 1993. On the other hand we are conscious of the danger that news items about individuals ought not to be able to be endlessly re-drawn to the public's attention when there is no longer a significant public interest in their value. Our proposed amendment makes it clear that whether the exemption applies depends on the *content* of the publication in question, not its form.

Recommendation:

Clause 6 (a) and (b): We suggest re-wording as follows:

Clause 6 (a): "the gathering of news, or the preparation or compiling of articles, programmes, books or other similar material of or concerning recent or current news, observations on recent or current news, or current affairs,…"

Clause 6 (b): "the dissemination, to the public or any section of the public, of any article programme, book or similar material of or concerning

(i) recent or current news:
(ii) observations on recent or current news:
(iii) current affairs"

PERSONAL OR DOMESTIC AFFAIRS EXCEPTION (cl 24);

30. We support retention of the exemption to allow individuals a sphere of personal and family life free of legal complications over privacy. Clause 24 should home in on these matters as clearly as possible ie matters which occur within a person's domestic realm and which are most appropriately dealt with in that realm. The defence should not become overly complex. We accept that it is probably necessary to continue to rely on the "offensiveness" filter in clause 24(3)(b) (although we note the lack of clear legal guidance about the meaning of this term

in case law or other sources). However, we query the rationale for cl 24(3)(a). Clause 212(2) of the Bill already contains offences relating to impersonation and misleading or deceptive conduct on the part of individuals and this would apply in the case of family or personal circumstances where there is malicious intent. Extending the Bill to other instances when malicious intent is not present may be unnecessary and burden the OPC with complaints. A typical situation may be a practical joke played within a family setting (eg birthday). When conduct is offensive to a person of ordinary sensibilities it is already covered by cl 24(3)(b). If paragraph (a) is to be retained we suggest it be limited to the obtaining of images through misleading conduct as opposed to any misleading conduct.

31. We also believe that the new "lawfulness" requirement in cl 24(2)(b) adds undesirable complexity to the exemption. Showing that information was collected lawfully will require detailed consideration not only of a number of legislative protections but also common law actions for breach of privacy and breach of confidence. This will be a complex task and it is not clear that it reflects the aim of this exemption (ie to exclude matters belonging in the domestic, rather than legal, sphere).

32. It also needs to be clear that something ceases to be part of a person's domestic affairs if he or she disseminates it to the world at large (eg if a person copies a private document at home and uploads it to an openly available internet site or if a person takes intimate photographs of a sexual partner then shares it online). Given that "offensiveness" is a subjective concept, in our view this type of behaviour should be expressly exempted from the operation of cl 24. Some further definition of "publicly available" might be necessary to make the scope of such a clause clear.

Recommendation: We recommend the committee reconsider the provisions of Cl 24

THE IMPACT OF VULNERABILITY ON FAIRNESS OF COLLECTION

33. Under clause 19 of the bill it is proposed that an agency collecting personal information must act "having regard particularly to the age of the individual concerned". It is far from clear why age has been singled out from any other kind of vulnerability.

34. The impetus for the amendment is likely to have been a concern for children's privacy. However, the addition of the phrase does little to address this very important issue – to do so, the Bill would need to consider children's privacy much more directly (as, for example, has occurred in the United States with the enactment of the Children's Online Privacy Protection Act). Also, it does not reflect the fact that age (whether youth or seniority) may not always equate to vulnerability – though where it does, it clearly should be properly considered. Nor is it the only type of vulnerability that should be considered in terms of how an agency collects personal information.

34. Instead, our view is that an agency should consider the vulnerability of the individual concerned, whether that vulnerability is the result of age, mental capacity, disability, language barriers, or family/occupational background. For instance, it may well be unfair and unreasonably intrusive for a service provider

to require someone who is vulnerable because of family issues to share highly personal information in an open plan office.

35. **Recommendation:**
IPP 4 (b) should read:

"by a means that, in the circumstances of the case (having regard particularly to the characteristics [or, alternatively, "vulnerability"] of the individual concerned)…"

We also suggest adding a **further sub-paragraph** modelled on IPP 11(2) as follows:

"Without limiting the generality of IPP 4 (1)(b), an example of a characteristic of an individual is the age of the individual"

RIGHTS OF THE CHILD: IPPs 2, 3, 6, 10 & 11

36. One of the common difficulties with these principles (which cover source, collection, access, and limits on use and disclosure) arises when the individual is a child. It is currently not clear under the Privacy Act what role parents play in ensuring that a child's privacy rights are protected or enforced.

37. In the health context, this has been managed successfully under the Health Act and Health Information Privacy Code (HIPC) by creating the role of a representative, which includes a parent or guardian for a child under the age of 16 years. This role is particularly important under rules 6 and 11, which help agencies identify when a child's health information should be given to parents.

38. We are aware that this is an issue that creates constant queries at all schools and any institutions looking after children under the age of 16. The Foundation notes that in the Bill (clause 120) the role of representative is created for parents or guardians in the event of a notifiable privacy breach involving a child under the age of 16. This appears to be a useful example that could be extended to other places in the Bill, particularly the IPPs.

39. Recommendation:
that the role of representative be extended to cover principles 2,3,6,10 and 11 and those principles are amended to incorporate the role of the representative (following the model in the HIPC 1994).

NOTIFIABLE PRIVACY BREACHES

40 We welcome the introduction of notifiable privacy breaches. We believe this is a very important element of protection. Being aware of a risk enables individuals to act to reduce that risk. But we believe the law should more precisely define the notification level.

41. Clause 117 refers to any types of harm listed in s 75(2)(b) – that is, the types of harm that define whether there has been an "interference with privacy". At one level, it appears logical to tie the standard of harm to one already used in the Act and interpreted in the case law. However, in practice, the standard is likely to create significant problems, and to lead to over-notification.

42. This is because its effect is to create a *low* threshold for agencies to have to notify privacy breaches (contrary to the Law Commission's view that only suitably serious cases should attract an obligation to notify: see 7.22). There is little or no guidance provided as to when to notify, except by reference to a notoriously flexible standard of harm. As a consequence agencies may tend to notify just to be on the safe side as opposed to when an appreciable risk to individuals exists. Crying wolf too often may lead to individuals being de-sensitised to situations when notification can actually be useful.

43. We think that instead of a purely subjective approach, an objective measure should be used. For example the Australian statute refers to the condition in which "a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates". In the GDPR the breach must be "likely to result in a high risk to the rights and freedoms of natural" persons. In order to promote consistent application, there should be guidance available. Perhaps using examples of which breaches should be notified could do this.

44. We suggest the Bill needs to employ language (such as the "reasonable person" formulation), which encapsulates both an objective test and one that is future-proof as it allows the state of current technology and safeguards to be a factor. Hence factors that can be taken into account include whether the personal information subject to the breach was protected by encryption and other measures or whether steps have been taken to recover the data.

45. The reference to section 75(2)(b) attempts to ensure that breaches that might result in trivial or minor harms are not covered. As the section (s 66 in the current Act) has been interpreted to require significant loss or humiliation, so a mere breach of an IPP would be insufficient. But the public may need considerable education in this aspect. Perhaps a couple of examples in the legislation might be helpful.

46. In addition, we are not convinced the *revealing of a trade secret* should be an unconditional exception for notifying individuals. It is irrelevant to whether the agency should be required to notify the Privacy Commissioner (who must in any case protect information that is secret, or privileged). This standard may in practice prove too easy to reach, as agencies would be free to define this themselves. Also, some breaches may well be serious enough to justify the revelation of trade secrets.

47. **Recommendation: Clause 117 (1)**

We support re-wording this as follows:
- "notifiable privacy breach means a privacy breach that a reasonable person would conclude has caused any of the types of harm listed in section 75(2)(b) to an affected individual or individuals or where a reasonable person would conclude there is a risk it will do so"

We also recommend **removing the exception for revelation of trade secrets**

INCREASED PENALTIES; ONGOING COMPLIANCE

48. We support the Privacy Commissioner's recommendations in his report to Parliament of February 2017 to:

- **increase the level of fines** provided for in the Bill to $100,000 for individuals and $1m for corporates, for serious breaches, to bring us closer to GDPR and Australian law;
- a requirement to show **ongoing compliance** with privacy law to allow the Commissioner to identify and address systemic issues.

SIMPLIFYING THE PROVISIONS ON ACCESS TO PERSONAL INFORMATION

49. Many provisions in part 4 of the Bill now contain a distinction between requests by individuals for confirmation about whether an agency holds their personal information (IPP6(1)(a)) and requests for access to that personal information (IPP6(1)(b)). Our view is that this is unnecessarily complex.

50. While IPP6 has always catered for these two types of requests, the provisions in parts 4 and 5 of the current Privacy Act are relatively simply drafted. They treat all IPP6 requests in the same breath. They do not try to specify how an agency should act depending on whether the request is made under IPP6(1)(a) or (b). That is a pragmatic approach – and it works. It has not created any practical problems. In contrast, the Bill's drafting shows how lengthy, repetitive and confusing it becomes for the ordinary reader when an attempt is made to split out how the different access requests should be handled. Given IPP(1)(a) requests are relatively rare – more often, people just ask for their information – the introduction of the complexity is even more puzzling.

51. The problems are the same in relation to requests to correct information, and requests to attach a statement of correction to a record. Again, the distinction is immaterial in practice – most people just ask for correction. Which form of correction is available will simply depend on the circumstances and can be worked out.

52. The access provisions – the right for people to see what information an agency has about them – lie at the core of the Act. Without those rights, it is hard for a person to see whether the other privacy principles have been upheld, to hold the agency to account for its actions, or to understand the situation in which they find themselves. It is therefore vital that the provisions relating to access (and, to some extent correction) should be easily understood by individuals, and easily applied by agencies. The current drafting in the Bill makes the provisions harder to understand, without adding any additional rights, obligations or value.

52 **Recommendation:**
Part 4 We therefore strongly urge simplification of the new access provisions, to **remove the distinction between the subclauses in IPP6 and IPP7**. The provisions should refer only to IPP6, and IPP7 (as relevant), and any unnecessarily repetitive provisions deleted.

BETTER PROTECTION FOR VICTIMS OF VIOLENCE

53. For many people, having their location and contact details on a public register can create serious, even deadly, safety risks. Many (if not most) public registers therefore currently offer victims of violence and harassment the opportunity to suppress some of their personal information, particularly their contact details.

54. However, it is hard for people to identify all the public registers on which their details may be displayed. For instance, they may be aware that they can ask to be placed on the closed electoral roll, but may not think about asking for their contact details to be suppressed from other registers.

55. The Foundation agrees with the Privacy Commissioner that suppressing information for safety reasons should be simpler. People should be able to apply to a central agency, and supply the evidence (usually a protection order or harassment order) to support their application for suppression. That central agency should then be responsible for distributing the application to all public registers. Registrars can then be responsible for making a decision about whether to suppress information in line with their normal operational rules for the register.

Recommendation:

56. We therefore **recommend** that a **section should be added alongside those relating to public registers, establishing a central mechanism for suppression applications on safety grounds.**

AUTOMATED PROCESSING

57. A noticeable absence from the Bill is any provision for protection in the environment of **automated processing**. We understand this is a complex issue. But there is growing awareness that where algorithms or automated profiling are used, there is the potential for discriminatory or otherwise prejudicial decisions to be made about individuals. Few or no rights are currently available for access and redress. This issue is included in the GDPR, and we urge the committee and the government to monitor progress in Europe and take action in if required to provide appropriate rights for New Zealanders. NZPF suggests that when developing appropriate rights the committee and government give consideration to two key principles in regard to automated processing. First, there ought to be **a right to manual equivalence**, meaning that an agency ought not to be able to use as a defence for breach of an IPP that the personal information was collected, used or disclosed robotically or through automated processes where such a defence would be unavailable had the processing been undertaken manually. This suggested right is closely tied to the right proposed below, viz. that of the **right to contextual integrity.** Secondly, when automated processing is likely to result in the types of harms listed in cl. 75(2)(b), the individual should have the **right to human intervention** before the processing takes place.

RIGHT TO BE FORGOTTEN

58. The so-called "right to be forgotten" has recently been highlighted in overseas developments, including cases and in the GDPR (art 17). However, the supposed right has been invoked in New Zealand in the context of the tort of publicity given to private facts and arguably is substantially present within the IPPs contained in the Privacy Act 1993 and the proposed legislation

to replace it, the Privacy Bill 2018. PFNZ argues that
while the IPPs specifically provide for deletion in some instances (see cl. 6 definition of "correct") the availability of the right largely depends on the manner in which it has been applied in cases decided before the Human Rights Review Tribunal (HRRT) as well in the numerous case notes issued by the Privacy Commissioner. The digital sphere poses special challenges to the need for erasure and related data privacy concerns, including the limits of correction, data quality (the need to ensure personal information is accurate prior to using it) and data retention limits. For example, there is the issue of websites linking outdated or irrelevant information and search engines (usually robotically) indexing them. PFNZ supports the addition of the **right to contextual integrity when information is linked or indexed online**. For example, when an insolvent person has been discharged from bankruptcy, continued publication of links or material concerning the circumstances of the insolvency would be unwarranted (unless say a business partner of the individual were to subsequently become insolvent). Hence if person A (the original agency that published the information) would no longer be entitled to publish it, then person B ought to not also be entitled to publish it. We believe the Bill ought to address these issues – perhaps by addition of a whole new Part or Subpart – addressing both automated processing and contextual integrity when linking or re-publication of personal information takes place. Freedom of expression considerations would, of course, need to be factored in. Incorporation of these aspects would in our view in large measure serve to ensure New Zealand continuing to enjoy "adequacy" status for transfers of personal information from the EU.

CONCLUSION

58. As one of our members, Rick Shera, said in the attached article published recently in the *NZ Herald*: "International consistency is no longer a nice to have. It is a must for a law that is one of the main bulwarks against global online overreach into our personal lives." To protect individuals and strengthen their rights, and to strengthen and simplify our law, we urge the committee to consider our recommendations and give priority to passing the Privacy Bill.

59. As noted above, we have drawn on various PFNZ members' specialist expertise (eg on the GDPR) and can further explain or assist the committee, or officials, in certain areas if required.

60. We would appreciate the opportunity for representatives of the Privacy Foundation New Zealand to speak to the Committee in support of our submission.