



**Australian
Privacy
Foundation**

2 November 2015

<http://www.privacy.org.au>
Secretary@privacy.org.au
<http://www.privacy.org.au/About/Contacts.html>

Katerina Pavlidis

Adviser, Regulation and Strategy
Regulation and Strategy Branch
Office of the Australian Information Commissioner
GPO Box 5218 SYDNEY 2001
consultation@oaic.gov.au

Dear Ms Pavlidis

Consultation draft: PCEHR (Information Commissioner Enforcement Powers) Guidelines 2015

This submission by the Australian Privacy Foundation (the APF) is in response to requests by the OAIC for comments on the proposed PCEHR (Information Commissioner Enforcement Powers) Guidelines 2015.

It follows previous APF submissions on health privacy which are available on-line, a selection of which are detailed at the end of this submission.

Standing of the Australian Privacy Foundation

The Australian Privacy Foundation (the APF) is the nation's premier civil society organization concerned with privacy.

Its membership includes lawyers, academics, information technology experts, health informatics fellows, communication policy analysts and non-specialists. It has been recognised through invitations to provide testimony in parliamentary inquiries and other consultations regarding data protection, along with participation in high-level international fora. A brief backgrounder is attached.

Overall observations

As a general observation the APF is disappointed that the Guidelines are drafted in such broad, general and vague terms. It was not legally necessary for that to be the case. It is certainly not desirable from a policy perspective. As proposed they can essentially mean what the reader, and the Information Commissioner, wants them to mean. Guidelines should serve two functions. The first is, clearly, as a legislative instrument which will provide guidance to the Information Commissioner in the exercise of statutory powers. Drafting the guidelines in such broad terms, without specifying what transgressions will attract greater attention and more assertive action, the Information Commissioner acquires unto himself such flexibility as to justify inertia without accountability. The second function is to make it clear to organisations and agencies how the Information Commissioner will approach the regulation of the legislation. That some issues will warrant a more assertive form of action than others. The draft guidelines as currently constituted do not fulfill that role.

Part 1 Preliminary

1. The APF has no comment to make about this Part. It sets out matters which are of no controversy and are necessary boilerplate

Part 2 General principles relating to enforcement action and the exercise of investigative powers under the PCEHR Act and the Privacy Act

2. The APF is concerned about the scope of clause 6.3 in particular that which provides:

The Information Commissioner may decline to investigate or further investigate a complaint if there is no reasonable likelihood of a conciliated outcome.

That the Information Commissioner has the power and exercises it is not the issue. The issue is the basis for declining to investigate. The APF is very aware of the Information Commissioner exercising his power to decline to investigate. What is far less clear is the criteria used or factors considered in exercising that power. There should be some form of criteria, or relevant factors, which are used when making a decision to decline to continue to investigate a matter. The APF believes it is a discretion exercised too regularly, with little associated policy logic and without sufficient scrutiny and transparency. This is the antithesis of effective regulation.

3. The APF is concerned about the vagueness of the wording set out above. It is not necessary, or desirable, to know why the Information Commissioner declines each complaint however it is important to understand the logic and parameters in the process the Information Commissioner operates. That may be used to educate those who may or may not wish to make a complaint in future. At the moment there is little discernible logic in the decision making process involved in declining to investigate some complaints.
4. Even as drafted the APF is concerned about the vagueness of the drafting. What constitutes a reasonable likelihood of a conciliated outcome? What factors are relevant? It does not have to be an exhaustive list. The current structure is not helpful. There are no tangible parameters or factors which gives any party, whether a putative complainant or respondent or an interested body such as the APF can consider. As it stands a non-responsive respondent may decline to co-operate. That should never be a factor in declining to investigate. Without some form of criteria against which the Information Commissioner decides not to investigate or to further investigate there remains the residual concern that decisions are arbitrary. This does not assist in building a culture of compliance with privacy regulation or confidence of individuals that their complaints will be properly considered. Given compliance generally is poor that is a matter of concern.
5. As drafted the factors set out in clause 7.1 are uncontroversial in and of themselves. Unfortunately they are so broad as to be anodyne. They do not provide any impetus or guidance for the Information Commissioner to take action in certain circumstances as a matter of priority. In the APF's view it would be beneficial if there was provision made for the Information Commissioner to give priority to breaches involving the release of sensitive information, or even particular types of sensitive information for example. It is a discipline upon the Information Commissioner and serves as notice on those bound by the legislation. Given the anemic approach to enforcement action taken in the past this would both make it clear to those affected by the legislation that the Information Commissioner will in the future adopt an approach consistent with effective regulation.

Part 3 Use of enforcement powers under the PCEHR Act and

6. Clause 8.3 as drafted is overly broad and anemic. It should be amended. The APF recommends redrafting in the following terms:

To be acceptable to the Information Commissioner, the terms of an enforceable undertaking must:

- a. describe the alleged contravention(s) that is the subject of the Undertaking

- b. outline specific steps the person will take to rectify the contravention so as to ensure that it is not repeated or continued. This will usually include, as a minimum, a requirement for the person to complete reviews and establish a monitoring and reporting framework;
- c. contain dates by which the person is required to complete each step having regard to the need that those dates are both reasonably capable of being complied with but also that they be completed at the earliest practical date. The convenience of the person is not a relevant factor;
- d. be capable of implementation and include action which is capable of being measured or tested objectively;
- e. be certain and capable of enforcement.

7. Clause 8.4 should be amended to provide:

The Information Commissioner will not accept an enforceable undertaking that:

- a. denies or otherwise seeks to qualify responsibility for an alleged contravention of the PCEHR Act or Privacy Act;
- b. merely undertakes to comply with the law without providing verifiable and specific details of how total compliance will be achieved;
- c. seeks to impose terms or conditions on the Information Commissioner.

8. Clause 8.5 is drafted in very vague and broad terms which defy easy understanding. Each of the 3 factors set out have defects being:

- (a) reference to the particular circumstances of the matter is, at minimum, trite. As drafted the particular circumstances may not be taken into account when deciding to accept an undertaking. How can the Information Commissioner not consider the particular circumstances of a case/matter, better described as the facts? Under what conditions will the particular circumstances not be considered? The process is not a theoretical exercise. Subsection 8.5(a) is poorly drafted, giving rise to the possibility of a clearly unintended and legally ridiculous outcome.
- (b) the factors in subsection 7.1 encompass all relevant factors that a decision maker would consider. Put another way, it is difficult to envisage any other factor that could possibly be considered. That catch all approach renders the operation of the sub section essentially meaningless.
- (c) if the Information Commissioner does not believe the Respondent has the ability to comply with the terms of the undertaking then it can not be considered as an option. Similarly if the Information Commissioner is of the view the respondent has no intention of complying with the terms of the undertaking then the process should not commence. To do otherwise would be an abrogation of the Information Commissioner's responsibilities and a misuse of his or her discretion. As drafted subsection 8.5(c) is not

drafted in mandatory terms. That is an error. This issue should be a stand alone pre requisite and, accordingly, should be drafted in mandatory terms. As currently drafted the Information Commissioner may, or may not, consider this as a relevant factor. To not consider this as a relevant factor would be foolish.

9. Sub section 8.8(a) is vague. What does “impractical” encompass? If it relates to a cost of compliance by the respondent the starting point must be that that is an irrelevant consideration. Or at minimum it should be severely constrained as any sort of consideration. As drafted it has no practical and objective meaning. What may or may not be acceptably “impractical” should be considered through the prism of, and restricted to, acts, facts, matters or things which were not known or could not reasonably have been foreseen at the time of entering into the undertaking. Put another way, if compliance is impractical because of information was withheld by the respondent and now becomes an issue or events which the respondent was aware of in the future but hoped would not occur then the problem is the respondent’s alone. It should deal with it. As drafted this subsection means very little. The requirements should be more onerous.
10. Subsections 8.9 – 8.10 are drawn in such broad and vague terms as to be almost meaningless. The starting point is that a breach of an undertaking is a very serious event. While the actions set out in sub section 8.9(a) – (d) are uncontroversial the terms set out in paragraph 8.10 can mean whatever the reader, and most particularly the Information Commissioner, chooses. Clearly the particular circumstances are relevant. And it would be difficult to undertake any sort of consideration without having regard to at least some of the factors in sub section 7.1. The guidelines should be drafted in more assertive terms, to the effect that the Information Commissioner will approach a breach on the basis that action will be taken under one of more of 8.9(a) – (d) unless there are strong policy or factual considerations to warrant a lesser response. As drafted the consequences of a breach may be insignificant, if any action is taken at all. That is poor policy and an abrogation of statutory responsibilities.

Enforceable undertakings under the Privacy Act

11. For reasons set out in paragraph 8 above sub section 9.5 is inadequate. Similarly sub sections 9.8 and 9.10 also deficient for the reasons set out in paragraphs 9 & 10 above.

Determinations

12. Paragraphs 10.6 and 10.8 - 10.10 are anodyne to the point of meaningless. They are also vague and general and do not illuminate the process adopted by the Information Commissioner. It remains unacceptably opaque. The language is so general and bureaucratic that it can mean anything in practice. As a Guidance it has little utility for any interested party.

13. Sub section 10.10(d) as drafted causes concern. It currently provides:

whether the person has cooperated with the Information Commissioner's enquiries or investigation, and if not, whether the Commissioner believes that it is necessary to make formally binding declarations that the person must take certain steps to address the interference with privacy

This may be understandable if the basis of this sub section is a statutory requirement. It is not immediately apparent what that provision might be. If there is no statutory requirement the provision should be deleted. Whether a person/respondent does not cooperate is irrelevant. There are ample powers under sections 44 – 47 of the Privacy Act to obtain necessary evidence to make a determination. That the provisions are little used is not to the point. The cooperation or otherwise of a respondent is a wholly irrelevant consideration for the purpose of deciding whether to make a determination.

14. Sub section 10.10(e) should be redrafted. As currently drafted it is an inchoate and incorrect consideration of the Information Commissioner's role. Whether the Information Commissioner and respondent disagree whether an interference with the privacy has occurred is irrelevant. It is what the Information Commissioner decides based on the facts available that is the issue. A determination is the end of the process initiated by the Information Commissioner. Clearly if the Information Commissioner makes a determination the question is resolved. The primary purpose of a determination is not to set precedent if that is what is being suggested in sub section 10.10(e). To the extent that this sub section 10.10(e) has any meaning it is likely to reinforce and endorse a timid approach to making determinations. That is the antithesis of good regulation.
15. Sub section 10.10(f) implies a public interest test that may be applicable or a relevant factor in considering whether to make a determination. There is no such requirement in the Privacy Act. It is an *ultra vires* consideration. As a matter of law it should not be contained in a legislative instrument.
16. For reasons set out in paragraph 8 above sub sections 10.12 and 11.2 should be redrafted.

Injunctions

17. Sub sections 11.1 and 12.1 are uncontroversial. They recount the Information Commissioner's powers. Sub sections 11.2 and 12.2 makes little policy sense. As drafted the provisions state that the principles and factors relevant to the use of injunctive relief is the same as other enforcement options. That is legally incorrect. The relevant criteria in the grant of injunction have been the subject of considerable development and statement by the courts, including but not limited to the Federal and High Courts. Those factors should be considered in the guidelines. Put another way, it is artificial not to do so. It ignores the legal reality.

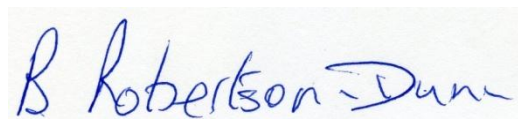
18. Interestingly the APF notes there is no recorded decision of the Privacy Commissioner exercising his or her powers under section 98 of the Privacy Act in the 27 years it has been in operation. The power is comparable to the previous Trade Practices Act, now Australian Consumer Law, and the Corporations Act 2001. The failure to use the provision is not because the behavior of agencies and organisations have been model citizens or their transgressions so minor so as to not warrant its use. There are ample examples of extremely poor compliance and significant breaches in the last 27 years. The only inference open is that the provision has been rendered dead letter because of a policy, *de facto* or otherwise, by Privacy Commissioners to refrain from its use. This has been a failure of public policy. This should be remedied in the Guidelines with a stated willingness to use this power in the event of a serious ongoing breach, for example. The power in section 98 is not restricted. There is no reason why its use should be.

Civil Penalty Provisions

19. The factors set out in sub section 13.4 are essentially copies of the contents of sub sections 8.10 and 11.2. Like those sub sections they are so broad and vague as to be meaningless. Civil penalty proceedings can be a very important part of effective regulation of the legislation. The guidance should specify that the proceedings will be considered as a *prima facie* starting point in the event of a significant data breach involving sensitive information as a result of a failure to of data security to comply with industry standards, for example. Civil penalty proceedings will have an impact on improving compliance with the legislation. The lack of assertive action in the past has resulted in a poor culture of compliance.

Thank you for giving us the opportunity to comment on these guidelines.

Yours sincerely

A handwritten signature in blue ink that reads "B Robertson-Dunn". The signature is written in a cursive, slightly slanted style.

Dr Bernard Robertson-Dunn

On behalf of the Board of the APF

Bernard.Robertson-Dunn@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies <http://www.privacy.org.au/Papers/>
- Resources <http://www.privacy.org.au/Resources/>
- Media <http://www.privacy.org.au/Media/>
- Current Board Members <http://www.privacy.org.au/About/Contacts.html>

- Patron and Advisory Panel <http://www.privacy.org.au/About/AdvisoryPanel.html>

The following are some of the submissions previously provided to the OAIC

APF submission - eHealth record system OAIC Enforcement Guidelines.

<https://www.privacy.org.au/Papers/OAIC-PCEHREnf-120924.pdf>

Guidelines for developing codes

Issued under Part IIIB of the Privacy Act 1988 – Consultation draft Submission to the Office of the Australian Information Commissioner April 2013

<https://www.privacy.org.au/Papers/OAIC-CodeDevG-130415.pdf>

Improving OAIC's Privacy regulatory action policy

Submission to the Office of the Australian Information Commissioner (OAIC) 31 March 2014

<https://www.privacy.org.au/Papers/OAIC-RegPolicy-140331.pdf>

[eHealth record system \(PCEHR\) Data Breach Notification](#), Submission to OAIC (29 Sep 2012)

[eHealth record system \(PCEHR\) Enforcement Guidelines](#), Submission to OAIC (24 Sep 2012)

[Guide to Privacy Regulatory Action](#), Submission to OAIC (12 Dec 2014)

[OAIC's Draft Guide re Privacy Impact Assessments](#), Submission to OAIC (31 Mar 2014)