

ONLINE PRIVACY BILL AND PRIVACY ACT DISCUSSION PAPER: INCREASED ENFORCEMENT RISK AND REGULATORY CHANGE

17 December 2021 | Australia

Legal Briefings - By **Christine Wong, Thomas McClintock and Soraya Pradhan**

As explored in our earlier briefing article, the recent release of the exposure draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (the **Exposure Draft**) and the Privacy Act Review - Discussion Paper (the **Discussion Paper**) canvass a wide array of reforms to privacy regulation in Australia.

This update focuses on what this signals for future enforcement of privacy breaches. Please see [our previous article](#) for an overview of the changes.

The Exposure Draft and Discussion Paper signal an increased focus on the enforcement of privacy breaches in the future, and greater penalties being imposed for those breaches. This heralds a shift away from regulatory action which has historically focused on “softer” compliance steps, such as the resolution of complaints and issuing of determinations.

The Exposure Draft and Discussion Paper acknowledge that the scale of new challenges presented by evolving technology requires a rethink of privacy laws and how they should be effectively enforced. This is consistent with the uptick in technology platforms related investigations undertaken by the Information Commissioner (see further below).

Against that backdrop, a key driver of **effective regulatory enforcement** will be the adequacy of resourcing received by the Information Commissioner as well as the flexibility of its regulatory toolkit. For **individual enforcement of rights** (including via class actions), a key driver will be whether or not a direct right of action for individuals or statutory tort are introduced.

Submissions on the Exposure Draft were due on 6 December 2021 and submissions on the Discussion Paper are due on 10 January 2022.

TOP 10 TAKEAWAYS

Our top 10 takeaways are set out below.

<p><u>ICON6.PNG</u></p> 	<p>QUERY <i>“Query” icon is for items previously considered in the ACCC’s Digital Platforms Inquiry (DPI Report) or Australian Law Reform Commission Report 123 released in June 2014, Serious Invasions of Privacy in the Digital Era (ALRC Report).</i></p>
<p><u>ALERT.PNG</u></p> 	<p>ALERT “Alert” icon is for items not subject to previous discussion</p>

INVESTIGATORY POWERS

ICON6.PNG



1. ISSUE INFRINGEMENT NOTICES OR SEEK CRIMINAL PENALTIES

New powers to **issue infringement notices or seek criminal penalties** in the event of repeated non-compliance with notices to produce information and contained in the **Exposure Draft**.

ALERT.PNG



2. UNDERTAKE PUBLIC INQUIRIES

The **Discussion Paper** suggests new powers to **undertake public inquiries** as directed or subject to Ministerial approval (akin to the ACCC's powers).

RESOURCING MODEL FOR THE INFORMATION COMMISSIONER

The **Discussion Paper** canvasses:

ALERT.PNG



3. INTRODUCE A NEW FUNDING MODEL

a new funding model, including the imposition of levies on entities which operate in a high privacy **risk** environment.

ALERT.PNG



4. DISCUSS ALTERNATIVE REGULATORY MODELS.

alternative regulatory models, including the separation of complaints handling from enforcement.

ENFORCEMENT OUTCOMES - EXPANDING THE TOOLKIT

The **Exposure Draft** proposals allow the Commissioner to take an expanded set of actions including:

	<p>5. REVIEW OR REMEDIATION New powers to issue infringement notices or seek criminal penalties in the event of repeated non-compliance with notices to produce information and contained in the Exposure Draft.</p>
	<p>6. INCREASED CIVIL PENALTIES FOR SERIOUS AND REPEATED INTERFERENCES WITH PRIVACY This would increase to \$10m, three times the value of the benefit obtained or 10% of domestic annual turnover, bringing the regime in line with existing civil penalty regimes, such as under the Australian Consumer Law.</p>
<p><u>ALERT.PNG</u></p> 	<p>7. PROPOSED INTRODUCTION OF A CIVIL PENALTY AND INFRINGEMENT NOTICE REGIME The proposed introduction of a civil penalty and infringement notice regime for lower level interferences with privacy. This suggests a desire to pursue less serious breaches as part of driving overall compliance.</p>

INDIVIDUAL RIGHTS OF ACTION

ICON6.PNG



8. POTENTIAL DIRECT RIGHT OF ACTION

Introduction of a direct right of action.

A direct right of action would allow individuals to bring claims against APP entities for breaches of the Act.

The introduction of this right would represent a step change in exposure for organisations and privacy class action risk, which has emerged in a significant way in other jurisdictions. Given privacy incidents often affect a very large number of individuals, even if there is only non-financial loss or nominal damage, the overall quantum may be significant.

Allied to that would be greater judicial consideration and clarification of privacy legislation.

The Discussion Paper notes the potential for an overwhelming number of claims if a direct right of action were to be implemented, and so proposes requirements for the complainant to make a complaint to the OAIC and attempt conciliation, before being able to seek leave from the Federal Court to commence proceedings.

At this stage, no threshold of seriousness is proposed before direct right of action claims could be brought. The Discussion Paper notes that further issues regarding the use of class actions will be addressed in the separate and ongoing consideration of the class action regime by the Parliamentary Joint Committee on Corporations and Financial Services.

As the Discussion Paper does not provide a definitive recommendation on the form the statutory tort may take, the consequences of such a model is unclear.



9. POTENTIAL STATUTORY TORT OF PRIVACY

Introduction of a statutory tort for serious interference with privacy

Similarly, the introduction of a statutory tort has the potential to change exposure for organisations. Multiple models of statutory tort are raised for consideration – as the form of the tort informs the extent of the exposure, the response to the suggested options will be a key area to watch. Unlike the direct right of action, a statutory tort may allow individuals to bring claims for breaches of privacy falling outside of the provisions of the Act. The Discussion Paper noted the model of statutory tort recommended in the ALRC Report, which limits the circumstances where claims may be brought, contains a seriousness threshold and allows for damages for non-financial loss such as emotional distress, as well as damages for financial loss or other remedies.

In noting criticisms of the ALRC Report, the Discussion Paper ventilates alternate models employed by other jurisdictions. This includes a minimalist statutory tort, allowing the common law to develop as required and actions in equitable breach of confidence.

ALERT.PNG



10. EXTENDING THE SCOPE OF ORDERS MADE BY THE FEDERAL COURT

Enabling the Federal Court to make any orders it sees fit following a serious or repeated interference with privacy.

This may include ordering companies to take steps to ensure such conduct is not repeated or continued, take action to redress the complainant's loss or damage or pay compensation.

This proposal intends to prevent the OAIC from having to make a separate application after the conclusion of the civil penalty proceeding.

Our more detailed outline of the reforms is provided below.

HOW DOES THIS SIT AGAINST THE OAIC'S RECENT REGULATORY ACTIVITY?

In the last 12 month period, the OAIC's investigation activity has seen a particular focus on technology, including online platforms. Significant examples include:

7-ELEVEN

the Commissioner initiated an investigation into 7-Eleven Stores in relation to facial images and faceprints of customers obtained through facial recognition technology used while customers were undertaking a customer feedback survey. In September 2021, the Commissioner found that this private information was taken without consent or notification and had interfered with the privacy of their customers. 7-Eleven was found to have breached the APPs and the Commissioner made declarations that the conduct not be continued, but did not sanction 7-Eleven.

CLEARVIEW

The Commissioner also initiated an investigation into Clearview AI in relation to a tool which collected images from individuals that were publically available online and offered a facial recognition tool to law enforcement. The investigation was joint with the UK Information Commissioner's Office (**ICO**). In October 2021, the Commissioner found that, despite the limited availability of an opt-out mechanism, Clearview's tool involved collection of biometric personal information without consent or notification, and that reasonable steps were not taken to ensure the information was accurate, complete and relevant, in breach of the APPs. The Commissioner declared that the practice must cease.

A TECHNOLOGY COMPANY

In a further Commissioner initiated investigation into a technology company, the Commissioner found in June 2021 that it interfered with the privacy of 1.2 million Australians by failing to take reasonable steps to protect their personal information or destroy or de-identify personal information. User information was subject to unauthorised access in a cloud-based cyber-attack in 2016. Declarations were made, including that the company must prepare policies to address the conduct, and engage an independent expert to prepare a report.

FACEBOOK

In 2020, the Commissioner commenced proceedings against Facebook alleging serious and repeated interferences with privacy of over 300,000 Australian Facebook users in contravention of section 13G of the Act. The Commissioner claimed that a tool available on Facebook's platform, used by the "This is Your Digital Life" application, requested and obtained personal information of Facebook friends of those who had installed the application, despite those affected individuals not installing the application themselves. The proceedings remain ongoing.

While the decisions and commencement of proceedings above provide a strong indication of the increased focus on regulating technology companies' use of personal information, the OAIC is yet to take aggressive action or obtain significant penalties. This is a sharp contrast from the privacy enforcement under the GDPR in the European Union, which has given rise to frequent enforcement activity resulting in multi-million euro fines against Amazon (€746m), WhatsApp (€225m) and Google (€50m).

The OAIC has had long-standing difficulties with obtaining funding. The Discussion Paper notes that appropriate resourcing is a necessary component of undertaking substantive enforcement action, in particular to initiate and sustain court proceedings against large multinational technology giants that have the potential to last for years.

The budget for the 2022 financial year considers an increase in the OAIC's funding to around \$28m. This funding is still significantly less than the ACCC, ASIC or even AUSTRAC. As such, while this increase likely indicates an increase in activity by the OAIC, it is unclear whether this will be sufficient for frequent cost-intensive methods of enforcement such as commencing court proceedings.

The Discussion Paper's proposal to impost an industry funding arrangement is intended to bolster the OAIC's funding model. The Discussion Paper details the success of similar models as used by ASIC and the ICO. The response to and potential implementation of this funding model may be a critical component in the OAIC's future regulatory strategy and will be an area to watch in future reform proposals.

Further specific details of the proposals can be downloaded below:

[Download PDF](#)

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



CHRISTINE WONG
PARTNER, SYDNEY

+61 2 9225 5475
Christine.Wong@hsf.com



JULIAN LINCOLN
PARTNER, HEAD OF
TMT & DIGITAL
AUSTRALIA,
MELBOURNE

+61 3 9288 1694
Julian.Lincoln@hsf.com



KAMAN TSOI
SPECIAL COUNSEL,
MELBOURNE

+61 3 9288 1336
kaman.tsoi@hsf.com



MARINE GIRAL
SOLICITOR,
MELBOURNE

+61 3 9288 1496
marine.giral@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2022

SUBSCRIBE TO STAY UP-TO-DATE WITH INSIGHTS, LEGAL UPDATES, EVENTS, AND MORE

Close