HERBERT SMITH FREEHILLS

REGULATORY ENFORCEMENT IN CYBER SPACE: WHAT HAVE WE SEEN AND WHAT CAN WE EXPECT?

02 December 2021 | Australia
Legal Briefings – By **Tania Gray, Christine Wong, Nataly Sikorski, Scott Preswick and Adam Irwin**

Australia has a congested, complex and fast-moving regulatory framework covering cyberspace. Our experts will plug you in.

KEY TAKEAWAYS

- The regulatory landscape is congested, with varied obligations that are relevant to cyber security incidents administered by a patchwork of regulators
- The number of cyber security related regulations is increasing.
- At the same time, we are seeing a shift away from government and regulators viewing the attacked as the victim. With this comes increasing exposure to the risk that regulators will take enforcement action against businesses that fail to take adequate steps to prevent cyber-attacks and data breaches.
- These trends are likely to continue. Businesses should keep an eye on overseas developments to remain ahead of the curve.
- Enforcement action can lead to significant penalties and reputational harm. To minimise the risk of regulatory enforcement action, businesses must be proactive in complying with their cyber security obligations.

WHO REGULATES CYBER SECURITY?

The regulatory landscape is congested, with varied obligations that are relevant to cyber security incidents administered by a patchwork of regulators

Australia does not have a unified regulatory framework for managing cyber risks or cyber security incidents.

Instead, cyber security regulations are divided among a mix of sector and/or conduct specific obligations.

SEM217509---OPTION-2-INFOGRAPHIC-V3.JPG

Set out below are Australia's key regulators in the cyber security area, and the conduct they regulate.

ALL BUSINESSES

AUSTRALIAN COMPETITION AND CONSUMER COMMISSION (ACCC)

- The ACCC can take enforcement action against businesses for engaging in misleading or deceptive conduct towards consumers (s 18, Australian Consumer Law (**ACL**)).
- In the cyber security context, businesses must ensure that any representations they make about the collection of consumer data and/or the cyber security characteristics of their products are accurate (s 29, 33-34, ACL)

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC)[1]

- ASIC can take enforcement action against companies and directors if they breach their obligations under the *Corporations Act 2001* (Cth).
- ASIC may commence proceedings against AFSL holders if they fail to put in place systems to prevent, detect and respond to cyber security incidents (s 912A, Corporations Act)
- ASIC may also take enforcement action where companies fail to comply with their continuous disclosure obligations, for example by failing to disclose cyber-attacks or data breaches (s 674, Corporations Act).

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC)

- Organisations and agencies covered by the *Privacy Act 1988* (Cth) must notify the OAIC and affected persons of any loss or unauthorised disclosure of personal information that is likely to result in serious harm (Privacy Act 1988 (Cth) pt IIIC).
- The Government has recently released an exposure draft of the Online Privacy Code,

which will apply to social media organisations, data brokerage organisations, and large online platforms. The current proposal includes obligations to cease using or disclosing personal information on request, and greater protections for children and vulnerable groups. Submissions on the Online Privacy Bill are due by 6 December 2021.[2]

AFP, DFAT, CDPP

- Paying ransoms to hackers may breach a number of criminal laws if which may lead to investigation by the AFP and / or DFAT and possible prosecution.[3]

AUSTRALIAN CYBER SECURITY CENTRE (ACSC)

- The ACSC's voluntary guidelines represent best practice for complying with Australian cyber security standards.
- Further, a bill has been introduced earlier this year in June which would require public and private entities (other than small businesses) to report any ransomware payments to the ACSC.[4]

CRITICAL INFRASTRUCTURE

DEPARTMENT OF HOME AFFAIRS

- Operators of key national services may be given additional reporting and security requirements under proposed amendments to critical infrastructure laws.[5]

FINANCIAL SERVICES

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (APRA)

- APRA-regulated entities must comply with prudential standard CPS 234, which requires entities to clearly define IT security related roles and responsibilities, and maintain information security capability which is commensurate with the size and extent of threats to its IT assets, and maintain a compliant IT policy.
- APRA-regulated entities are also obliged to notify APRA of information security incidents and weaknesses shortly after becoming aware of them.

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC)

- ASIC can take enforcement action against companies and directors if they breach their obligations under the *Corporations Act 2001* (Cth).
- ASIC may commence proceedings against AFSL holders if they fail to put in place systems to prevent, detect and respond to cyber security incidents (s 912A, Corporations Act)
- ASIC may also take enforcement action where companies fail to comply with their continuous disclosure obligations, for example by failing to disclose cyber-attacks or data breaches (s 674, Corporations Act).

LISTED ENTITIES

AUSTRALIAN SECURITIES EXCHANGE (ASX)

- ASX listed entities must comply with their continuous disclosure obligations, by disclosing information that could materially affect the value of that company's securities. This could relevantly include, for example, cyber-attacks or data breaches (ASX Listing Rule 3.1).

RECENT REGULATORY TRENDS

The number and scope of cyber security regulations is increasing

While there are already a significant number of regulations for Australian businesses to consider in the context of cyber security, the Commonwealth Government is considering further cyber specific regulations which are likely to increase the regulatory burden on Australian businesses.

This includes:

Cyber Security Strategy 2020: As we have previously noted, the Commonwealth Government is continuing its work on its Cyber Security Strategy 2020, through which it is considering introducing stronger cyber security regulations to make Australia more resilient to cyber security threats. This includes consideration of mandatory governance standards for large business, cyber security codes, mandatory standards for smart devices and standards requiring manufacturers and suppliers to disclose software vulnerabilities.

Critical infrastructure reforms

As we have previously discussed (see our briefings here and here), the Government is also in the process of amending the *Security of Critical Infrastructure Act 2018*.[6] Under the proposed amendments, owners of key infrastructure assets will be required to:

- notify the Government of imminent cyber security incidents as soon as possible after becoming aware of them; and

- in the case of a serious incident, comply with an expansive range of directions given by the Minister for Home Affairs.

These powers will apply to a broader class of critical infrastructure, affecting assets in the aviation, banking, financial markets, food and groceries and telecommunications sectors.

Privacy Act

The Government's review of the Privacy Act has led to a number of significant proposed reforms to privacy legislation, as outlined in an exposure draft[7] and discussion paper,[8] which are both currently open for submissions (see our briefing here). Some of these proposals would increase penalties for breaches under the Privacy Act. They would also increase the likelihood of enforcement action by the OAIC, as well as private individuals (including class actions arising from new direct rights of action or statutory torts).

Regulators are considering investigation and enforcement action following cyber incidents

Businesses that fail to understand their cyber security obligations are increasingly at risk of regulatory action. We are seeing a shift away from government and regulators viewing the attacked as the victim.

Regulators have taken enforcement action against businesses for cyber security-related breaches, including by commencing court proceedings and imposing fines. For example:

- **ASIC** commenced its first action alleging deficiencies in cyber security practices in the Federal Court of Australia against RI Advice, a financial services company. ASIC has alleged that RI Advice failed to take reasonable steps to manage a series of cyber security incidents, and breached s912A of the Corporations Act as a financial services licensee (see our briefing here).

- The **ACCC** commenced proceedings against an online health booking platform that disclosed personal information to insurance brokers without consumers' consent, resulting in a $2.9 million fine.[9] Soon after that, the ACCC prosecuted another tech company for misleading consumers about the collection, retention and use of consumers' data.[10] While these actions did not relate to cyber-attacks, they demonstrate that the ACCC is focused on misleading business practices which undermine the ability of consumers to make informed decisions regarding the use and collection of their personal

data. This could extend to the nature of statements made about data security.

- The **OAIC** recently issued a determination against a multi-national company for failing to prevent unauthorised third parties from accessing its customers' personal information in a cyber-attack.

So, what can businesses expect in the future?

FUTURE DIRECTIONS IN ENFORCEMENT

Expect more enforcement action

While it is early days in enforcement of cyber regulations, the regulators are making clear that with the increasing prevalence of cyber-attacks and the centrality of data, cyber security is a regulatory priority. This includes enforcement.

- The **OAIC** has voiced its support for stronger penalties for breaches of the Australian Privacy Principles, particularly for large multinational corporations.[11]

- The **ACCC** is well-positioned to prosecute businesses that misrepresent their cyber security posture to consumers. In 2020, the consumer regulator received a $27 million funding boost to address digital security issues.[12]

- **ASIC** has identified cyber threats and cyber security as a strategic priority for the 2021-2025 period. While ASIC has said it will continue to support improving the cyber resilience of its regulated population in line with the approach of the Government,[13] the ASIC Commissioner has stated that they will litigate when necessary.[14] ASIC intends to employ 'decisive, deterrence-based enforcement action' in order to mitigate cyber risks and maintain the integrity of the financial market.[15]

- **APRA** has said that it will take a 'much more targeted approach to ensuring CPS 234 is being fully complied with, and holding boards and management accountable where it is not'.[16]

Expect Australia to follow overseas trends

An increased focus on the enforcement of cyber security obligations is not a uniquely Australian experience. Rather, the Government has made clear that it is looking overseas in its assessment of Australia's cyber security strategy.[17]

It is therefore possible that Australia will see some of the following overseas cyber trends:

- **Actions taken in relation to consumer harm**: Enforcement action has been taken against companies that have misled users about a product's level of security,[18] and those providing services with security flaws.[19]
- **Model cyber security regulation:** The cyber security code being considered by the Government may be modelled on overseas examples. In Europe, for example, the General Data Protection Regulation imposes security requirements for data processing which must include technical and organisational measures appropriate to the risk involved if the data were to be accessed by unauthorised third parties.[20]
- **Focus on cyber ransoms**: In addition to 31 other countries, Australia has agreed to focus attention on cyber ransoms by increasing domestic law enforcement measures and sharing information with overseas regulators.[21]

Businesses can remain ahead of the curve by keeping an eye on comparable overseas regulators and enforcement action being taken.

What are some things that you can do to avoid being the target of enforcement action?

HOW TO MINIMISE THE RISK OF REGULATORY ENFORCEMENT ACTION

Know your legal obligations

Recent trends in regulatory enforcement send a clear message: non-compliance has consequences. However, with the ever-increasing number of regulations, it is difficult for businesses to know their obligations.

Businesses should pay attention to the state of play in this rapidly changing field, and proactively seek advice from legal advisors and other experts if they are unsure about their obligations.

Understand best practice

Against a backdrop of increasingly demanding regulation, it is fundamentally important that businesses understand best practice for IT security. However, this is not easy.

For example, in the RI Advice case, ASIC's case was that RI Advice had to have all 68 documents that ASIC pleaded to be the baseline Cybersecurity Documentation and Controls necessary to adequately manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network. RI Advice put on a strike out application in relation to this pleading, which was dismissed. While substantive consideration of ASIC's case by the court is ongoing, it is clearly a complicated matrix for companies to have regard to, especially in circumstances where ASIC confirmed that it did not allege that the minimum cybersecurity requirements were mandated by any particular laws, regulations or industry standards.[22]

Take steps to minimise cyber risk and maximise operational resilience

Given the risk of enforcement action, businesses must be proactive in preventing, detecting and managing cyber security risks. Cyber security is no longer just an issue for the IT department. Regulators have made clear that directors need to understand management's view of cyber risks; the potential likelihood and impacts of risk events; and the steps taken to address the risks.[23] Failure to do so could lead to significant enforcement actions in the event of a cyber-attack.

WHAT NEXT?

Keep an eye out for our next article in this series which will look at the increased risk of cyber class actions.

RELATED INSIGHTS

Visit our Cyber in Australia page

1. Certain obligations are sector specific.
2. https://www.herbertsmithfreehills.com/latest-thinking/online-privacy-bill-and-privacy-act-discussion-paper-stricter-enforcement-online
3. https://www.herbertsmithfreehills.com/latest-thinking/cyber-ransoms-are-on-the-rise-what-do-you-need-to-know
4. https://www.herbertsmithfreehills.com/latest-thinking/mandatory-notification-of-ransomware-payments-in-australia-appears-likely
5. https://www.herbertsmithfreehills.com/latest-thinking/parliamentary-intelligence-body-backs-two-step-adoption-for-australias-new-critical; https://www.herbertsmithfreehills.com/latest-thinking/securing-australias-critical-infrastructure-government-reforms-will-leave-no-sector
6. *Security Legislation Amendment (Critical Infrastructure) Bill 2021*.
7. Attorney-General's Department, *Online Privacy Bill Exposure Draft* https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.
8. Attorney-General's Department, *Privacy Act Review Discussion Paper* (October 2021) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.
9. https://www.herbertsmithfreehills.com/insight/costs-of-deception-%E2%80%93-big-fine-from-australian-watchdog-shows-need-for-credible-privacy.
10. https://www.herbertsmithfreehills.com/latest-thinking/key-learnings-from-accc-v-google-no-2-for-disclosing-data-practices.
11. Office of the Australian Information Commissioner, *Australia's 2020 Cyber Security*

Strategy: A call for views – submission to the Department of Home Affairs (11 November 2019) https://www.oaic.gov.au/engage-with-us/submissions/australias-2020-cyber-security-strategy-a-call-for-views-submission-to-the-department-of-home-affairs [41].

12. Australian Government, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (12 December 2019) https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf 8.

13. *ASIC Corporate Plan 2021-25: Focus 2021-22* 8 https://download.asic.gov.au/media/qzcaljce/asic-corporate-plan-2021-25-focus-2021-22-published-26-august-2021.pdf.

14. Sean Hughes, *Conversation with ASIC: AFIA Risk Summit* (16 February 2021) https://asic.gov.au/about-asic/news-centre/speeches/conversation-with-asic-afia-risk-summit/.

15. Karen Chester, *Speech at the Australian Institutional Investor Roundtable* (22 April 2021) https://asic.gov.au/about-asic/news-centre/speeches/australian-institutional-investor-roundtable/.

16. Australian Prudential Regulation Authority, *Executive Board Member Geoff Summerhayes – speech to Financial Services Assurance Forum* (26 November 2020) https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services.

17. Australian Government, *Strengthening Australia's cyber security regulations and incentives* (13 July 2021) https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf.

18. Federal Trade Commission, *FTC Requires Zoom to Enhance its Security Practices as Part of Settlement* (9 November 2020) https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.

19. Federal Trade Commission, *ASUS settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk* (23 February 2016) https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

20. *General Data Protection Regulation* art 32.

21. Melissa Coade, 'Australia signs up to White House counter ransomware agenda', *The Mandarin* (18 October 2021) https://www.themandarin.com.au/172322-australia-signs-up-to-white-house-counter-ransomware-agenda/.

22. Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2021] FCA 1193, [72], [75], [111].

23. Sean Hughes, *Conversation with ASIC: AFIA Risk Summit* (16 February 2021) https://asic.gov.au/about-asic/news-centre/speeches/conversation-with-asic-afia-risk-summit/.; Australian Prudential Regulation Authority, *Executive Board Member Geoff Summerhayes – speech to Financial Services Assurance Forum* (26 November 2020) https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services.

KEY CONTACTS

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

TANIA GRAY
PARTNER, SYDNEY

+61 2 9322 4733
Tania.Gray@hsf.com

CHRISTINE WONG
PARTNER, SYDNEY

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

PETER JONES
PARTNER, SYDNEY

+61 2 9225 5588
peter.jones@hsf.com

LEGAL NOTICE