elevenM

Office of the Australian Information Commissioner

Direct Right of Action for Privacy

Research Memo

14 July 2020

Contents

Executive summary

Background to the proposed direct right of action

On 4 December 2017, then Treasurer, the Hon Scott Morrison MP, directed the Australian Consumer and Competition Commissioner (**ACCC**) to conduct an inquiry into digital platforms (**DP Inquiry**). The DP Inquiry looked at the effect that digital search engines, social media platforms and other digital content aggregation platforms have on competition in media and advertising services markets. Approximately 18 months later, the ACCC released its final report, making 23 recommendations, of which four related to Australia's privacy regime.

Recommendation 16(e) of the final DP Inquiry report is to amend the *Privacy Act 1988* (Cth) (**Privacy Act**) to introduce a direct right of action for individuals which enables individuals to bring their own actions and class actions against entities bound by the Privacy Act for an interference with their privacy under that Act (**direct right of action**). Specifically, the ACCC recommended that individuals should have a direct right of action in the Federal Court or the Federal Circuit Court to seek compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for the financial and non-financial harm suffered as a result of an infringement of the Privacy Act and the Australian Privacy Principles (**APPs**).

The ACCC considered that allowing individuals to enforce their rights under the Privacy Act is critical to the effectiveness of those rights. Currently, individuals may only seek limited redress under the Privacy Act to seek an injunction for breach of the Privacy Act (s80W Privacy Act) or lodge a complaint with the OAIC (s36 Privacy Act). In the OAIC's submission to the inquiry, it supported the introduction of a direct right of action.

This research memo

We have been asked by the OAIC to deliver a research memo addressing domestic and international regulatory regimes (privacy or otherwise comparable) where individuals may directly take action in court to seek compensation for breaches of the law. In conducting this research, we have been instructed to consider the following issues:

- threshold requirements (e.g. can individuals take action in response to any breach/interference or only serious breaches?)
- procedural considerations (e.g. do individuals first need to complain to the national regulator? Or any other dispute resolution body?)
- elements of the action (e.g. what does an individual need to prove/establish to succeed with the action?)
- remedies (e.g. damages – should they be capped?)
- regulator's role (e.g. does the relevant regulator have the right to join proceedings or appear as a friend of the court?).

We are instructed that analysis, observations, and recommendations arising from the research are out of scope and are expected to be undertaken in future, separately.

Key findings

In Australia, the following regulatory regimes incorporate a direct right of action for consumers to seek compensation through the courts:

- *Competition and Consumer Act 2010* (Cth) (**CC Act**) in relation to restrictive trade practices, contravention of industry codes, excessive payment surcharges, carbon tax price reduction obligation, and the consumer data right;

- *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**), *Corporations Act 2001* (Cth) (**Corps Act**) and *National Consumer Credit Protection Act 2009* (Cth) (**NCCPA**) in relation to unconscionable conduct and consumer protection regarding financial services, compensation orders, best interests obligations and breaches of the NCCPA[1];

- *Australian Human Rights Commission Act 1986* (Cth) (**AHRC Act**) in relation to unlawful discrimination; and

- Australian Financial Complaints Authority (**AFCA**) *Complaint Resolution Scheme Rules* (**CRSR**) in relation to credit, banking, insurance, and superannuation.

The underlying legislation or rules outline the regulator's role. Some regulators have specific rights in relation to the direct right of action. ASIC and the ACCC have rights to intervene in certain proceedings with all the rights, duties and liabilities of a party. Others have a right to assist the court as *amicus curiae*. Both ASIC and the ACCC follow guidelines and defined principles when considering whether to intervene in private proceedings.

In the absence of statutory intervention, there is currently no general right to privacy under Australia's common law. While the High Court has recognised there is no impediment to the Australian courts creating a cause of action for invasion of privacy, this is yet to occur. The lack of reform at common law has led to growing calls for the introduction of a tort of privacy through statute that would give individuals the right to sue for serious invasions of privacy. The introduction of such a tort was one of the key recommendations from the DP Inquiry, in addition to the recommendation for the direct right of action.

There are analogous areas of law which already serve to protect individuals' privacy in certain contexts. These include the law of confidentiality by virtue of a contract or fiduciary relationship. Existing statutory consumer law, specifically the prohibition on misleading and deceptive conduct in the Australian Consumer Law under the *Competition and Consumer Act 2010* (Cth) have also been relied upon to seek remedies for privacy breaches.[2]

---

[1] There is significant overlap in the provisions considered under the Competition and Consumer Act 2010 (Cth), the Australian Securities and Investments Commission Act 2001 (Cth) and the National Consumer Credit Protection Act (Cth) 2009.
[2] See, for example, the *Australian Competition and Consumer Commission v Google Australia Pty Ltd & Anor* filed in the Federal Court of Australia registry on 29 October 2019.

Overseas, the following regimes incorporate a direct right of action for consumers to seek compensation and may provide a useful point of comparison for the OAIC:

- The European Union's General Data Protection Regulation (**GDPR**), the ePrivacy Directive, and the Privacy and Electronic Communications Regulations allow data subjects to bring private rights of action under certain circumstances. European residents can also seek redress via the *Judicial Redress Act of 2015* (USA), which grants private rights of action to citizens against some U.S. government agencies.

- US federal law (including the *Health Insurance Portability and Accountability Act 1996*) does not provide a private right of action that would enable individuals to sue companies directly for privacy intrusions, but several state privacy laws do, for example, state health privacy laws, Illinois's biometric privacy law and the *California Consumer Protection Act 2020* which allows users to sue a company for statutory damages where the data breach is a result of the company's negligence.

- In Japan, data subjects have the right to sue business operators that have collected their personal information unlawfully or processed the data in a way that is not disclosed or approved by the data subject under the *Act on the Protection of Personal Information*.

- In South Korea, the *Personal Information Protection Act 2011* enables private parties to bring lawsuits seeking damages or other civil remedies if there are data breaches or other violations of data privacy law.

- In Singapore, any person who suffers loss or damage directly as a result of a contravention of any of the main data protection provisions under the *Protection of Personal Data Act* may also commence a private civil action for loss or damage.

- The Philippines *Data Privacy Act* provides a private right of action for damages for inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorised use of personal data. Privacy torts also give redress to individuals.

- Under Canadian federal data privacy law, PIPEDA, there is currently no direct statutory right of action for breach of the right to privacy – however, the federal Privacy Commissioner has proposed a direct right of action that would bring Canadian privacy laws closer to the GDPR. A federal scheme would supplement provincial schemes in British Columbia, Manitoba, Newfoundland and Labrador, Ontario and Saskatchewan.

- Similarly, there is currently no direct right of action for individuals in Hong Kong under the *Personal Data Privacy Ordinance* but in January 2020, the Privacy Commissioner and the Hong Kong Government introduced expansions to the PDPO to mirror and in some cases, exceed the GDPR. The changes include a private right of action.

- New Zealand's new Privacy Act 2020 does not create enforceable rights, except for IPP 6 in respect of public sector agencies. However, any individual may make a complaint to the Privacy Commissioner about an interference with privacy and these complaints can ultimately reach the Human Rights Review Tribunal and the courts. The new Act clarifies right to take privacy class actions, by providing for representative cases on behalf of one or more aggrieved individuals.

Part 1: Australian Legal Frameworks

Part 1A: Non-privacy regimes applicable under Commonwealth or harmonized regimes

Division 1: Potentially comparable non-privacy regimes identified

The following regulatory regimes incorporate a direct right of action for consumers to seek compensation through the courts and provide a useful point of comparison for the OAIC. The underlying legislation or rules outline the regulator's role. This varies under the regimes identified, although there is significant overlap in the provisions considered under the *Competition and Consumer Act 2010* (Cth), the *Australian Securities and Investments Commission Act* 2001 (Cth) and the *National Consumer Credit Protection Act* (Cth) 2009.

Some regulators have specific rights in relation to the direct right of action.

Specifically, ASIC and the ACCC have rights to intervene in certain proceedings with all the rights, duties and liabilities of a party[3]. Both ASIC and ACCC have developed guidelines including principles to be considered when deciding whether to intervene.

Similarly, special-purposes Commissioners (as defined under various human rights legislation) have a right to assist the court as *amicus curiae*[4]. An *amicus curiae* is a person who seeks to assist the court and does not involve becoming a party to the proceedings[5]. ASIC may also appear as *amicus curiae* under court rules (e.g. *Federal Court (Corporations) Rules 2000*) or, where applicable, the court's own inherent authority[6]. ASIC states that it is generally more likely to appear as *amicus curiae* than to intervene as a party[7].

While most examples of direct rights of action for consumers relate to financial or other consumer complaints where loss and damage is usually easily quantifiable (i.e.it is financial harm or economic loss), the compensation regime for unlawful discrimination under the *Australian Human Rights Act 1986* (Cth) provides for damages to be awarded for non-economic loss, including hurt, humiliation and distress. In quantifying such awards of damage, the decided cases indicate that awards should be restrained but not minimal, and not so low as to diminish the respect for the public policy of the legislation[8]. Aggravated and exemplary damages have also been awarded in limited unlawful discrimination matters[9].

Australian Competition and Consumer Commission

***Competition and Consumer Act 2010* (Cth) (CC Act)**

Restrictive trade practices, contravention of industry codes, excessive payment surcharges, carbon tax price reduction obligation, consumer data right

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
An individual who suffers loss or damage by conduct of another person that was done in contravention of specified CC Act prohibitions on restrictive trade practices, contravention of industry	An action may be commenced within 6 years after the day on which the cause of action that relates to the conduct accrued[11]. Individuals are not required to complain to the Australian Competition and Consumer Commission (**ACCC**) prior to commencing proceedings. Further, where:	Individuals must prove the defendant has contravened the prohibition on the relevant conduct specified in prohibitions on	Provided the court is satisfied that the individual has suffered loss or damage due to the defendant's contravention of the prohibited conduct, there are no specified caps on the amount the individual may recover in respect of the loss or damage from the defendant in the CC Act.	The ACCC may, with the leave of the Court and subject to any conditions imposed by the court, intervene in any proceeding	A person who brings an action in relation to a contravention of a prohibition on restrictive trade practices may at any time during proceedings seek an order that the applicant is not liable for the costs of any respondent to the proceedings, regardless of the outcome

[3] See, for example, the role of ASIC in respect of unconscionable conduct and consumer protection in relation to financial services under the ASIC Act.
[4] See the role of special-purpose Commissioners under the AHRC Act and related legislation.
[5] ASIC's approach to involvement in court proceedings – see https://asic.gov.au/about-asic/asic-investigations-and-enforcement/asic-s-approach-to-involvement-in-private-court-proceedings/#intervention .
[6] *Ibid.*
[7] *Ibid*.
[8] See Federal Discrimination Law Chapter 7 Damages and Remedies linked here https://humanrights.gov.au/our-work/legal/federal-discrimination-law-chapter-7-damages-and-remedies#7_2_1c .
[9] *Ibid.*
[11] The cause of action accrues when the loss and damage is suffered. See Miller's Australian Competition and Consumer Law Annotated (Westlaw AU) [CCA.82.160] Practice and procedure: time limit – when cause of action accrues.

Australian Competition and Consumer Commission

Competition and Consumer Act 2010 **(Cth) (CC Act)**

Restrictive trade practices, contravention of industry codes, excessive payment surcharges, carbon tax price reduction obligation, consumer data right

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
codes, excessive payment surcharges, carbon tax price reduction obligations; and the consumer data right obligations may recover the amount of the loss or damage by action against that other person or against any person involved in the contravention.[10]	a) criminal or civil penalty proceedings have been commenced and a court considers it is appropriate to make a pecuniary penalty order or impose a fine; and b) it is appropriate to order the defendant to pay compensation to a person who has suffered loss or damage in respect of the contravention or the involvement; and c) the defendant does not have sufficient financial resources to pay both the pecuniary penalty or fine and the compensation, then the court must give preference to making an order for compensation.[12]	restrictive trade practices, contravention of industry codes, excessive payment surcharges, carbon tax price reduction obligations; and the consumer data right.	Proportionate liability also applies to a claim for damages for misleading and deceptive conduct. There is a defence available for defendants other than a body corporate, who has or may have engaged in contravention of prohibitions on restrictive trade practices, carbon tax price exploitation, false or misleading statements about carbon tax repeal or other specified conduct subject to pecuniary penalties but acted honestly and reasonably and, having regard to all the circumstances of the case, ought fairly to be excused. In these circumstances the court may relieve the person either wholly or partly from liability to damages on such terms as the court thinks fit.[13]	instituted under the CC Act. If the ACCC intervenes in a proceeding, the ACCC is taken to be a party to the proceeding and has all the rights, duties and liabilities of such a party.[14]	or likely outcome of the proceedings.[15] This provision appears to have been included for the benefit of consumers who may be deterred by the prospects of an adverse costs order. Many of the CC Act provisions relating to the direct right of action for consumers overlap with the equivalent provisions in the ASIC Act (discussed below).

Australian Securities and Investments Commission

Australian Securities and Investments Commission Act 2001 **(Cth) (ASIC Act),** ***Corporations Act 2001*** **(Cth) (Corps Act) and** ***National Consumer Credit Protection Act*** **(Cth) 2009 (NCCPA)**

Unconscionable conduct and consumer protection in relation to financial services,[16] compensation orders,[17] best interests obligations,[18] breaches of the NCCPA[19]

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
Provided individuals have suffered loss or damage by conduct of another person that contravenes a provision of Subdivision C (unconscionable conduct)[20] or Subdivision D (consumer protection),[21] the	An action may be commenced within 6 years after the day on which the cause of action that relates to the conduct accrued. Individuals are not required to complain to the Australian Securities and Investments Commission (**ASIC**) prior to commencing proceedings. Further, where criminal or civil penalty proceedings have been commenced and a court considers it is	Individuals must prove the defendant has contravened the prohibition on the relevant conduct specified in Subdivision C (unconscionable	Provided the court is satisfied that the individual has suffered loss or damage due to the defendant's contravention of the prohibited conduct, there are no specified caps on the amount the individual may recover in respect of the loss or damage from the defendant under the ASIC Act.	ASIC may, with the leave of the court and subject to any conditions imposed by the Court, intervene in any proceeding instituted under this Division[24]. If ASIC intervenes in a proceeding, it is taken to be a party to the proceeding and has all the	ASIC contends it does not lightly intervene in matters where a case primarily concerns the personal legal rights and remedies available to the parties unless there is a broader regulatory benefit that may be achieved through its intervention.[26]

[10] s82 CC Act,
[12] s79B CC Act.
[13] s85 CC Act
[14] The ACCC will consider intervention in private proceedings under the Act in one or more of the three following circumstances: (i) issues of significant public interest; (ii) construction of the *Trade Practices Act* (now *Competition and Consumer Act*) in untested areas or clarifying its operation; and (iii) international conduct i.e. anti-competitive conduct or consumer exploitation on an international scale. See linked guidelines published on the ACCC website in 2002 and republished in 2013 https://www.accc.gov.au/system/files/ACCC%20Intervention%20in%20Private%20Proceedings.pdf .
[15] s82(3) to (7) CC Act.
[16] Part 2, Division 2 ASIC Act
[17] s1317H, 1317HA, 1317HB, 1317HC, 1317HE Corps Act.
[18] s961M Corps Act
[19] s178 NCPPA.
[20] s12CA to s12CC ASIC Act
[21] s12DA to 12DN ASIC Act
[24] ASIC is guided by the following four general principles when deciding whether to intervene in private proceeding: (i) whether intervention is of strategic regulatory significance; (ii) whether the benefits of intervention outweigh the costs of doing so; (iii) whether issues specific to the case warrant intervention; and (iv) whether alternatives are available, including appearing as amicus curiae or ASIC taking action. See linked Information Sheet 180 https://asic.gov.au/about-asic/asic-investigations-and-enforcement/asic-s-approach-to-involvement-in-private-court-proceedings/#decision
[26] ASIC – Investigations and enforcement – approach to involvement in private court proceedings - see https://asic.gov.au/about-asic/asic-investigations-and-enforcement/asic-s-approach-to-involvement-in-private-court-proceedings/#intervention

Australian Securities and Investments Commission

Australian Securities and Investments Commission Act 2001 **(Cth) (ASIC Act),** ***Corporations Act 2001*** **(Cth) (Corps Act) and** ***National Consumer Credit Protection Act*** **(Cth) 2009 (NCCPA)**

Unconscionable conduct and consumer protection in relation to financial services,[16] compensation orders,[17] best interests obligations,[18] breaches of the NCCPA[19]

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
individual may recover the amount of the loss or damage by action against that other person or against any person involved in the contravention.	appropriate to make a pecuniary penalty order, a relinquishment order or impose a fine, the court must consider the effect that making the order or imposing the fine would have on the amount available to pay compensation to persons who might reasonably be expected to be entitled to recover compensation for loss or damage suffered as a result of the contravention; and give preference to making an appropriate amount available for compensation.[22]	conduct) or Subdivision D (consumer protection).	However, in respect of actions for misleading and deceptive conduct where an individual has contributed to the loss and there is an absence of intent on the part of the defendant, the damages that the claimant may recover in relation to the loss or damage are to be reduced to the extent to which the court thinks just and equitable having regard to the claimant's share in the responsibility for the loss or damage.[23] Further, proportionate liability also applies to a claim for damages for misleading and deceptive conduct.	rights, duties and liabilities of such a party.[25]	While we have focused on consumer direct rights of action, ASIC may intervene in a variety of court proceedings, provided the proceedings 'relate to a matter arising under' the Corps Act or the NCCPA. For example, a matter arising under different legislation or the general law, but which has implications for the interpretation or administration of the Corps Act or NCCPA may 'relate to a matter arising under' those Acts.

Australian Human Rights Commission

Australian Human Rights Commission Act 1986 **(Cth) (AHRC Act)**

Redress for unlawful discrimination

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
An aggrieved individual must first lodge a complaint with the Australian Human Rights Commission (**AHRC**) setting out the acts, omissions or practices giving rise to alleged unlawful discrimination.[27] If the complaint is terminated by the President of the AHRC[28] then an individual who was an affected person in relation to the complaint may apply to the Federal Court or Federal Circuit Court (**the Court**) alleging unlawful discrimination on the part of one or more of the respondents to the terminated complaint.[29] The application must not be made unless:	The application to the court must be made within 60 days of the date of issue of the notice of termination of the complaint,[33] or within such further time as the Court allows.[34]	The Court must be satisfied that "unlawful discrimination" has occurred. "Unlawful discrimination" is defined to mean any acts, omissions or practices that are unlawful under: (a) Part 4 of the Age Discrimination Act 2004; or (b) Part 2 of the Disability Discrimination Act 1992; or (c) Part II or IIA of the Racial Discrimination Act 1975; or (d) Part II of the Sex Discrimination Act 1984, and includes any conduct that is an offence under: (a) Division 2 of Part 5 of the Age Discrimination Act 2004 (other than section 52); or (b) Division 4 of Part 2 of the Disability Discrimination Act 1992; or	Provided the court is satisfied that "unlawful discrimination" has occurred, the court may make such orders (including a declaration of right) as it thinks fit including an order requiring a respondent to pay to an applicant damages by way of compensation for any loss or damage suffered[36] because of	"Special-purpose Commissioners" (defined to include the Aboriginal and Torres Strait Islander Social Justice Commissioner, the Disability Discrimination Commissioner, the Human Rights Commissioner, the Race Discrimination Commissioner, the Sex Discrimination Commissioner, the Age Discrimination Commissioner and the National Children's Commissioner) have the function of assisting the court, as amicus curiae, in the following proceedings:[38] (a) proceedings in which the special-purpose Commissioner thinks that the orders sought, or likely to be sought, may affect to a significant extent the human rights of persons who are not parties to the proceedings; (b) proceedings that, in the opinion of the special-purpose Commissioner, have significant implications for the administration of the relevant Act or Acts;	The AHRC may help an individual to prepare the forms for an application.[42]

[22] s12GCA ASIC Act.
[23] s12GF(1B) ASIC Act.
[25] s12GO ASIC Act.
[27] s46P AHRC Act, read with s46PO AHRC Act.
[28] Pursuant to s46PO AHRC Act.
[29] s46PO(1) AHRC Act.
[33] Under s46PH(2).
[34] s46PO(2).
[36] Damages may be awarded for hurt, humiliation and distress. Awards should be restrained in quantum, but not minimal. For further guidance and examples of awards see Federal Discrimination Law Chapter 7 Damages and Remedies linked here https://humanrights.gov.au/our-work/legal/federal-discrimination-law-chapter-7-damages-and-remedies#7_2_1c
[38] Under Part IIB Division 2 of the AHRC Act.
[42] s46PT AHRC Act, for applications under Part IIB Division 2.

Australian Human Rights Commission

***Australian Human Rights Commission Act 1986* (Cth) (AHRC Act)**

Redress for unlawful discrimination

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
(a) the President of the Commission is satisfied that the subject matter of the complaint involves an issue of public importance that should be considered by the courts;[30] or (b) there is no reasonable prospect of the complaint being settled by conciliation;[31] or (c) the Court gives leave.[32]		(c) subsection 27(2) of the Racial Discrimination Act 1975; or (d) section 94 of the Sex Discrimination Act 1984. The unlawful discrimination alleged in the application to the Court: (a) must be the same as (or the same in substance as) the unlawful discrimination that was the subject of the terminated complaint; or (b) must arise out of the same (or substantially the same) acts, omissions or practices that were the subject of the terminated complaint.[35]	the conduct of the respondent.[37] No cap on compensation is specified.	(c) proceedings that involve special circumstances that satisfy the special-purpose Commissioner that it would be in the public interest for the special-purpose Commissioner to assist the court concerned as amicus curiae.[39] The President of the AHRC may provide the court with a written report on a complaint that has been terminated,[40] but the report must not set out or describe anything said or done in the conciliation process.[41]	

[30] s46PH(h) AHRC Act.
[31] s46PH(1B)(b) AHRC Act, read with s46PO(3A).
[32] s46PO(3A)(a) AHRC Act, read with s46PO(3A).
[35] s46PO(3).
[37] s46PO4(d) AHRC Act.
[39] s46 PV AHRC Act
[40] Under paragraph 46PF(1)(b) or section 46PH.
[41] s46PS AHRC Act.

Australian Financial Complaints Authority

Complaint Resolution Scheme Rules (CRSR) - Credit, Banking, Insurance and Superannuation

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
A complaint must be made by an Eligible Person[43] about a Financial Firm[44] that is a member of the Australian Financial Complaints Authority (**AFCA**), including its employees and agents.[45] There are some additional threshold requirements that must be met for AFCA to consider a complaint. In summary: (a) the complaint must arise from a customer relationship or other circumstance that brings the complaint within AFCA's jurisdiction. (b) there must be a sufficient connection with Australia. (c) generally, there is a time limit within which the complaint must be submitted to AFCA. (d) if the complaint is about a Traditional Trustee Company Service that involve Other Affected Parties, the Complainant must get the consent of all Other Affected Parties.[46]	There must be a sufficient connection to Australia.[47] Varying time limits apply to complaints, depending on the type of complaint. For superannuation complaints: (a) relating to the payment of a disability benefit because of total and permanent disability: i. if the Complainant has permanently ceased employment, it must have made a claim to the Financial Firm for the payment of a disability benefit within two years of permanently ceasing employment and the Complainant must have submitted the complaint to AFCA within four years of the Financial Firm's decision about the disability claim. ii. if the Complainant has not permanently ceased employment, the Complainant must have submitted the complaint to AFCA within six years of the Financial Firm's decision about the disability claim. (b) relating to death benefits, the Complainant must have objected to the payment of the death benefit proposed by the Financial Firm within 28 days of being given notice of the proposed decision; and submitted the complaint to AFCA within 28 days of being given a notice from the Financial Firm of its decision in relation to the payment of the death benefit.[48] (c) about a statement given to the Commissioner for Taxation,[49] the complaint to AFCA must have been submitted within 12 months of notice being given by the Financial Firm of the time period to complain with a copy of the statement. (d) AFCA will generally not consider other types of Superannuation Complaint unless it was submitted to AFCA within two years of the date of the IDR Response.[50] Where a complaint relates to a variation of a credit contract as a result of financial hardship, an unjust transaction or unconscionable interest and other charges under the National Credit Code, AFCA will generally not consider the complaint unless it was submitted to AFCA before the later of the following time limits: 1. within two years of the date when the credit contract is rescinded, discharged or otherwise comes to an end; or	Provided the threshold requirements are met and no exclusions apply, AFCA has jurisdiction to resolve complaints.	An AFCA Decision Maker has the power to take a range of remedial actions including making an award of compensation. In the case of a Superannuation Complaint, there is no monetary limit on the amount that may be awarded to the Complainant.[55] For most other complaints, a limit per claim applies.[56]	AFCA is the dispute resolution scheme for financial services, including entities regulated by the Australian Prudential Regulation Authority (APRA). AFCA considers complaints about: (a) credit, finance and loans (b) insurance (c) banking deposits and payments (d) investments and financial advice (e) superannuation.	The provisions in relation to threshold issues, time limits and remedial actions (including caps on compensation awards) are complicated and inconsistent. A possible explanation is that AFCA considers complaints that previously would have been handled by the Financial Ombudsman Service, the Credit and Investments Ombudsman and the Superannuation Complaints Tribunal.

[43] Defined in clause E1.1.of the Complaint Resolution Scheme Rules (CRSR) to mean: a) an individual or individuals (including those acting as a trustee, legal personal representative or otherwise); b) a partnership comprising of individuals – if it carries on a business, the business must be a Small Business; c) the corporate trustee of a Self-Managed Superannuation Fund or a family trust – if it carries on a business, the business must be a Small Business; d) a Small Business (whether a sole trader or constituted as a company, partnership, trust or otherwise); e) a not-for-profit organisation or club – if it carries on a business, the business must be a Small Business unless the not-for-profit organisation or club is also a charity registered with the Australian Charities and Not-for-profits Commission; f) a body corporate of a strata title or company title building which is wholly occupied for residential or Small Business purposes; or g) the policy holder of a group life or group general insurance policy, where the complaint relates to the payment of benefits under that policy.
[44] Defined in clause E1.1 of the CRSR to mean an AFCA Member. Special extended definitions of "Financial Firm" also apply for the purpose of a Superannuation Complaint, a complaint relating to a Traditional Trustee Company Service. "Financial Firm" also includes any employee, representative, agent or contractor of the Financial Firm including any person who has actual, ostensible, apparent or usual authority to act on behalf of the Financial Firm or authority to act by necessity in relation to a financial service.
[45] Specifically, complaints about a decision of a trustee of a Regulated Superannuation Fund or an Approved Deposit Fund, an RSA Provider, or an insurer (where the premiums under the policy have been paid from an RSA.
[46] Clause A.4.3 CRSR. See also clause B1 in relation to superannuation, clause B2 in relation to other complaints.
[47] Clause B.3
[48] Clause B.4.1.3 CRSR.
[49] Referred to in section 1053(2) of the *Corporations Act 2001* (Cth).
[50] B.4.1 CRSR.
[55] Section D explanatory note and clause D.1.3.CRSR.
[56] See table in clause D.4 of the CRSR.

Australian Financial Complaints Authority **Complaint Resolution Scheme Rules (CRSR) - Credit, Banking, Insurance and Superannuation**					
Threshold requirements	**Procedural considerations**	**Elements of the action**	**Remedies**	**Regulator's role**	**Comments**
	2. where, prior to lodging the complaint with AFCA, the Complainant was given an IDR Response[51] in relation to the Complaint from the Financial Firm - within two years of the date of that IDR Response.[52] In other situations, AFCA will generally not consider a complaint unless it was submitted to AFCA before the earlier of the following time limits: (a) within six years of the date when the Complainant first became aware (or should reasonably have become aware) that they suffered the loss; and (b) where, prior to submitting the complaint to AFCA, the Complainant was given an IDR Response in relation to the complaint from the Financial Firm - within two years of the date of that IDR Response.[53] Extensions may be available in limited complaints where special circumstances apply.[54]				

[51] Internal Dispute Resolution Response
[52] B.4.2.1 CRSR
[53] Clause B4.3.1 CRSR
[54] Clause B.4.4 CRSR

Division 2: Other non-privacy regimes identified and considered

The remaining non-privacy regimes identified in the scope of work were considered as part of this engagement, but ultimately determined **not to provide a useful point of comparison** for the OAIC. These regimes generally did not include a direct right of action for consumers. Some regimes required consumers to apply for compensation through the regimes identified in Division 1 above (for example, APRA-regulated entities are required to seek compensation through the AFCA). Other regimes were determined to be either broadly equivalent to the OAIC's existing powers or not comparable to the OAIC's regime. We have, in any event, summarised these regimes in the table below for completeness and further context for the OAIC's consideration of frameworks.

Australian Communications and Media Authority

Broadcasting and Telecommunications

Source of regulatory powers	Permitted enforcement action	Engagement with consumers	Comments
The Australian Communications and Media Authority (**ACMA**) has regulatory powers over broadcasting (including radio and television) and telecommunications. ACMA can investigate activities under the *Australian Communication and Media Authority Act 2005 (Cth),* the *Radiocommunications Act 1992 (Cth),* the *Broadcasting Services Act 1992 (Cth),* the *Telecommunications Act 1997 (Cth)* and the *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth),* the *Spam Act 2003 (Cth),* the *Do Not Call Register Act 2009 (Cth)* and the *Interactive Gambling Act 2001 (Cth).*[57]	The enforcement powers that may be exercised by ACMA against broadcasting, telecommunications and other regulated entities comprise: (a) issuing an informal warning with compliance guidance; (b) issuing a formal warning; (c) issuing an infringement notice; (d) issuing a remedial direction with compliance guidance; (e) accepting court-enforceable undertakings; and (f) applying to the Federal Court for civil penalty orders or injunctions.[58]	Receiving, investigating and enforcing complaints. Providing guidance and recommendations.	ACMA's powers are similar to the OAIC's existing powers. There is no direct right of action for consumers.

Australian Building and Construction Commission

Building and Construction Industry

Source of regulatory powers	Permitted enforcement action	Engagement with consumers	Comments
The Australian Building and Construction Commission (**ABCC**) is an Australian Government agency responsible for ensuring that building work in Australia is carried out fairly, efficiently and productively. It is established under the *Building and Construction Industry (Improving Productivity) Act 2016* (Cth)[59] (**BCIIP Act**). The ABCC is led by the Australian Building and Construction Commissioner (the Commissioner). The Commissioner has powers and functions under legislation to help promote better workplace relations for building work and to ensure that building work is carried out fairly, efficiently and productively.	The Commissioner's functions include education and advice, investigation and enforcement. The ABCC monitors compliance with, and enforces the workplace relations laws that apply to, the building and construction industry. Its jurisdiction covers those who are, by statutory definition, a 'building industry participant': someone who is involved with 'building work'. 'Building industry participant' and 'building work' are terms defined by the BCIIP Act.	The ABCC does not have the power to order a wrongdoer to pay compensation. If ABCC investigates a complaint and the matter goes to court, it can seek penalties against the wrongdoer, but the court decides on penalties to be paid or other orders the wrongdoer must follow. These other orders can include paying compensation. Disputes in the building and construction industry sometimes result in private court action between one or more parties. Where the matter involves 'building industry participants' or 'building work', the Commissioner has a right to intervene in court proceedings, and to make submissions in proceedings before the Fair Work Commission. The Commissioner will intervene where there is public interest in doing so and will use the power to intervene as one means of achieving improved standards of conduct in the building and construction industry.	The powers to intervene in court proceedings may be of interest.

[57] ACMA: The legislation we enforce https://www.acma.gov.au/our-role-compliance-and-enforcement and Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era (DP80)' (27 March 2014) Chapter 15, New Regulatory Mechanisms.
[58] ACMA: Taking the right regulatory action https://www.acma.gov.au/our-role-compliance-and-enforcement.
[59] Chapter 2, BCIIP Act.

Part 1B: Privacy relief under common law and other legal principles

In the absence of statutory intervention, there is currently no general right to privacy under Australia's common law. While the High Court has recognised there is no impediment to the Australian courts creating a cause of action for invasions of privacy, this is yet to occur.

The lack of reform at common law has led to growing calls for the introduction of a tort of privacy through statute that would give individuals the right to sue for serious invasions of privacy. The Australian Law Reform Commission first recommended the creation of a tort for invasion of privacy in 2008, and again in 2014. It was also a recommendation in the DP Inquiry Final Report in 2019. The calls for reform in Australia are largely in response to the (potentially) highly invasive nature of modern technology and modern media practices, meaning the private information of individuals is more vulnerable than ever before.

There are analogous areas of law which already serve to protect individuals' privacy in certain contexts. These include the law of confidentiality, which applies in circumstances where it is expected that a duty of confidence would apply. For example, a duty of confidentiality is owed by a lawyer to their client, by a doctor to their patient, and by an employee to their employer. Individuals' rights have also been protected through general protections against property searches and seizures. Alternatively, a duty of confidentiality may arise as a matter of contract law through the incorporation of confidentiality clauses into a consumer agreement.

Existing statutory consumer law, specifically the prohibition on misleading and deceptive conduct in the Australian Consumer Law under the *Competition and Consumer Act 2010* (Cth) have also been relied upon to seek remedies for privacy breaches.[60]

[60] See, for example, the *Australian Competition and Consumer Commission v Google Australia Pty Ltd & Anor* filed in the Federal Court of Australia registry on 29 October 2019.

Part 2: Foreign Jurisdictions

European Union

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
The GDPR, the ePrivacy Directive, and the Privacy and Electronic Communications Regulations allow data subjects to bring private rights of action under certain circumstances[61]. These circumstances include the ability to prove that substantial harm[62] has occurred because of privacy violations. Action must be commenced within two years of discovery of the violation.	Data subjects are required to report potential violations to their National Data Protection Authority who will then decide whether to investigate. If the DPA chooses not to investigate, the data subject can file a complaint with the court of competent jurisdiction.	Individuals have the right to an effective judicial remedy (i.e. to pursue a lawsuit) against the responsible data processor or controller, and individuals may obtain compensation for their damages from data processors or controllers if the National DPA does not take action.	Any private action based on failure to comply is limited to compensation for the damages suffered, since administrative fines (including fines based on percentages of revenue under the GDPR) may only be sought by supervisory authorities	The National DPA has responsibility for investigating the initial complaint. If the data subject is not satisfied, a complaint can be filed with the local court of competent jurisdiction. The Regulator normally does not get involved in private rights of action but rather focuses on sanctions against organisations. However, the National DPA can intervene or appear as amicus curiae if the complaint was filed within its jurisdiction or the violation has the potential to impact its jurisdiction[63].	There is some debate about whether certain Member State's national systems require the enactment of domestic legislation to officially create or grant the ability of a private individual to enforce the GDPR within the national court system. Currently, Germany, Ireland, Italy, Netherlands, and Spain have proposed private rights of actions for violation of national data protection laws. Decisions are expected at the end of 2020. Prescribed defences under the GDPR include: • A legally binding and enforceable instrument between public authorities. • Binding Corporate Rules (BCRs) • Standard contractual clauses adopted by the local regulatory authority. • Standard contractual clauses adopted by a Supervisory Authority and approved by the local regulatory authority. • An approved code of conduct • An approved certification mechanism The OAIC has asked specifically about whether the UK's Data Protection Act 2018 creates a private right of action that could be enforced? The Act does not address a private right of action, however, there have been cases where class action suits have been filed on behalf of various plaintiffs.
EU residents have been granted rights of judicial redress under the U.S. Judicial Redress Act of 2015 that grants private rights of action to citizens of certain foreign countries or regional economic organisations (covered countries) against U.S. government agencies but not private companies. The individual must prove that harm has occurred because of the unauthorised disclosure of personal data or the inability to obtain access to personal data.	The Judicial Redress Act enables a covered person to bring suit in the event of 1) intentional or wilful unlawful disclosure of a personal data and 2) improper refusal to grant access to or amendment of the individual's personal data.	Under the Judicial Redress Act, the private right of action may only be brought against a designated Federal agency or component. Under the Judicial Redress Act, a "covered person" means a natural person who is a citizen of a covered country. The covered person must prove that harm occurred because of unauthorised disclosure of personal data or the inability to access the personal data.	Remedies are determined based on the extent of harm and whether remediation was attempted.	The U.S. Department of Justice under the direction of the U.S. Attorney General is responsible for enforcing the Redress Act and evaluating complaints.	The following regional economic integration organisation and countries have each been designated by the Attorney General as a covered country: 1. European Union; 2. Austria; 3. Belgium; 4. Bulgaria; 5. Croatia; 6. Republic of Cyprus; 7. Czech Republic; 8. Estonia; 9. Finland; 10. France; 11. Germany; 12. Greece; 13. Hungary; 14. Ireland; 15. Italy; 16. Latvia; 17. Lithuania; 18. Luxembourg; 19. Malta; 20. Netherlands; 21. Poland; 22. Portugal; 23. Romania; 24. Slovakia; 25. Slovenia; 26. Spain; 27. Sweden; and 28. United Kingdom. The following components of a Federal agency have each been designated by the Attorney General as a designated Federal agency or component: 1. United States Department of Justice;

[61] The three regimes don't directly interact, although they all deal with privacy issues. The GDPR deals with the processing of any personal data. The ePrivacy Directive deals with mandatory consents for the use of cookies. The Privacy and Electronic Communications Regulation specifically relates to direct marketing, traffic monitoring, and location data. The GDPR touches each of them so a data subject can file a complaint under the GDPR or if specifically related to the use of cookies or marketing can file a complaint under the specific law.
[62] Substantial harm has not been clearly articulated however, this is commonly interpreted as physical harm, mental or emotional harm, identify theft, financial harm, abuse or discrimination.
[63] For example, the French DPA (CNIL) took action against Facebook even though Google's European headquarters is in Ireland. Since the DPA in Ireland was not taking action, CNIL stepped in.

European Union					
Threshold requirements	**Procedural considerations**	**Elements of the action**	**Remedies**	**Regulator's role**	**Comments**
					2. United States Department of Homeland Security; 3. United States Securities and Exchange Commission; and 4. United States Commodity Futures Trading Commission. 5. Bureau of Diplomatic Security, United States Department of State; 6. Office of the Inspector General, United States Department of State; 7. Alcohol and Tobacco Tax and Trade Bureau, United States Department of the Treasury; 8. Financial Crimes Enforcement Network, United States Department of the Treasury; 9. Internal Revenue Service, Division of Criminal Investigation, United States Department of the Treasury; 10. Office of Foreign Assets Control, United States Department of the Treasury; 11. Office of the Inspector General, United States Department of the Treasury; 12. Office of the Treasury Inspector General for Tax Administration, United States Department of the Treasury; and 13. Special Inspector General for the Troubled Asset Relief Program, United States Department of the Treasury.

Canada

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
The Canadian federal data privacy law, PIPEDA, does not provide for a direct statutory right of action for breach of the right to privacy. However, the Privacy Commissioner has proposed the need for one. Please see the comments section. Five of the ten Canadian provinces have adopted statutes which have created the tort of invasion of privacy: British Columbia, Manitoba, Newfoundland and Labrador, Ontario and Saskatchewan. In these five provinces, an individual has a valid cause of action against any person who violates his or her right to privacy even if no substantial harm can be proven. Except for Manitoba's, these statutes require proof that the defendant acted wilfully and without a claim of right. Action must be commenced within three years of discovery of the violation.	Under PIPEDA, an individual first needs to file a complaint with its Provincial Privacy Commissioner. The Commissioner will then review the complaint, conduct an inquiry, and make an order. It is only when the order rendered by the Commissioner has become final, as a result of there being no further right of appeal, that the individual affected by the order has a cause of action against the organisation for damages.	Under the privacy laws in British Columbia, Manitoba, Newfoundland and Labrador, Ontario, and Saskatchewan, the plaintiff needs to demonstrate one of the following: 1. Intrusion upon the plaintiff's seclusion or solitude into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness In awarding damages in an action for a violation of privacy of a person, the court can consider all circumstances of the case including: 1. The nature, incidence and occasion of the act, conduct or publication constituting the violation of privacy of that person; 2. The effect of the violation of privacy on the health, welfare, social, business or financial position of that person or his family; 3. Any relationship, whether domestic or otherwise, between the parties to the action; 4. Any distress, annoyance or embarrassment suffered by that person or his family arising from the violation of privacy; and 5. The conduct of that person and the defendant, both before and after the commission of the violation of privacy, including any apology or offer of amends made by the defendant.	Monetary sanctions range from $20,000 CAD to a maximum of $350,000 CAD depending on the severity of the violation and the degree of harm to an individual.	Privacy Commissioner of Canada enforces the PIPEDA, while Provincial Privacy Commissioners are responsible for enforcing the privacy laws in their Provinces. However, under PIPEDA, the Privacy Commissioner would have the right to intervene in relation to a violation of that law. If the violation is under a provincial law, the Provincial Privacy Commissioner can intervene.	The Privacy Commissioner of Canada proposed in early 2020 a rights-based approach to privacy that would bring Canadian privacy laws closer to the European Union's General Data Protection Regulation ("GDPR"), which the Commissioner believes is a strong example of rights-based legislation. The parliament is expected to adopt the proposal by end of 2020. The Commissioner has proposed that Parliament enact rights-based privacy legislation which includes the following parts: **1. Define the right to privacy broadly (e.g., "freedom from surveillance, without justification") and recognize the quasi-constitutional nature of privacy laws.** The Commissioner argues that a rights-based approach to privacy should recognize the quasi-constitutional status of a right to privacy. This recognition along with a broad definition of privacy would form the basis for a set of laws whose purpose is to protect the freedom of individuals to live and develop in a modern society without fear of unjustified surveillance by state or commercial entities. In the Commissioner's view, this is consistent with the Supreme Court of Canada's recent privacy-related decisions that recognize the fundamental importance of privacy in a free and democratic society. The Commissioner argues that changes in the laws of other jurisdictions show that federal privacy law has fallen behind in protecting the privacy rights of Canadians. **2. Draft the law by including specific rights and obligations.** The Commissioner notes that current federal privacy laws are primarily data protection statutes as opposed to laws that protect the privacy rights of individuals. The Commissioner suggests that privacy laws should remain technology-neutral and maintain a set of principles so that the laws can endure over time in the face of technological change. However, he argues that although PIPEDA contains important principles like consent, access, and transparency, principles alone are not sufficient to adequately protect individual privacy rights. Therefore, the Commissioner argues for the addition of specific rights and obligations. In the Commissioner's view, rights-based laws would increase trust in both government and the digital practices of companies. They would also encourage responsible innovation, which may help both the private and public sectors maintain competitiveness internationally as privacy laws continue to evolve in other jurisdictions. **3. Increase enforcement mechanisms.** The Commissioner argues that his office needs significantly greater powers in order to increase compliance by organizations. Under PIPEDA, the Commissioner cannot issue orders against organizations and must bring an action in Federal Court, and only in respect of complaints that the Commissioner did not initiate. In the Commissioner's view, this allows companies to stall and ignore any recommendations and findings of the Commissioner until the issue is litigated in Federal Court. Therefore, his argument is that additional enforcement powers would enable quick and effective remedies to ensure greater compliance. The new powers would include the ability to conduct proactive inspections, and to issue binding orders and fines (subject to judicial review). In addition, the Commissioner proposes giving a public authority (the Commissioner or another public body) the power to issue binding guidance under PIPEDA. This would help translate some of the existing principles into practical requirements that would be easier to enforce. The Commissioner also argues that individuals should have an independent right of action in court for violation of their privacy rights.

USA (Federal)

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
Federal law does not provide a private right of action that would enable individuals to sue companies directly for privacy intrusions, but several state privacy laws include private rights of action. Illinois's biometric privacy law allows users whose biometric data is illegally collected or handled to sue the companies responsible. The California Consumer Protection Act allows users to sue a company for statutory damages if their personal information is involved in a data breach as a result of the company's negligence. Without a private right of action, individuals have to rely on federal or state enforcers, like the FTC, to protect their privacy. Currently there is opposition to a private right of action from companies and policymakers. However, The US legal system provides numerous ways for an individual to remedy violations of privacy by government agencies. The burden is on the consumer to show proof of substantial harm as a result of privacy abuses.	Individuals must file complaints with the states Attorney Generals stating how and to what extent their privacy rights have been negatively impacted and the extent of harm they have suffered.	The burden is on the individual to prove substantial and measurable harm has occurred.	The US legal system provides numerous ways for an individual to remedy violations of privacy even though the private right of action is not explicitly defined in the federal privacy laws. In the US, persons who suffer substantial harm from a privacy violation can seek remedies in both civil and criminal cases. Civil suits allow qualifying individuals, including EU persons, to sue the US government for violations of law that can result in monetary damages and injunction of ongoing illegal actions. Unlike criminal violations of law, which must be prosecuted by an agent of the government, any qualifying individual can bring a civil suit as long as he or she meets the thresholds required for the alleged wrongful act. The burden is on the individual to prove substantial harm. The Federal Privacy Act ("Act") specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised on agency violations of the Act or agency regulations promulgated thereunder. An individual claiming such a violation by the agency may bring the civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs against the agency. In addition, the court may direct the agency to grant the plaintiff access to his/her records, and when appropriate direct the agency to amend or correct its records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or wilful refusal by the agency to comply with the Act. In the case of "criminal violations" of the Act (Section 3 of the Act, 5 U.S.C. Sec. 552a(i) limits these so-called penalties to misdemeanours), an officer or employee of an agency may be fined up to $5,000 for: 1. Knowingly and wilfully disclosing individually identifiable information which is prohibited from such disclosure by the Act or by agency regulations; or 2. Wilfully maintaining a system of records without having published a notice in the Federal Register of the existence of that system of records. In addition, an individual may be fined up to $5,000 for knowingly and wilfully requesting or gaining access to a record about an individual under false pretences. While the Act does not establish a time limit for prosecutions for violation of the criminal penalties provision of the Act, it does limit the bringing of civil action to two years from the date on which the cause of action arose. See 5 U.S.C. Sec. 552a(g)(5). However, the time limit for filing a civil action may be tolled for material and wilful misrepresentation by the agency of any information which is required to be disclosed, if the misrepresentation is material to the liability of the agency. A civil action may be filed in the U.S. District Court in the district where the requester resides or has his/her principal place of business; in which the agency records are located; or in the District of Columbia.	The Federal Trade Commission is currently the primary privacy enforcer, but its authority is limited. The FTC is responsible for protecting consumers from unfair or deceptive acts or practices. It is constrained as an enforcement agency that focuses primarily on interstate commerce and consumers and has not defined what constitutes unfair or deceptive acts or practices in the context of privacy rights. State Attorney Generals are responsible for enforcing state privacy laws but have no jurisdiction over federal privacy laws.	Although there is no private right of action for consumers under U.S. Federal laws, individuals can join class action lawsuits against companies that have violated their privacy rights. Most class action lawsuits are filed against companies that have experienced massive data breaches. However, the burden is on the plaintiffs to prove that they have suffered irreparable harm. Class action lawsuits are expensive and time consuming, averaging 5 to 7 years to settle. The reason most individual consumers cannot sue companies for privacy violations is due to the fact that most large U.S. companies have put legal clauses in the fine print of their customer agreements that bars consumers from suing them in federal court, and instead force victims to pursue arbitration or, in some cases, file suit in small claims court. The vast majority of U.S. Fortune 500 companies keep consumers out of court by including mandatory arbitration clauses in their customer agreements. Sometimes referred to as forced arbitration, mandatory arbitration is a form of dispute resolution that generally requires consumers to handle any legal disputes outside the federal court system. Companies usually have them in their "terms of service" agreements that consumers agree to when they use or purchase a product or service. Instead of going to federal court, arbitration agreements require individuals to go before an arbitrator or a panel of arbitrators, who may even be hired by the company, to decide the final outcome of the dispute. There are typically few options to appeal if the consumer doesn't like the ruling. Arbitration is a private proceeding that consumers typically navigate by themselves, so there is no easily accessible public record and no giant group of people calling attention to the issue. 93% of companies that enforce arbitration, also ban class action lawsuits. This protects companies from exposing systemic problems or wrongdoing. In mid-2019, the U.S. Congress introduced the FAIR Act that would eliminate forced arbitration clauses in any employment, consumer, and civil rights cases. Instead, companies, consumers and employees would need to voluntarily agree to arbitration. However, the Act was never voted on due to an influx of lobbying money from U.S. companies to defeat the Act.

USA (Federal)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
There is no private cause of action in HIPAA, so it is not possible for a patient to sue for a HIPAA violation. Even if HIPAA Rules have clearly been violated by a healthcare provider, and harm has been suffered as a direct result, it is not possible for patients to seek damages. While HIPAA does not have a private cause of action, it is possible for patients to take legal action against healthcare providers and obtain damages for violations of state laws. In some states, it is possible to file a lawsuit against a HIPAA covered entity on the grounds of negligence or for a breach of an implied contract, such as if a covered entity has failed to protect medical records. In such cases, it will be necessary to prove that damage or harm has been caused as a result of negligence or the theft of unsecured personal information.	If HIPAA Rules are believed to have been violated, patients can file complaints with the federal government and in most cases, complaints are investigated. Action may be taken against the covered entity if the complaint is substantiated and it is established that HIPAA Rules have been violated. The complaint should be filed with the Department of Health and Human Services' Office for Civil Rights (OCR). A complaint should be filed before legal action is taken against the covered entity under state laws. Complaints must be filed within 180 days of the discovery of the violation, although in limited cases, an extension may be granted. Complaints can also be filed with state attorneys general, who also have the authority to pursue cases against HIPAA-covered entities for HIPAA violations.	The actions taken against the covered entity will depend on several factors, including the nature of the violation, the severity of the violation, the number of individuals impacted, and whether there have been repeat violations of HIPAA Rules.	Remedies under the HIPAA Rules are based on a four-tier approach. The four categories used for the penalty structure are as follows: Tier 1: A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules Tier 2: A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of "willful neglect" of HIPAA Rules) Tier 3: A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation Tier 4: A violation of HIPAA Rules constituting "willful neglect", where no attempt has been made to correct the violation. The associated penalties for violations per record include: Tier 1: Minimum fine of $100 per violation up to $50,000 Tier 2: Minimum fine of $1,000 per violation up to $50,000 Tier 3: Minimum fine of $10,000 per violation up to $50,000 Tier 4: Minimum fine of $50,000 per violation In addition to financial penalties, covered entities are required to adopt a corrective action plan to bring policies and procedures up to the standards demanded by HIPAA.	Penalties for HIPAA violations can be issued by the Department of Health and Human Services' Office for Civil Rights (OCR) and state attorneys general.	Both Covered Entities and Business Associates are required to comply with HIPAA. Covered Entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centres, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities. Covered entities can be institutions, organizations, or persons. A Business Associate is a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

USA (California)

California Consumer Protection Act 2020 (CCPA)

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
Section 1798.150(a)(1) of the CCPA provides that "any consumer whose nonencrypted and nonredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure" due to a business's failure to "implement and maintain reasonable security procedures" may commence a civil action to recover either: 1) actual damages; or 2) statutory damages between $100 and $750 per consumer per incident (whichever is greater). There is a four-year limitation period for commencing an action.	The CCPA only creates a private right of action against businesses that fail to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.	CCPA law provision does afford businesses some protection from consumer suits seeking statutory damages. Specifically, under CCPA Section 1758.150(b), a consumer must provide a business with 30 days' written notice of the alleged CCPA violation that leads to the "unauthorized access and exfiltration, theft, or disclosure" of the consumer's personal information. The business then has 30 days to cure the violation and notify the consumer that: 1) the violation has been cured; and 2) no further violations will occur[64]. If the business is able to act quickly to cure the violation and inform the subject consumer of such, then the consumer may not bring suit for individual or class-wide statutory damages. Critically, consumers are not required to provide advance notice prior to bringing actions for actual damages.	Civil actions can result in remedies to recover: 1) actual damages; or 2) statutory damages between $100 and $750 per consumer per incident (whichever is greater). This means that the maximum amount an individual consumer can recover in a proceeding, regardless of the severity of the breach, is $750.	The Attorney General of the State of California is responsible for bringing enforcement actions against an organisation if it is proven that the organisation failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Also, the Attorney General has a right to intervene in proceedings.	By creating a right to statutory damages for each violation, this provision of the CCPA law makes it much easier for a consumer to bring a civil action following a data breach. Proving actual damages as a result of a data breach can be difficult, if not impossible. However, California consumers no longer need to prove such damages to recover. Given the fact that damages do not need to be proven, it is predicted that the CCPA will be a boon to the plaintiff's bar, who will bring class actions on behalf of California data breach plaintiffs.

[64] Consumers may exercise their right of access to verify that the business has taken the stated remediation actions and can bring an action if they are dissatisfied, but the cost of attorney's fees may prove to be a deterrent.

Japan

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
Under the Act on the Protection of Personal Information (APPI) data subjects have the right to sue business operators (civil action) that have collected their personal information unlawfully or processed the data in a way that is not disclosed or approved by the data subject. An organisation that is involved in a data breach may, depending on the circumstances, be subject to the suspension, closure or cancellation of the whole or part of its business operations, an administrative fine, penalty or sanction, civil actions (private right of action) and class actions or a criminal prosecution. There is a four- year limitation period for commencing an action.	Data subjects who believe they may have suffered harm as a result of a data breach or privacy violation must first file a complaint with the PPC prior to initiating a private right of action. If no resolution or an unacceptable resolution by the PPC occurs, the data subject may take a private right of action. The individual only able to bring suit if the regulator determines there is significant cause, having regard to the potential harm, the history of violations, and the remediation actions taken by the organisation in violation of the APPI.	Data subjects must be able to prove that they have, or are likely to, experience substantial personal, emotional or physical harm as a result of a privacy violation[65].	A business operator that violates privacy rights under the APPI can be sentenced to imprisonment with forced labour of not more than six months or to a fine of not more than ¥300,000 (i.e. this is an to an administrative fine imposed by the regulator). If an individual exercises a private right of action, the courts can decide on the quantum of damages. Note: A business operator is any organisation that processes personal data.	Personal Information Protection Commission (PPC) is responsible for determining if a data subject has significant cause to file a civil suit against a business operator.	Although there is no express provision in the APPI creating an obligation to notify data subjects or data authorities in the event of a data security breach, the APPI Guidelines stipulate that actions to be taken in response to data breach or privacy violation are set out separately from the Guidelines. The PPC has set out the following actions: 1. Submission of a mandatory internal report on the data breach and/or privacy violations and measures to prevent expansion of the damage; 2. Mandatory investigation into any cause of the data breach or privacy violation; 3. Confirmation of the scope of those affected by the data breach or privacy violation; 4. Development and implementation of preventive measures; 5. Mandatory notifications to any person (to whom the personal information belongs) affected by the data breach or privacy violation; 6. Mandatory prompt public announcement of the facts of the data breach or privacy violation, and preventive measures to be taken; and 7. Prompt notifications to the PPC about the facts of the data breach or privacy violation and preventive measures to be taken except for where the data breach or privacy violation has caused no actual, or only minor, harm (e.g., wrong transmissions of facsimiles or emails that do not include personal data other than names of senders and receivers).

[65] Substantial harm has not been clearly articulated however, this is commonly interpreted as physical harm, mental or emotional harm, identify theft, financial harm, abuse or discrimination.

South Korea

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
South Korea has maintained some of the strictest, if not the strictest laws and regulations on data privacy for two decades. The Personal Information Protection Act ("PIPA"), a general omnibus statute governing data privacy matters, was enacted in 2011. In addition to the PIPA, there are other sector-specific statutes in South Korea and different regulatory agencies are in charge of enforcing different statutes. In terms of enforcing data privacy statutes, there are three primary categories of remedy. First, government agencies could order corrective measures and impose administrative fines. Second, there are possibilities of criminal penalties since many statutes contain provisions providing for criminal liability for violations. Third, victims of data breaches or other injured parties can of course bring civil lawsuits/private rights of action in pursuit of monetary damages for negligence. Private parties can bring lawsuits seeking damages or other civil remedies if there are data breaches or other violations of data privacy law. The burden of proof to substantiate that the Personal Information Processor was at fault or negligent is shifted from the plaintiff to the defendant. In terms of the general civil procedure, in order to ameliorate the burden for small-claim plaintiffs, a "group lawsuit" was also introduced, by which a consumer organization or not-for-profit civic group is allowed to bring a lawsuit on behalf of the individuals who suffered privacy harms.	If individuals believe their privacy has been violated by exposure or misuse of their personal data, they can file a complaint with the PIPC who in turn will ask for an investigation by the appropriate regulatory agency. In addition, individuals can file a civil or criminal compliant directly with the appropriate regulatory agency or the Minister of the Interior or the courts.	Individuals can file a complaint or suit even if they have no substantial proof that they have been harmed by the privacy violation. Exposure of personal data that does not lead to harm is still considered a privacy violation under the PIPA.	Compensatory damages as well as moral damages may be awarded. Punitive damages in the amount up to three times the substantiated harm may be awarded, provided that the Personal Information Processor was grossly negligent or failed to show a lack of intent. Further, statutory damages are now available up to 3 million Korean Won or 3% of annual revenue, whichever is higher, with no requirement on the part of plaintiffs to substantiate the actual harm suffered, provided that the Personal Information Processor was negligent or had intent to cause harm.	The Personal Information Protection Commission ("PIPC"), the main regulatory agency under the PIPA, however, it lacks enforcement authority. Instead, multiple government agencies play supplemental roles in order to make sure that data privacy laws and regulations are complied with.	It is important to recognise that many of the statutes dealing with data privacy matters, including the PIPA, the IC Network Act, the Location Information Act, and the Credit Information Act, contain provisions allowing for criminal punishment of data breaches and other violations. Possible criminal sanctions include not just criminal fines but also imprisonment. The availability of criminal punishment plays an important practical role in enforcing data privacy in South Korea. The mere possibility of criminal punishment has a significant deterrent effect on potential violators. Additionally, the availability of criminal punishment also implies that the prosecutors' office and police often assume the role of de facto investigators and enforcers of data privacy matters. The prosecutors' office and/or police can (and do) instigate their own investigations and bring criminal charges, independent of any administrative or civil proceedings. Such criminal charges are often followed by administrative proceedings and civil lawsuits.

Hong Kong

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
There is currently no direct right of action for individuals under the Personal Data Privacy Ordinance (PDPO), however in January 2020, the Privacy Commissioner and the Hong Kong Government introduced expansions to the PDPO to mirror and in some cases, exceed the GDPR. The changes include a private right of action.	None	None	None	The Privacy Commissioner has responsibility for enforcing the PDPO	Recently, enhancements to the Hong Kong's Personal Data Privacy Ordinance ("PDPO") has been gaining momentum as the Hong Kong Government and the Privacy Commissioner ("Commissioner") endeavour to update the PDPO in line with international standards and to address new challenges to data protection amidst the rapid development of information and communication technologies. The reform proposals, introduced in January 2020, are at a preliminary stage and no draft bill is available yet. However, the Constitutional and Mainland Affairs Bureau of the Government ("CMAB") and the Commissioner have issued a consultation paper and sought feedback from members of the Legislative Council ("LegCo") at the LegCo Panel on Constitutional Affairs meeting on 20 January 2020. Several key directions for reform have been proposed: 1. Establish a mandatory mechanism for notification of any privacy violations data breach (including data security breach leading to unlawful or accidental destruction, alteration, loss, unauthorized disclosure of, or access to personal data) that have a "real risk of significant harm" as soon as practicable and, under all circumstances, in not more than five (5) business days. 2. Raising the levels of fines for existing criminal offences on breach of the Commissioner's enforcement notice; and introduce new administrative fines and direct sanctioning powers of the Commissioner for contravention of the PDPO. 3. Provide individuals with a private right of action to sue organisations for privacy violations that could result in real risk of significant harm. 4. Clarify and supplement the PDPO's existing data protection principles with the new requirements on data users to (i) formulate a clear data retention policy and (ii) notification of such policy to data subjects, to enhance accountability and transparency of data users' practices on protecting and handling personal data. 5. The objectives of these proposed reforms are to enhance the deterrent effect and to more properly reflect the severity of the offences under the PDPO. 6. Recognize the pressing need for increased direct regulation of data processors to enhance data security, and to ensure accountability, governance and control of data users' outsourcing and data processing activities from both data users and data processors. 7. Introduce new regime in the PDPO for direct regulation of data processors, including placing direct legal obligations on data processors (and their sub-contractors) to, amongst other things, be directly accountable for data retention and data security, and handling data breach notifications. 8. Amend and expand the PDPO's existing definition of "personal data" to cover not only information that relates to an "identified" person, but to also cover information relating to an "identifiable" person, in order to better satisfy public expectations in light of the prevalent use of data analytics, profiling and tracking technologies for identifying individuals. 9. Directions for proposed reform on this particular issue under consideration include, e.g. (i) introducing legislative amendments to specifically address doxxing behaviour, (ii) conferring further statutory powers on the Commissioner to request the take-down/removal of doxxing contents from social media platforms, websites and other online platforms, (iii) enhancing the relevant criminal investigation, prosecution and enforcement powers under the PDPO. **Note:** Doxxing means the search for and publishing of private or identifying information about a particular individual on the Internet, typically with malicious intent. It is anticipated that the new legislation will be introduced by the end of 2020.

New Zealand

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
The *Privacy Act 2020* will come into effect on 1 December 2020, replacing the *Privacy Act 1993*. The Privacy Act states that the IPPs do not create enforceable rights, except for IPP 6 in respect of public sector agencies. However, any individual may make a complaint to the Privacy Commissioner about an interference with privacy. Such complaints can ultimately reach the Human Rights Review Tribunal and the courts.	An individual must first complain about an interference with privacy to the Privacy Commissioner. If the Commissioner either refuses to investigate the complaint, refuses to continue an investigation or decides the complaint has no substance, the individual may commence proceedings in the Tribunal. The Commissioner may also refer a complaint to the Director of Human Rights Proceedings, who may commence proceedings in the Tribunal on behalf of the aggrieved individual. If the Commissioner has issued an access direction in respect of a complaint about IPP 6, the aggrieved individual may enforce this direction by applying to the Tribunal for an access order. The standard of proof at the Tribunal is balance of probabilities. An individual may appeal the Tribunal's decision to the High Court and beyond.	For the Tribunal to find that there has been an 'interference with privacy', it must be satisfied than an action has breached one of the IPPs, an AISA, an information matching provision, or the privacy breach notification provisions, and that this breach has caused the affected individual harm. Harm can relate to loss, damage or injury, loss of rights or benefits, or significant emotional harm (including humiliation, loss of dignity and injury to feelings). Harm is not required in relation to a breach of IPPs 6 or 7. In this case, any refusal without a proper basis will constitute an interference (though the Tribunal will still need to consider harm as a means to quantify damages as per section 103(1) of the Act). The Tribunal has previously held that a breach need only be a contributing factor to the harm, not the sole cause.	The Privacy Act 2020 does not provide for any punitive damages in respect of breaches of the IPPs etc. While the Act does create several new criminal offences, with associated fines (as explained in our Comments), none of these relate to general breaches of the IPPs. Remedies for individuals include a declaration of interference, orders for actions to be taken or ceased, or the payment of compensatory damages. The Tribunal has the discretion to award damages of up to $350,000 per aggrieved individual.	The Privacy Commissioner acts as 'gatekeeper' for the Tribunal, insofar as individuals must first complain to the Commissioner, and the Commissioner may attempt to settle a complaint. As noted, the Commissioner may also refer a complaint to the Director of Human Rights Proceedings, which may result in proceedings in the Tribunal. The Commissioner may also take proceedings in the Tribunal to enforce a compliance notice and has the right to appear. The Commissioner has the right to appear in any proceedings before the Tribunal, where the Director of Human Rights Proceedings has declined to appear. Also, the Commissioner may be asked to appear as amicus curiae in civil proceedings.	The Privacy Act 2020 clarifies the right to take privacy class actions, by providing for representative cases on behalf of one or more aggrieved individuals. The Tribunal may award damages of up to $350,000 in respect of each aggrieved individual in a class action, with the result that class action complaints could represent a significant financial risk to a defendant agency. Criminal penalties are also now available in respect of breaches of certain Privacy Act provisions, such as where a person misleads an agency in order to gain access to personal information, where an agency destroys a document that is the subject of an access request, or where an agency fails to notify a serious privacy breach to the Commissioner. The penalty for each of these offences is a fine of $10,000. Criminal penalties are available under the Crimes Act 1961, in respect of the unlawful interception of private communications, as well as certain unlawful monitoring and surveillance activities.

Singapore

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
Under the Protection of Personal Data Act, an aggrieved individual who believes his/her privacy rights have been violated may make a complaint to the Commission. Additionally, any person who suffers loss or damage directly as a result of a contravention of any of the main data protection provisions may also commence a private civil action in respect of such loss or damage suffered. Action must be commenced within two years after the violation is discovered.	Any person who suffers loss or damage directly as a result of non-compliance by an organisation with the data protection provisions under the PDPA has a right of action for relief in civil proceedings in a court. However, where the PDPC has made a decision under the PDPA in respect of such a contravention, this right is only exercisable after such a decision issued by the PDPC becomes final after all avenues of appeal have been exhausted. The court may grant relief as it thinks fit, including an award of an injunction or declaration, or damages.	The individual filing the right of action has the burden of proving substantial loss or personal damage has occurred.	Non-compliance with certain provisions under the PDPA constitute an offence, for which a fine or a term of imprisonment may be imposed. The amount of the fine and the length of imprisonment vary, depending on which provisions are breached. For instance, a person found guilty of making requests to obtain access to or correct the personal data of another without authority may be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding 12 months, or both. Intentionally disposing of, altering, falsifying, concealing or destroying a record containing personal data or information about the collection, use or disclosure of personal data is an offence that may be punishable upon conviction with, in the case of an individual, a fine of up to S$5,000, and in the case of an organisation, a fine of up to S$50,000. The obstruction of PDPC officers in the course of their investigations or provision of false statements to the PDPC may be punishable upon conviction with, in the case of an individual, a fine of up to S$10,000 or imprisonment for a term not exceeding 12 months; and in the case of an organisation, a fine of up to S$100,000.	The Personal Data Protection Commission (PDPC) has the authority to initiate investigations and enforce sanctions. In the private, civil action, the PDPC can be asked to testify specifically related to its investigation and the outcome of the investigation.	Currently, there is no strict requirement prescribed under the PDPA to notify the PDPC or individuals of breaches of data security. However, in its Public Consultation on Approaches to Managing Personal Data in the Digital Economy, the PDPC has proposed a mandatory data breach notification requirement under the PDPA, to better oversee the level of incidences and management of data breaches at the national level. According to the PDPC's responses to the public consultation (published 1 February 2018), the PDPC has proposed that organisations notify both the affected individuals and the PDPC in situations where the breach is 'likely to result in significant harm or impact to the individuals to whom the information relates'. If the breach does not pose any risk of impact or harm to affected individuals, but is of a significant scale (e.g., 500 affected individuals), the PDPC has proposed that organisations notify the PDPC only. In relation to the timeframe for notification, the PDPC has stated in its response that it intends to provide for an assessment period of up to 30 days from the day the organisation first becomes aware of a suspected data breach, to assess whether the suspected data breach is eligible for notification. Following the organisation's assessment, where the organisation determines that the data breach is eligible for reporting, then the organisation must notify the relevant parties and the PDPC as soon as practicable, but no later than 72 hours' from the time of determination. The mandatory data breach notification requirement is not in effect yet but is expected to be implemented by the end of 2020.

The Philippines

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
The Philippines Data Privacy Act provides a private right of action for damages for inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. The Philippines legal system also has privacy torts that provide redress to individuals whose right to privacy defined in the Data Privacy Act has been violated.	In order to file a private right of action individuals must show that they suffered physical, emotional or financial harm due to unauthorized processing, processing for unauthorized purposes, negligent access, improper disposal, unauthorized access or intentional breach, concealment of breach involving sensitive personal information, unauthorized disclosure, and malicious disclosure.	Individuals must first file a complaint with the Privacy Commissioner who in turn will decide whether or not to launch an investigation. Individuals may file a private right of action regardless of whether the Privacy Commissioner takes action.	Remedies in the Philippines for privacy violations depend on the nature of the violation or breach. The following outlines the remedies: 1. *Unauthorised Processing of Personal Information and Sensitive Personal Information* (a) The unauthorised processing of personal information shall be penalised by imprisonment ranging from one (1) year to three (3) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law. (b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law. 2. *Accessing Personal Information and Sensitive Personal Information Due to Negligence* (a) Accessing personal information due to negligence shall be penalised by imprisonment ranging from one (1) year to three (3) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorised under this Act or any existing law. (b) Accessing sensitive personal information due to negligence shall be penalised by imprisonment ranging from three (3) years to six (6) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorised under this Act or any existing law. 3. *Improper Disposal of Personal Information and Sensitive Personal Information* (a) The improper disposal of personal information shall be penalised by imprisonment ranging from six (6) months to two (2) years and a fine of not less than one hundred thousand pesos (Php100,000.00) but not more than five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection. (b) The improper disposal of sensitive personal information shall be penalised by imprisonment ranging from one (1) year to three (3) years and a fine of not less than one hundred thousand pesos (Php100,000.00) but not more than one million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection. 4. *Processing of Personal Information and Sensitive Personal Information for Unauthorised Purposes* The processing of personal information for unauthorised purposes shall be penalised by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than one million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorised by the data subject, or otherwise authorized under this Act or under existing laws. The processing of sensitive personal information for unauthorized purposes shall be penalised by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorised by the data subject, or otherwise authorised under this Act or under existing laws. 5. *Unauthorized Access or Intentional Breach* The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.	The Privacy Commissioner has the authority to initiate investigations and enforce sanctions.	The inclusion of imprisonment as a sanction for violations of the Privacy Act has had a major impact on minimizing the number of privacy violations or data breaches, whereas financial penalties did little to deter violations.

The Philippines

Threshold requirements	Procedural considerations	Elements of the action	Remedies	Regulator's role	Comments
			6. *Concealment of Security Breaches Involving Sensitive Personal Information* The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than one million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach. 7. *Malicious Disclosure* Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than one million pesos (Php1,000,000.00). 8. *Unauthorized Disclosure* (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than one million pesos (Php1,000,000.00). (b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than five hundred thousand pesos (Php500,000.00) but not more than two million pesos (Php2,000,000.00). 9. *Combination or Series of Acts* Any combination or series of acts shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than one million pesos (Php1,000,000.00) but not more than five million pesos (Php5,000,000.00). 10. *Extent of Liability* If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalised under this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office.		