



Tuesday 15 October 2024

# Litigation – Statutory Tort and Direct Right

Presented by Christien Corns, Partner – K&L Gates, Rob Pulham, Special Counsel – K&L Gates, and Niall Watson-Dunne, Investment Manager - Omni Bridgeway

# Contents

01 Background

02 Development of the Law

03 Statutory Tort for Serious  
Invasions of Privacy

04 Direct Right

05 Part 9 s 80UA(4)

06 Recommendations



# New Privacy Laws

## Background

- On 12 September 2024, the long awaited *Privacy and Other Legislation Amendment Bill 2024* (Cth) (the Privacy Bill) was released
- The Privacy Bill includes the proposed statutory tort for serious invasions of privacy, which represents a significant development in the law in respect of a general right to privacy
- The so called “direct right of action” as contemplated by the Privacy Act Review Report



# Development of the Law



## ***Australia Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199 – Key Facts***

- An unidentified trespasser installed hidden cameras in the licensed possum killing and processing abattoirs
- The footage was given to the Animal Liberation Ltd and then subsequently forwarded to the Australian Broadcasting Corporation (the ABC)
- Operators of the abattoirs applied for an interlocutory injunction to restrain the ABC from distributing, publishing, copying or broadcasting the footage
- The application was dismissed at first instance but reversed on appeal. The ABC appealed to the High Court

# *Australia Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199 - Arguments*

## Australian Broadcasting Corporation

- The right to privacy is not one that can be enjoyed by corporations
- It had broken no law or principle which justifies an order preventing it from broadcasting the material that has come into its possession, maintaining that it is 'free to broadcast, simply because there is no law against it'

## Lenah Game Meats Pty Ltd

- Court should depart from older authorities, declaring that 'Australian law now recognises a tort of invasion of privacy' available to natural persons and corporations
- Should the ABC publish, distribute, copy or broadcast the material, it would constitute an actionable invasion of a right to privacy

## ***Australia Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199 - Outcome***

- The High Court found in favour of the ABC
- The abattoirs failed to obtain an injunction to prevent the ABC from broadcasting the footage



## ***Australia Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199 – Findings (November 2001)***

- No general statutory right to privacy has been enacted in Australia
- Any development of the tort will be to the benefit of natural, not artificial persons:
  - “Whatever development may take place in [the context of a tort of invasion of privacy] ... will be to the benefit of natural, not artificial, persons.”*
- Court favoured the approach that existing laws and legal principles should be developed to allow for legal protections for privacy interests, but cautioned against the introduction of a new tort as there was a lack of precision of the concept of privacy

## ***Giller v Procopets* [2004] VSC 113 & *Giller v Procopets* (2008) 24 VR 1 - Facts**

- Ms Giller, the Plaintiff, and Mr Procopets, the Defendant, separated after being in a de-facto relationship for approximately three years
- Following their separation, the Plaintiff obtained an interim intervention order against the Defendant after an alleged assault
- Following the application for the intervention order, the Plaintiff and Defendant remained intimately involved, during which the Defendant filmed their sexual activities using a video camera, without the knowledge of the Plaintiff
- Following an altercation between the parties, the Defendant threatened to distribute the video and photographs, including to the Plaintiff's employer. The Defendant also showed the video to various individuals

# ***Giller v Procopets* [2004] VSC 113 & *Giller v Procopets* (2008) 24 VR 1 - Arguments by Plaintiff at First Instance**

One of the causes of action claimed by the Plaintiff was a claim for compensatory, aggravated and exemplary damages for *invasion of privacy*.

## **Findings at First Instance - April 2004**

The law for breach of privacy has *not* developed to the point where the law in Australia recognises an action for breach of privacy.

## **Findings at On Appeal (December 2008)**

- The trial judge erred by failing to consider authorities which supported the development of a tort of invasion of privacy in Australia
- The Court considered the Australian Law Reform Commissions' recommendation that the federal legislation provide for a "statutory cause of action for a serious invasion of privacy"
- As the Court was satisfied that compensation on the ground of breach of confidence was sufficient and therefore there was no need to further discuss the development of the tort



# Statutory Tort for Serious Invasions of Privacy

## Elements of the Tort (s. 7)

- 1 An invasion of privacy: (1) intrusion upon seclusion and / or (2) misusing information relating to the plaintiff
- 2 Reasonable expectation of privacy in all of the circumstances
- 3 The invasion of privacy was intentional or reckless
- 4 “Serious” invasion
- 5 The public interest in protecting a plaintiff's privacy must outweigh any competing public interest(s) in the invasion of privacy identified by the defendant



The statutory tort for serious invasions of privacy would provide a flexible framework to address current and emerging privacy risks and provide individuals with the ability to better protect themselves and seek compensation for a broader range of serious invasions of privacy, including physical privacy, as well as misuse of information.

Explanatory Memorandum, 2024



# Intrusion Upon Seclusion

Watching, listening to, or recording someone's private activities or private affairs. Examples:

- Taking a photo of someone in a change room
- 'Tapping' phone calls or 'hacking' into someone's computer

# Misuse of Information

Collecting or disclosing someone's private information. Examples:

- Unauthorised disclosure of highly sensitive medical records
- Unauthorised disclosure of intimate photographs (“revenge porn”)



## Both (1) An Intrusion Into Seclusion and (2) Misuse of Information

Example: hacking into an individual's private electronic device and disseminating intimate photographs.

# Reasonable Expectation of Privacy

A Court will consider factors such as:

- Nature of the information (eg intimate, medical, financial)
- Place where the information occurred
- Where the private information was stored
- Attributes of the plaintiff (eg age, occupation, cultural background)
- Means to obtain the private information
- Purpose of the disclosure of information / intrusion
- Whether the information was already in the public domain
- Conduct of the plaintiff (eg did they invite publicity?)

## Fault: Intentional or Reckless

- The plaintiff must prove that the defendant intentionally or recklessly invaded the plaintiff's privacy
- Proof of negligence is not sufficient to establish the fault element
- According to the Explanatory Memorandum: “*“Recklessness” includes situations where a person is aware of a substantial risk and—having regard to the circumstances known to them—it is unjustifiable for the person to take the risk.*”

## When Will the Invasion be ‘Serious’

- Whether an invasion of privacy is ‘serious’ is an objective test
- The tort is intended to protect intangible interests and the dignity of the plaintiff, and is therefore actionable without proof of damage

## Factors Considered ‘Seriousness’

The Court will consider factors including:

- The degree of the offence, distress or harm to dignity that the invasion is likely to cause
- Knowledge and motive of the defendant (eg malice)
- The nature and extent of the privacy intrusion
- The sensitivity of the personal information involved

# Public Interest Balancing Test



# Remedies

- Interim injunctions / injunctions
- Damages (excl. aggravated damages)
- Account of profits
- Order requiring an apology

- Any other remedy the Court considers appropriate
- Correction order
- Destruction / delivery up of material
- Declaration

# Defences

- The invasion was required / authorised by law or court / tribunal order
- The plaintiff consented to the invasion
- The defendant reasonably believed the invasion was necessary to prevent / lessen a serious threat to life / health or safety of a person
- The invasion was incidental to the lawful defence of persons or property and was proportionate, necessary and reasonable
- Defamation defences:
  - Including, absolute privilege, publication of public documents, fair report of proceedings of public concern, exemption for journalism



## Standard Limitation Periods

- One year after the day that the plaintiff becomes aware of the invasion of privacy
- If the plaintiff is unaware of the invasion of privacy, three years after the day the invasion of privacy occurred
- If the plaintiff was under 18 years of age when the invasion of privacy occurred, before the plaintiff's 21st birthday

# Exemptions



The invasion of privacy by "journalists" in respect of the collection, preparation for publication and publication of "journalistic material"



Enforcement bodies



Intelligence agencies



Persons under 18 years of age

## Potential Application of the Law

- The Victims of Crime Assistance Tribunal (VOCAT) recently accidentally shared hundreds of email addresses, some believed to belong to victims of crime, within an administrative email chain
- VOCAT sent an email detailing administrative changes to the compensation application process for Victorian victims of crime — but hundreds of email addresses were able to be seen by all recipients

# Elements of the Tort

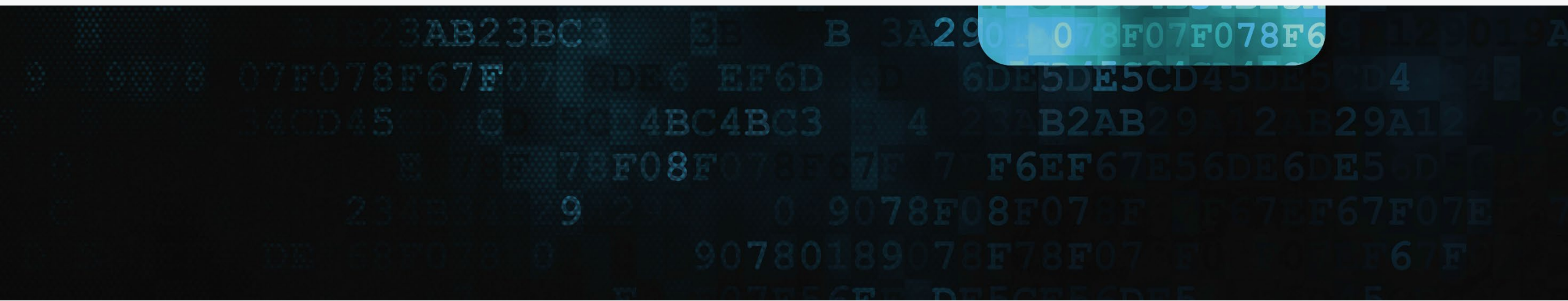
- 1** *An invasion of privacy:* misusing the email addresses of victims of crime (many of which included first and last names) by publishing them in an email from VOCAT which was able to be seen by all recipients
- 2** *Reasonable expectation of privacy in all of the circumstances:* victims of crime applicant would reasonably expect in all the circumstances that their email addresses used as part of an application for compensation would not be disseminated to others
- 3** *The invasion of privacy was intentional or reckless:* the disclosure of the email addresses was an administrative error rather and so may not meet the high threshold of “recklessness” and may only be “negligent”
- 4** *Serious invasion:* the invasion was not motivated by malice, however, the degree of the offence may be considered to be “high” given that the victims of crime may have been identified to the wider public
- 5** *The public interest in protecting a plaintiff's privacy must outweigh any competing public interest(s) in the invasion of privacy identified by the defendant:* this aspect does not appear to be relevant on the facts and is unlikely to be raised by VOCAT

## Defences / Remedies

- No defences appear applicable on the facts
- The cause of action may fail on the basis that the invasion was negligent rather than “reckless”
- It is unlikely that a Court would be satisfied by the argument that (1) VOCAT was aware of the substantial risks around disclosing private email addresses of victims of crime, many of which include first and surnames and (2) having regard to the circumstances known to them—it is unjustifiable for the person to take the risk as the email was meant to be sent to those email addresses, it appears they should have been “blind copied”
- If the cause of action was successful, potential remedies could include a Court ordering damages or an apology by VOCAT



# Direct Right



## Direct Right of Action

- A “direct right of action” would enable individuals to bring their own actions and class actions against entities bound by the *Privacy Act 1988* (Cth) (Privacy Act) for an interference with their privacy under that Act
- At this stage, a “direct right of action” as contemplated by the Review Report has not been included in the Privacy Bill
- Currently, an individual is required to make a complaint to the Office of the Australian Information Commissioner (OAIC) and the OAIC can decide whether or not to conduct an investigation
- The OAIC’s enforcement powers include seeking enforceable undertakings, determinations, injunctions and application for a civil penalty order

## Potential Application of the Law

- Optus recently experienced a ‘cyber incident’ that resulted in the compromise of some customers’ personal information
- Personal information of more than nine and a half million former and current customers of Singtel Optus Pty Limited and its subsidiaries were accessed by a cyber attacker. This includes passport details and driver licence numbers



## Potential Application of the Law Cont.

- An Australian Privacy Principle (APP) under the Privacy Act includes, “An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure...”
- If there was a “direct right of action”, an individual could make a claim against Singtel Optus Pty Limited and/or the relevant subsidiaries that it arguably did not take reasonable steps to protect sensitive information
- More facts would be needed about what steps were taken to protect the data which was compromised

# Part 9 s 80UA(4)

## Privacy Bill, Part 9 s 80UA(4)

- Pursuant to s 80UA(4) of the Privacy Bill:
  - The Federal Courts may make any orders in civil penalty proceedings where a contravention of a civil penalty provision under the Privacy Act has been established and if the Court “has determined, or will determine, under the Regulatory Powers Act that an entity has contravened a civil penalty provision of the Privacy Act (other than those contained in Part IIIA)
- These orders may include the payment of damages to an individual by way of compensation for any loss or damages suffered due to the contravention
- The Court may exercise this power:
  - ....(b) on application, from an (i) an individual who has suffered, or is likely to suffer, 4 loss or damage as a result of the contravention

# Litigation Impacts

- How are significant "breach of privacy" claims currently pleaded
- How might future significant "breach of privacy" claims be pleaded
- Potential for class actions based on "direct rights" of action

# Recommendations

## Next Steps: How to Prepare

- Know what personal information you collect and hold and why you hold it (eg data inventory)
- Implement the appropriate steps to keep the information secure
- Delete personal information you no longer need
- Get your breach response planning sorted – speak with our Privacy Team at K&L Gates for more information
- Ensure compliance with the Privacy Act

# Contacts



**Christien Corns**

Partner  
Melbourne  
+61 3 9640 4248  
[Chrisiten.Corns@klgates.com](mailto:Chrisiten.Corns@klgates.com)



**Rob Pulham**

Special Counsel  
Melbourne  
+61 3 9640 4414  
[Rob.Pulham@klgates.com](mailto:Rob.Pulham@klgates.com)



**Niall Watson-Dunne**

Investment Manager  
Sydney  
+61 2 8223 3567  
[NWatsonDunne@omnibridgeway.com](mailto:NWatsonDunne@omnibridgeway.com)

K&L GATES