The Legal Protection of Personal Images Shared on Social Networks in Australia

Eugenia Georgiades

Bachelor of Arts (Hons), Bachelor of Laws, Graduate Diploma Legal Practice, Master of Laws

School of Law, Griffith University

This thesis is submitted in fulfilment of the requirements of the degree of Doctor of Philosophy

December 2016
Abstract

Social networks have changed the nature of communication in the modern world: they have changed how people communicate, the frequency and mode of communication, and how people relate to those communications. Social networks have also changed the type of information that is communicated. One of the notable developments has been a proliferation of the sharing of images that people have taken themselves. From the ubiquitous selfie through to group shots, personal images are now a key part of modern social communication.

A number of problems have arisen as a consequence of the rapid increase in the sharing of personal images online. This is because personal images uploaded online are, more now than ever, prone to misuse. Third parties are easily able to reuse, distort and alter images that are uploaded on social networks. As a result, people are at risk of losing control over the images that they upload online.

The aim of this thesis is to critically examine the ways in which Australian law protects personal images that are shared on social networks. It also aims to suggest ways in which the law in this area might be improved. Focusing on intellectual property (and related laws), Part I looks at the way that images are currently protected under Australian law, showing that while there is some legal protection for images uploaded on social networking sites, the protection is inadequate. Part II explores some changes that could be implemented to improve the protection of personal images in Australia. In particular, Part II looks at the possibility of expanding the scope of privacy law and of incorporating image rights and a right to be forgotten into Australian law. This is followed by a brief conclusion that looks at other possible initiatives, such as criminalising the publication of sexual images online to prevent revenge porn.
Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person, except where due reference is made in the thesis itself.

(Signed)_____________________________________
Eugenia Georgiades

Acknowledgements

I would like to thank my supervisors, Brad Sherman, Leanne Wiseman and Allan Ardill, for their support throughout the thesis. I would also like to thank Jay Sanderson.

I thank Pernilla White for providing editorial assistance, in particular for formatting and proofing chapters of the thesis. I would like to thank Susan Jarvis for her assistance in the final edit of the thesis, specifically for formatting and proofreading.
# Contents

Abstract ........................................................................................................................................... iii

Statement of Originality .................................................................................................................. iv

Acknowledgements ........................................................................................................................ iv

Part I Existing Legal Protection for Personal Images on Social Networks in Australia

Chapter 1 ......................................................................................................................................... 1

Introduction .................................................................................................................................... 3

1.1 Introduction ............................................................................................................................ 3

1.2 Changes Bought About By Social Network Sites ................................................................. 7

1.3 Why should we protect personal images? ............................................................................. 13

1.4 Balancing competing interests ............................................................................................. 21

1.5 Overview ............................................................................................................................... 23

1.6 Existing Scholarship On Social Networks, Image Rights And The Law ............................ 25

1.7 Overview of Social Networks ............................................................................................... 27

Chapter 2 Terms of Use, Personal Images and Social Networks ............................................. 34

2.1 Introduction ............................................................................................................................. 34

2.2 Licensing and Ownership of Personal Images ...................................................................... 36

  2.2.1 Facebook .......................................................................................................................... 37

  2.2.2 Twitter .............................................................................................................................. 39

  2.2.3 Instagram ......................................................................................................................... 40

2.3 Collection of Images .............................................................................................................. 41

  2.3.1 Facebook ........................................................................................................................ 41

  2.3.2 Twitter ............................................................................................................................ 44

  2.3.3 Instagram ....................................................................................................................... 45

2.4 Use of Images .......................................................................................................................... 48

  2.4.1 Facebook ........................................................................................................................ 48

  2.4.2 Twitter ............................................................................................................................ 50

  2.4.3 Instagram ....................................................................................................................... 51

2.5 Sharing and Disclosing .......................................................................................................... 51

  2.5.1 Facebook ........................................................................................................................ 52

  2.5.2 Twitter ............................................................................................................................ 56

  2.5.3 Instagram ....................................................................................................................... 56
5.3.4 Where there is no relationship between the parties: Strangers ........................................ 130
5.4 Has there been a Breach of Duty? .............................................................. 132
5.5 Possible Defences .................................................................................. 134
5.5.1 Consent ............................................................................................... 134
5.5.2 Public Interest ..................................................................................... 135
5.6 Conclusion ............................................................................................... 136

Part II Possible Solutions .................................................................................. 137

Chapter 6 Expanding Privacy Law .................................................................. 142
6.1 Introduction ........................................................................................................ 142
6.2 A New Statutory Tort of Invasion of Privacy for Serious Invasions of Privacy ...... 143
6.2.1 Intrusion Upon Seclusion ........................................................................... 144
6.2.2 Is a Social Network Page a ‘Secluded’ Space? ........................................... 145
6.2.3 Is Uploading an Image on a Social Network Page an Intrusion Upon Seclusion? ... 146
6.2.4 Scope of Protection ................................................................................. 147
6.3 Effectiveness of the Tort in Protecting Personal Images Shared Online .......... 148
6.4 A Misuse of Private Information .................................................................. 149
6.4.1 What is ‘Private Information’? ................................................................. 150
6.4.2 Is There a Reasonable Expectation of Privacy? ......................................... 152
6.4.3 Is the Disclosure of Private Facts Highly Offensive to a Reasonable Person? ...... 154
6.4.4 Expanding the Law of Confidence to Include Private Information ............. 155
6.5 Conclusion ................................................................................................. 157

Chapter 7 An Australian Right to Publicity? ................................................. 160
7.1 Introduction ................................................................................................. 160
7.2 What are Publicity Rights? ........................................................................... 162
7.2.1 The Use of the Plaintiff’s Identity .......................................................... 163
7.2.2 The Use Must Constitute an Advantage, Commercial or Otherwise .......... 163
7.2.3 The Use of the Image is Without a Person’s Consent ................................ 164
7.2.4 The Use of the Image Results in Injury .................................................. 165
7.3 Exceptions to the Right of Publicity ............................................................. 167
7.3.1 Public Interest and Newsworthiness ....................................................... 167
7.3.2 Freedom of Expression ......................................................................... 169
7.4 Problems with a Right of Publicity? ............................................................ 173
7.4.1 No Law Against Being Photographed .................................................... 174
7.4.3 A Right of Publicity May Not Extend to Dead People ............................ 175
7.4.4 Publicity Rights May be Lost When Entering into a Social Network Contract .... 176
Chapter 8 ......................................................................................................................... 178

The right to be forgotten in Australia ............................................................................. 178

8.1 Introduction .................................................................................................................. 178

8.2 Requirements for Protection ....................................................................................... 183

8.2.1 Data .......................................................................................................................... 183

8.2.2 Data Subject .......................................................................................................... 184

8.3 Use is Within the scope of the Right to be Forgotten .................................................. 185

8.4 Exceptions to the Right to be Forgotten ..................................................................... 188

8.5 Does Australia Need the Right to be Forgotten? ....................................................... 195

Chapter 9 Conclusion ....................................................................................................... 200

Bibliography ..................................................................................................................... 206

Cases ................................................................................................................................. 206

Legislation ......................................................................................................................... 210

Secondary sources ............................................................................................................ 212
Part I
Existing Legal Protection for Personal Images on Social Networks in Australia
Chapter 1

Introduction

1.1 Introduction

This thesis examines the effectiveness of the existing legal regimes in protecting personal images that are shared online. In Australia, the stark reality is that while there is some legal protection for personal images shared online, this is limited. The thesis examines how the law in this area can be improved. In particular, it argues that people whose image is captured in photographs that are shared on social networks ought to have the ability to control the use of their images through a right of publicity and a right to be forgotten. In considering the developments and legal protection afforded to personal images in the United States and Europe, it will be argued that Australian law is lagging behind these jurisdictions.

The last decade or so has seen an explosion on social networking. Web 2.0 sparked the growth of online participatory culture, where the user was a central actor in creating and sharing information.¹ The introduction of new websites and services enabled users to create and share things about themselves with other users on the Internet in an unprecedented way. Previously, online communication technologies such as email, email lists, text messaging and instant messaging existed in isolation.² Social networks changed the ways in which people share and


disseminate personal images in an online environment, and this has created a number of problems, particularly when images are used without permission, or when they are altered, changed or used for different purposes. Problems also arise when circumstances change, such as when a creator or subject changes their mind about an uploaded image, or when a creator or subject dies.

The origin of social network sites can be traced back to the formation of SixDegrees.com in 1997. This site enabled users to create profiles and list friends on their profile page and also to view their friend’s lists. At the time, SixDegrees was a pioneering online social network site that fused the features of creating profiles, friends’ lists and email messaging. SixDegrees paved the way for other sites that supported combinations of various profile and ‘friend’ articulated networks such as AsianAvenue, BlackPlanet and MiGente. These sites not only enabled users to create their own profiles; they also allowed them to identify friends without the approval of those connections.

While SixDegrees closed down in 2000 due to its inability to connect users with features other than accepting friend requests, various new sites were launched between 1997 and 2001 that shared some form of communication technology or a combination of communication technologies. LiveJournal, for example, allowed users to mark people as friends, to follow their journals and to manage privacy settings. In 2001, the next surge of sites centred on linking

---

3 Ibid 214.
4 Ibid.
5 Ibid.
6 Profiles existed as part of dating sites and email lists prior to SixDegrees starting up. These were visible on the user’s instant messaging service – for example, AIM (American Instant Messenger) – but not visible to other people, see Danah M Boyd and Nicole Ellison, above n 2, 214; Kevin Lewis, Jason Kaufman and Nicholas Christakis, ‘The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network’ (2008) 14(1) Journal of Computer-Mediated Communication 79, 80-1; Lin Kuan-Yu and Hsi-Peng Lu, ‘Why People Use Social Networking Sites: An Empirical Study Integrating Network Externalities and Motivation Theory’ (2011) 27(3) Computers in Human Behavior 1152, 1152-3.
8 See Dinah M Boyd and Nicole Ellison, above n 2, 215; Kaveri Subrahmanyam, Stephanie M Reich, Natalia Waechter and Guadalupe Espinoza. ‘Online and Offline Social Networks: Use of Social
personal and professional networks such as Ryze.com.\textsuperscript{9} Notably, sites such as Tribe.net, LinkedIn, Friendster and Ryze were all intertwined on a personal and professional level because the people behind the sites were all connected and believed they could exist without competing against one another.\textsuperscript{10}

In 2002, the popular social network site Friendster was developed to compete with Match.com an online dating site.\textsuperscript{11} Building on the common features of dating sites, it focused on introducing people to strangers.\textsuperscript{12} The distinguishing feature of Friendster was that it was ‘designed to help friends of friends meet based on the assumption that friends of friends would make better romantic partners than strangers’.\textsuperscript{13} Friendster’s popularity quickly surged to 300,000 users via word of mouth among various groups, particularly bloggers, attendees at the Burning Man arts festival and gay men.\textsuperscript{14} As Friendster’s popularity grew, the site began to

\begin{itemize}
  \item Danah M Boyd and Nicole Ellison, above n 2, 215; Zeynep Tufekci, ‘Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Site’ (2008) 28 (20) \textit{Bulletin of Science Technology and Society} 20, 21-23; Alessandro Acquisti and Ralph Gross, above n 1, 36.
  \item Danah M Boyd and Nicole Ellison, above n 2, 215. David Beer, above n 1, 517; Alessandro Acquisti and Ralph Gross, above n 1, 36.
  \item Danah M Boyd and Nicole Ellison, above n 2, 215; Z Tufekci, ‘Grooming, Gossip, Facebook and MySpace: What Can We Learn About These Sites from Those Who Won’t Assimilate?’ (2008) 11(4) \textit{Information, Communication & Society} 544, 545-7; Patrick Van Eeke and Maarten Truyens, ‘Privacy and
experience difficulties. Specifically, Friendster’s databases and servers were unable to keep up with the growing demands of users; effectively, users became frustrated with the faltering site and replaced Friendster with email. After the failure of Friendster, various new social networks were launched, which adopted the popular features of the early success of Friendster, such as the profile-centric feature.

Following the failure of Friendster, social networks surged in the early 2000s, first with MySpace and then with Facebook. Since 2003, a range of new social networks have proliferated. There are now social networks for everyone: from activists, religious groups and gamers through to travelers and photographers. Presently there are billions of users of social media with Facebook citing 1.11 billion users, 500 million Twitter users, and 100 million Instagram users. Popular sites such as Facebook, Twitter, Instagram, Pinterest, Flickr, Google+, YouTube and Windows Live have transformed the way people communicate and interact with each other. Social networks have enabled people to translate their existing physical networks into visible digital connections within


Danah M Boyd and Nicole Ellison, above n 2, 215; Alessandro Acquisti and Ralph Gross, above n 1, 36.


Danah M Boyd and Nicole Ellison, above n 2, 214–15; Richard Sanvenero, ‘Social Media and Our Misconceptions of the Realities’ [2013] 22(2) Information and Communications Technology Law 89, 90-1; Alessandro Acquisti and Ralph Gross, above n 1, 36.

Scholarship places the first online social network as SixDegrees in 1997; after the failure of SixDegrees, other sites emerged during the period between 1998 and 2001. See generally, Danah M Boyd and Nicole Ellison, above n 3, 214–15; David Beer, above n 1, 519; Alessandro Acquisti and Ralph Gross, above n 1, 36.

See generally Danah M Boyd and Nicole Ellison, above n 2, 214–15; David Beer, above n 1, 519.

See generally Danah M Boyd and Nicole Ellison, above n 2, 214, 216; David Beer, above n 1, 517-519; Alessandro Acquisti and Ralph Gross, above n 1, 36.


social network structures. Before a person can gain access to a social network, they are first required to create and complete an online profile. From the profile, users are also able to share and control information distributed to their contacts. Some social networks have a varied user base and offer photo-sharing, video sharing, instant messaging or blogging facilities that people can use to communicate with one another. These networks allow people to share their lives in an online environment.

1.2 Changes Bought About By Social Network Sites

Social networks have brought about a convergence of public and private worlds. Before social networks, people shared photographs by sending the physical photographs by post or via email. As communication technologies evolved, so too have social networks. Most social networks allow people to upload and share their images with multiple people instantaneously. In some

---


26 This allows the users to be interconnected with one another through a visible social network structure.


28 See generally, Alessandro Acquisti and Ralph Gross, above n 1, 36; Danah M Boyd and Nicole Ellison, above n 2, 214; Ralph Gross and Alessandro Acquisti, above n 1, 72-3.
situations, people who upload images on a social network page are able to identify or ‘tag’ a third party captured in a photograph. Third parties are able to upload images of other people without their permission or knowledge. Another consequence is that personal images that are shared online may be reused and reshared with ease and with limited restrictions.

While sharing information on social networks allows people to interact and communicate with greater ease, it also raises a number of problems. Problems may arise, for example, when a person uploads an image of themselves and that image is reshared and reused, or when people’s images are uploaded by third parties without permission. In thinking about the problems that potentially arise when personal images are captured and uploaded on social networks, it is important to note that two different groups are potentially affected: the people who create the images and the people whose images are captured in the photographs.

When a person takes a photograph of themselves and uploads it on a social network page, a number of problems potentially arise. This is because personal images that are shared on social networks may be reused and reshared without the permission of the person who uploaded the image. A well-known example of this occurred in 2012, when Randi Zuckerberg posted an image of her family on her Facebook page and a third party reposted the image on Twitter without her permission. While access to the uploaded image was restricted to ‘friends’, there was little she could do to stop her friends from reposting or re-sharing her image. Problems may also arise when a social network reuses or reshares images that have been uploaded on a person’s profile page. This occurs because when people upload and share images on their profile page, the network is able to collect the images and reuse them. Problems may also arise when a third party takes a photograph of someone and uploads their image onto their profile page. When the subject of the photograph does not wish to have their image captured

---

29 ‘Tagging’ is a Facebook feature that allows users to identify people in an uploaded image.

30 Sam Biddle, Watch Randi Zuckerberg Have a Facebook Freak Out over Her Photo Going Viral, Gizmodo (28 December 2012) <http://gizmodo.com/5971918/watch-randi-zuckerberg-have-a-facebook-freakout-over-her-photo-going-viral>.

31 A person may think that they are only sharing their image with their contacts, but may not realise that their contacts and their friends are able to access the image/s; see Alessandro Acquisti and Jens Grossklags, ‘Privacy Attitudes and Privacy Behavior’ (2004) Economics of Information Security 165; Alessandro Acquisti and Ralph Gross, above n 1, 36; Amanda Nosko, Eileen Wood and Seija Molema, ‘All About Me: Disclosure in Online Social Networking Profiles: The Case of FACEBOOK’ (2010) 26(3) Computers in Human Behavior 406, 406-7; Cliff Lampe, Nicole Ellison and Charles Seinfeld, above n 25, 436-7.
and uploaded online, the mere act of uploading the image may create problems. Problems may also arise when the uploaded image is reshared or reused by other parties or by a social network. When this happens, the person whose image is captured has a limited ability to control the use of their image and prevent any misuse. Problems may also arise when the image is distorted or altered. Another problem that may arise here is when there is a change in circumstance of the person uploading the image – for example, when a creator of an image has a change of mind or dies.

As social media has become increasingly pervasive, people’s images have become more prone to misuse, abuse and exploitation. One way that personal images are exploited is when third parties use people’s images for advertising purposes without permission. Social networks receive revenue through targeted advertising; each advertisement that appears on a person’s profile is specific to the information contained in their posts and images. In sharing and exchanging personal images on social networks, there are competing interests that each person has when they share images on social network. The problem here is that people whose images are captured in photographs and shared online have a limited ability to prevent the misuse of their image.

While Instagram, Twitter and Facebook all collect images that are uploaded and shared on their networks, the networks use the images differently. Social networks such as Twitter collect personal images and allow their affiliates and third party advertisers to access the images. For example, images may be indexed in search engines or used for advertising purposes. In contrast, Instagram uses personal images to personalise content and provide

---

32 See Twitter, Privacy Policy, Information Collection and Use, Tweets, Following, Lists and other Public Information (30 September 2016) <https://twitter.com/privacy?lang=en> which states: ‘Our Services are primarily designed to help you share information with the world. Most of the information you provide us through the Twitter Services is information you are asking us to make public. Your public information includes the messages you Tweet; the metadata provided with Tweets, such as when you Tweeted and the client application you used to Tweet; the language and time zone associated with your account; and the lists you create, people you follow, Tweets you mark as likes or Retweet, and many other bits of information that result from your use of the Twitter Services. We may use this information to make inferences, like what topics you may be interested in, and to customize the content we show you, including ads. Our default is almost always to make the information you provide through the Twitter Services public for as long as you do not delete it … For instance, your public user profile information and public Tweets are immediately delivered via SMS and our APIs to our partners and other third parties, including search engines, developers, and publishers that integrate Twitter content into their services, and institutions such as universities and public health agencies that analyze the information for trends and insights. When
information to users that may include advertising and marketing purposes.\textsuperscript{33} While Facebook uses personal images to ‘provide, improve and develop’ their service, it also provides ‘short cuts’ to people by making suggestions such as tagging friends in photographs or liking a product. This occurs when Facebook suggests that users tag their friends when they upload and share images on a profile page.

As a result of people sharing and exchanging personal images online, networks are able to collect personal images and use these images for advertising or marketing purposes. As we will see, this is because social network contracts/policies allow the networks to use and access all images that are uploaded; even if they are subject to restricted privacy settings. The result of this is that even though social networks have privacy settings, these settings do not necessarily guarantee that personal images are not misused.

Another problem that potentially arises when a person uploads their image onto a profile page is that a third party may distort or alter the image – for example, by turning the personal image into a meme. In these circumstances, copyright and moral rights may protect the creator of an image where the image is distorted or altered.

Problems also potentially arise when a person uploads an image and there is a change of circumstance – for example, the person changes their mind about the sharing of an image online. In situations where a person poses for a photograph and later changes their mind about the image being shared, they have a limited ability to prevent the use of their image. At best, a subject in an image can request the copyright owner to remove their image from the social

\textsuperscript{33} Instagram, \textit{Privacy Policy, Clause 2. How We Use Your Information} (19 January 2013) https://help.instagram.com/155833707900388: ‘In addition to some of the specific uses of information we describe in this Privacy Policy, we may use information that we receive to: help you efficiently access your information after you sign in; remember information so you will not have to re-enter it during your visit or the next time you visit the Service; provide personalized content and information to you and others, which could include online ads or other forms of marketing; provide, improve, test, and monitor the effectiveness of our Service; develop and test new products and features; monitor metrics such as total number of visitors, traffic, and demographic patterns; diagnose or fix technology problems; automatically update the Instagram application on your device; Instagram or other Users may run contests, special offers or other events or activities (“Events”) on the Service. If you do not want to participate in an Event, do not use the particular Metadata (i.e. hashtag or geotag) associated with that Event.’ Facebook, \textit{Data Policy How Do We Use This Information} (29 September 2016) https://www.facebook.com/full_data_use_policy
network. In the event that a copyright owner is willing to remove the photograph from their profile page the same problems that were discussed above arise. While a creator may have a limited ability to prevent the misuse of their images from being reshared online after they have changed their mind, a subject who changes their mind is unable to prevent the use of their image in most circumstances.

Further problems potentially arise when someone dies. While social networks like Facebook have provisions for how a person’s profile page may be accessed after they die, such as providing a ‘legacy’ contact, the provisions are limited in scope and provide little protection against misuse. A well-known example of the problems that arise when a person dies is the case of Nikki Catsouras who, in October 2006, was decapitated when she lost control of her father’s Porsche.34 The Californian Highway Patrol (CHP) followed standard procedure and took photographs of the crime scene.35 The crime scene was so gruesome that the coroner refused to allow the parents to identify the body.36 Two CHP employees then emailed nine of the gruesome photographs to their friends and family members on Halloween as shock value.37 The photographs subsequently went viral.38 After a long legal battle spanning copyright and privacy issues, the defendants settled with the Catsouras family in 2012. It is uncertain whether the European Court of Justice’s decision of Google Spain v Gonzalez,39 discussed in Chapter 8, influenced the defendants to settle, as a judge had ordered the two parties to talk ahead of a jury

36 Ibid.
37 Ibid.
38 Ibid.
The Catsouras case highlighted the limited protection in the United States for uploading and sharing deceased people’s images online.\(^{41}\)

Another problem that potentially arises is when images of deceased Aboriginal and Torres Strait Islander people are shared online. This is because there are customary practices against publishing images of deceased people during mourning periods. Problems also arise when people share and exchange images of deceased Aboriginal and Torres Strait Islander people on social networks because the publication may cause distress to family members.\(^{42}\) Another cultural practice is the prohibition on publishing names of deceased Aboriginal and


\(^{41}\) Some scholars argue that ‘families have a privacy interest in death scene images of deceased relatives’: Daniel Solove, Family Privacy Rights in Death Scene Images of the Deceased Concurring Opinions (27 April 2009) [http://concurringopinions.com/archives/2009/04/family_privacy.html](http://concurringopinions.com/archives/2009/04/family_privacy.html); see also, National Archives and Records Admin v Favish, 541 US 157 (2004) where the American Supreme Court stated: ‘We have little difficulty … in finding in our case law and traditions the right of family members to direct and control disposition of the body of the deceased and to limit attempts to exploit pictures of the deceased family member’s remains for public purposes … In addition this well-established cultural tradition acknowledging a family’s control over the body and death images of the deceased has long been recognized at common law. Indeed, this right to privacy has much deeper roots in the common law … An early decision by the New York Court of Appeals is typical: It is the right of privacy of the living which it is sought to enforce here. That right may in some cases be itself violated by improperly interfering with the character or memory of a deceased relative, but it is the right of the living, and not that of the dead, which is recognized. A privilege may be given the surviving relatives of a deceased person to protect his memory, but the privilege exists for the benefit of the living, to protect their feelings, and to prevent a violation of their own rights in the character and memory of the deceased. Schuyler v Curtis, 147 NY 434 (1895).’ See generally, Clay Calvert, ‘Privacy of Death: An Emergent Jurisprudence and Legal Rebuke to Media Exploitation and a Voyeuristic Culture’ (2005) 26 Loyola Los Angeles Entertainment Law Review 133, 133-42; Clay Calvert, ‘A Familial Privacy Right Over Death Images: Critiquing the Internet-Propelled Emergence of a Nascent Constitutional Right that Preserves Happy Memories and Emotions’ (2013) 40 (3) Hastings Constitutional Law Quarterly 475, 503; Catherine Leibowitz, ‘A Right to be Spared Unhappiness: Images of Death and the Expansion of the Relational Right of Privacy’ (2013) 32(1) Cardozo Arts & Entertainment Law Journal 347, 347-350.

While the name of the deceased person may be withheld, the publication of the image may still cause distress and harm to the family and the community.\textsuperscript{44}

1.3 Why should we protect personal images?

While there are many situations in the online world where images may be misused, the mere fact that something has been misused is not necessarily a reason why it should be protected. In this section I pause to consider what might be considered a fundamental question namely, why should we protect images online? Before considering the questions of why personal images should be protected, it is necessary to consider whether all images should be treated equally or whether the law should differentiate between different types of images. This is important because there are many different types of images online from the mundane and trivial through to the highly personal which may warrant different protection.

In some situations Australia, like the United Kingdom, has treated personal images differently, depending on the nature of the image.\textsuperscript{45} For example the law of breach of confidence has treated images differently depending on the information that is depicted in the photograph. While images that are of a sexual or intimate nature may be protected, an image of a person walking outside may not warrant protection. Here the law has been willing to pass judgment over the nature and quality of the information and to change the way the law applies over.


\textsuperscript{45} Personal images are a subset of ‘personal information’ that is currently protected under s 6 (1) of Privacy Act 1988 (Cth) and includes written information about a person. Because an image allows a person to be identified (even without written information identifying them), it is one of the most significant forms of identification because the image represents a person thus ‘identification of the person appears to be an obvious and sufficient condition for awarding protection.’ Tatiana Synodinou, ‘Image Right and Copyright Law in Europe: Divergences and Convergences’ [2014] 3 (2) Laws 181, 183; Susan Corbett, ‘The Retention of Personal Information Online: A Call for International Regulation of Privacy,’ (2013) 29 Computer Law and Security Review 246, 248.
accordingly. In other contexts, however, the law has been less willing to pass judgement over the quality of the image. This is the case, for example, with copyright law which has traditionally refused to pass judgment over the relative quality of artistic works; once a work is classified as an artistic work (such as a photograph), no consideration is given to the quality of the photograph.46

It is clear that there are many different types of images online. Some contain sensitive important information, while other images are trivial and of fleeting (if any) interest. While the former are deserving of protection, the latter are less so. Having said this, this does not mean that we should create a two-tier system which only protects certain types of images. As copyright law has long acknowledged it is often difficult (or dangerous) to pass judgement on artistic works such as photographs. This is particularly the case with personal images – some people may be highly sensitive to disclosure, while others thrive on it. A better option would be to accept all images from the sensitive to the trivial, but to take account of these difference in the application of the law (especially in relation to remedies and damages). With this in mind we now revisit the question: why should we bother protecting personal images online?

Given the diversity of images online and the myriad of different interests potentially affected it is not surprising that there is no single reason why personal images should be protected. Instead there is a patchwork of different reasons why images might be protected that will differ depending on the type of image in question. There are a number of different reasons why a person’s image warrants protection that span economic and non-economic considerations that are associated with image rights.47 The following section examines the arguments for protecting a person’s image.48


48 See Tatiana Synodinou, above n 45, 183, where the author suggests that ‘Protection of a person’s image often takes a dual form based on the privacy/property dichotomy that fails to express in legal terms the autonomy and the particular features of a person’s image. Based on the foregoing, a person’s image appears to be a legal asset with a multiple identity and an indiscernible nature.’ See generally, Huw Beverly-Smith, above n 47, 8-9.
One reason why we should protect a person’s image is because the image is ‘an intangible asset.’ As Beverley-Smith suggests, ‘the increasing commodification of the human image demands that any modern classification of interests in personality should take account of the fact that a person’s name or features are also valuable economic assets’. This typically occurs where celebrities, athletes, musicians images are used in connection with advertising and marketing purposes. Another reason for protecting images builds on the protection of personality which, in turn, is founded on Lockean labour theory. As Locke said:

every Man has a property in his own Person. This no Body has any Right to but himself. The Labour of his Body, and the Work of his Hands, we may say, are properly his. Whatsoever then he removes out of the State of Nature hath provided, and left it in, he hath mixed his Labour with, and joined to it something that is his own, and thereby makes it his Property.

Given, as Locke said, that everyone has ‘a property in his own person’ it can be argued that a person’s image is their property. Nimmer built upon Locke’s labour theory when he said ‘it would seem to be a first principle of Anglo-American jurisprudence, an axiom of the most fundamental nature, that every person is entitled to the fruit of his labors unless there are

---

49 See Tatiana Synodinou, above n 45.
51 See generally Huw Beverly-Smith, above n 47, 8-9; Alisa M. Weisman, ‘Publicity as an Aspect of Privacy and Personal Autonomy’ [1982] 55 Southern California Law Review, 727, 730 who states that ‘because most publicity cases have arisen in the commercial advertising context, many courts and commentators have thought and written about publicity primarily in economic terms’.
52 See Tatiana Synodinou, above n 45,183 where the author suggests that’ Protection of a person’s image often takes a dual form based on the privacy/property dichotomy that fails to express in legal terms the autonomy and the particular features of a person’s image. Based on the foregoing, a person’s image appears to be a legal asset with a multiple identity and an indiscernible nature.’ See generally, Gert Colombi Ciacchi, Brüggemeier, Patrick, Aurelia O’Callaghan, Personality Rights in European Tort Law (Cambridge University Press, 2010) 565-6.
54 John Locke, above n 53; W. J. Hamilton,’ Property According to Lock’ (1932) 41 Yale Law Journal, 864, 878.
important countervailing public policy considerations’.\(^{55}\) In *Edison v Edison Polyform Mfg.*,\(^{56}\) the court remarked that: ‘If a man’s name be his own property….. it is difficult to understand why the peculiar cast of one’s features is not also one’s property, and why it’s a pecuniary value, if it has one, does not belong to its owner, rather than to the person seeking to make an unauthorised use of it’. The Lockean labour theory is particularly important for celebrities who often invest a considerable amount of time and energy in their images. As Neville J says:

>[A] celebrity has a legitimate proprietary interest in his public personality. A celebrity must be considered to have invested his years of practice and competition in a public personality which eventually may reach marketable status. That identity, embodied in his name, likeness, statistics and other characteristics is the fruit of his labors and is a type of property.\(^{57}\)

One of the most powerful reasons why we should protect personal images is because abuse of a personal image potentially impinges on the fundamental human values of human dignity and autonomy. The need to protect dignity and autonomy is reflected in Article 1 of the *International Convention on Human Rights* which provides that ‘all human beings are born free and equal in dignity and rights’\(^{58}\) and in the preamble of *The Universal Declaration of Human Rights*, which provides that all human beings should have fundamental human rights of dignity and worth of human person.\(^{59}\) Allowing the misuse of personal images online has the potential to impinge on dignity and autonomy. This is because, as the Canadian Supreme Court said,

---


\(^{59}\) Article 3 also provides that ‘everyone has the right to life, liberty and security of person’. Article 18,’ Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.
The camera lens captures a human moment at its most intense and the snapshot “defiles” that moment … A person surprised in his or her private life by a roving photographer is stripped of his or her transcendency and human dignity, since he or she is reduced to the status of a “spectacle” for others … The “indecency of the image” deprives those photographed of their most secret substance.\(^{60}\)

As Beverley-Smith argues many ‘violations of individual personality are of a non-pecuniary nature, not only because they cannot be assessed in money terms with any mathematical accuracy, but also because they are usually of inherently non-economic value’.\(^{61}\) In part this is because there is an ‘organic link between the intangible value of image and the core of personality, human dignity’.\(^{62}\) Because a person’s image is an element of personality that is ‘inextricably linked to the self’, the economic aspects cannot be divorced from the moral aspects of personality that include human dignity.\(^{63}\)

While there may not be a ‘coherent notion of human dignity as a legal value,’ nonetheless dignitary interests in a personal image often reflect a broad spectrum of factors including reputation, privacy and liberty.\(^{64}\) As Rosen points out, misuse of a person’s image constitutes ‘an intrinsic offense against individual dignity’.\(^{65}\) As the Canadian Supreme Court

\(^{60}\) J Ravanas, La Protection des Personnes contre la Realisation de leur Image (Paris, 1978), 388-9 (as translated in Canadian Supreme Court Reports). Marginally less orotund in the original French. Cited in Les Editions Vice-Versa Inc v Aubry [1998] 1 SCR 591, para 69. See further Jonathan Morgan, ‘Privacy Confidence, and Horizontal Effect: “Hello” Trouble’, [2003] 62(2) The Cambridge Law Journal 444, 446-447, where the author stated that the court held that privacy ‘protects individual autonomy and the control of each person over his identity, which includes the use made of his image. The fact that the photograph was in a public place (and that it might be difficult to obtain the consent of everyone photographed there) was expressly stated to be irrelevant’: see Les Editions Vice-Versa Inc v Aubry [1998] 1 SCR 591, 59 (L’Heureux-Dube and Bastarache JJ); see also E. Picard, ‘The Right to Privacy in French Law’ in M Colvin (ed), Protecting Privacy (Oxford, 1999) 91.


\(^{63}\) See Tatiana Synodinou, above n 45. 197.

\(^{64}\) See Huw Beverley-Smith, above n 47,10-1.

\(^{65}\) Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America (Random House Inc, New York, 2000), 19; see Richard C. Post, ‘Three concepts of Privacy’ (2001) 89 Georgetown Law Journal, 2087, 2092. Post states that ‘to equate privacy with dignity is to ground privacy in social forms of respect that we owe each other as members of a common community’; see
said in *Les Editions Vice-Versa Inc. v Aubry*, it is important to protect personal images in order to safeguard a person’s ‘individual autonomy and the control of each person over their identity’.

Protecting dignity is closely aligned with the protection of autonomy which ‘is a complex assumption about the capacities, developed or underdeveloped, of persons, which enable them to develop, want to act on and act on higher order plans of action which take as their self critical object one’s life and the way it is lived’. Autonomy is also an important value because it requires that a person should be able to take ‘self-critical responsibility for one’s ends and the way they cohere a life’. Autonomy is the freedom that an individual has to control what is revealed about them. Waldman suggests that ‘autonomy, and the separation of the personal and the public are rights based.’ These rights, as Waldman suggests, reflect the ‘primacy of the individual over society.’ This is particularly significant because ‘privacy theory is focused on individual freedom and not only sees the individual as the locus of privacy.

---

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199, where Gleeson CJ noted that the foundation of privacy is human dignity.


67 Ibid see e.g. Jonathan Morgan, above n 60, 446-7.


69 See generally, Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World* [2015] 69 (3) *University of Miami Law Review* 559, 585, the author explains that theories of privacy are concepts of autonomy and choice: the choice to disseminate information…. and the correlative right to control what other know about us’. He further argues that ‘autonomy and choice are central to both Locke and Kant as both agree that the freedom to choose defines man’.

70 See generally, Ari Ezra Waldman, above n 70, 566.

71 See generally, Ari Ezra Waldman, above n 70, 566. The author states that these rights reflect Lockean and Kantian ideals which are ‘united by the respect they offer the individual and individual rights’; see John Locke, *Second Treatise of Government*, (C.B. Macpherson ed., Hackett Publishing Go 1980) 123, 243.
rights but also sees the protection of individual freedom as the ultimate goal of privacy'. It allows an individual the power and freedom to choose for themselves what is private and what is not.

Another reason why images should be protected is because misuse of a personal image may unduly intrude upon the private life of an individual. As Godkin noted, ‘nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion.’ The sanctity of the private sphere is reflected in many human rights treaties including the European Convention of Human Rights, which protects a person’s private or family life. Importantly, respect for the private life of an individual extends beyond the invasion of private physical spaces (such as the home) to include the taking of a photograph of someone in a public place. While ‘we venture into the public, in order to further our private lives, we do not ipso facto relinquish all claims to a private sphere. Even tacit consent to being observed by others cannot automatically extend to their taking and, a fortiori, publishing photographs.’ As Lord Hoffmann in Campbell v MGN Ltd said:

---

73 See generally, Ari Ezra Waldman, above n 70, 567.

74 See generally, Ari Ezra Waldman, above n70, 568. Waldman also claims that individual freedom is viewed from a privacy perspective that is a ‘necessary condition for generating the ideals of independence and autonomy’. The author also states that ‘previous theories of privacy reflected the individual’s right to seclude himself and exclude others from certain aspects of his life, whether intimate, deviant or not. They appreciate privacy as guaranteeing freedom from something: private places and private things were so called because they belonged to the individual, who had the power to control dissemination.’ (Ibid 581).


76 European Convention on Human Rights, Art 8, provides that Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. See Tatiana Synodinou, above n 45, 183-188.

77 See e.g. Jonathan Morgan, above n 60. See Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Report 123 (2014) at para [5.16], 76.

78 See Jonathan Morgan, above n 60.
the publication of a photograph taken by intrusion into a private place (for example, by a long-distance lens) may in itself be such an infringement [of the privacy of the personal information], even if there is nothing embarrassing about the picture itself.  

A person’s image is one of the core features that identifies them to others. As Mensel suggests, the protection of a person’s image is important because the face is ‘the most transparent part of the body’; it captures a person’s facial expression which is ‘real feelings, character and personality’. An image consists of a person’s identification and often is a representation of them which is an ‘obvious and sufficient condition for awarding protection’. A ‘person’s image constitutes one of the chief attributes of his or her personality, as it reveals the person’s unique characteristics and distinguishes the person from his or her peers.’ This is because it ‘presupposes the individual’s right to control the use of that image, including the right to refuse publication thereof.’ As the Grand Chamber of the European Court of Human Rights noted, ‘the right to the protection of one’s image is … one of the essential components of personal developments.’

---

79 Campbell v MGN Ltd [2004] 2 AC 457, 75.
82 See Tatiana Synodinou, above note 45; Jill Marshall above n 80.
83 Von Hannover v Germany (No. 2), Grand Chamber judgment of 7 February 2012, § 96.
84 Von Hannover v Germany (No. 2), Grand Chamber judgment of 7 February 2012, § 96.
85 Von Hannover v Germany (No 2) 2012, (Applications nos. 40660/08 and 60641/08), Grand Chamber Judgment, [96], Reklos v Davourlis, Application No 1234/2005. [2009] at 40 states ‘Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual’s right to object to the recording, conservation and reproduction of the image by another person. As a person’s image is one of the characteristics attached to his or her personality, its effective protection presupposes, in principle and in circumstances such as those of the present case… obtaining the consent of the person concerned at the time the picture is taken and not simply if and when it is published. Otherwise an essential attribute of personality would be retained in the hands of a third party and the person concerned would have no control over any subsequent use of the image.’
Another reason why we should protect images online is because of Australia’s obligations under international law. Specifically, we should provide effective protection to image because Australia is a signatory to the *International Covenant on Civil and Political Rights*. Of key importance here is Article 17 which provides that member states should ensure that citizens are protected from the unlawful interference with family, privacy, home or correspondence and reputation. Further, Article 1 provides that all people have the ‘right of self-determination and are free to determine and freely pursue their economic, social and cultural development’. These provisions demand that we ‘recognise the significance of individual privacy, particularly in view of the privacy threats posed by rapidly developing information, communication and surveillance technologies and an increasingly invasive media industry.’ They also suggest that we should ‘encourage the protection of other privacy interests founded on personal autonomy and dignity, such as the interest in protecting against intrusions upon seclusion.’

While Australia has incorporated elements of the *International Covenant on Civil Political Rights* into domestic law (notably anti-discrimination and privacy law), the extent of protection is inadequate. This is because there is no recognised right to one’s image (or to personal privacy). In order to comply with Australia’s international obligations more effective legal protection needs to be introduced.

### 1.4 Balancing competing interests

The law dealing with personal images builds upon and balances a range of competing interests. These include freedom of expression, the right for the public to know, the right to private life,

---

86 *International Covenant on Civil and Political Rights* Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49.

87 Ibid, Article 17.

88 Ibid, Article 1 provides ‘All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development.’


90 Ibid.
and the interests of creators. In determining where and how these different interests are to be balanced the law builds a range cultural, technological and ethical considerations. Traditionally when drawing the balance the law has consistently prioritised freedom of expression over all other interests. This traditional view was captured in a comment by Lord Hoffman in *R v Central Television Plc* that:

> It cannot be too strongly emphasized that outside the established exceptions or any new ones which Parliament may enact in accordance with its obligations under the Convention [for the Protection of Human Rights and Fundamental Freedoms] *there is no question of balancing freedom of speech again other interests. It is a trump card which always win.*

Over the last two decades there has been a lot of commentary on the way in which digital technologies have challenged and unsettled traditional arrangements. The position is equally true in relation to the protection of personal images. The advent of the internet in general and social networks in particular means that the traditional balancing of interests used in relation to images needs to be rethought and re-evaluated. Of particular importance is the need to rethink the balance between freedom of expression and the right to private life. The new digital world means that ordinary people are all creators with competing interests. One of the recurrent themes of the thesis is that changes in technology mean that we need to recalibrate the line between freedom of expression and other interests. In many ways this is the key challenge posed by the new technologies that is addressed in the subsequent chapters.

---

91. As Lord Denning MR said in *Shering Chemicals Ltd v Falkman* [1981] 2 WLR 848, 865: ‘Freedom of the press is of fundamental importance in our society. It covers not only the right of the press to impart information of general interest or concern, but also the right of the public to receive it. It is not to be restricted on the ground of breach of confidence unless there is a ‘pressing social need’ for such restraint. In order to warrant a restraint, there must be a social need for protecting the confidence sufficiently pressing to outweigh the public interest in freedom of press.’

1.5 Overview

The aim of this thesis is to investigate the role that Australian law might play in dealing with these problems. To this end, the thesis examines the effectiveness of the existing legal regimes in protecting personal images that are shared online.

The thesis is limited to the protection of personal images in which copyright, breach of confidence, privacy and contract issues exist within social networks in Australia. It will not deal with patents and trademark issues on social networks. Patents and trademark infringement relate to commercial intellectual property rights; the thesis focuses on the amateur copyright interests. In the earlier stages of Facebook’s social network development, several trademark and patent infringement issues occurred.93 In 2008, Hasbro, which has the rights to sell Scrabble, launched a trademark infringement action against Facebook for its ‘Scrabulous’ app.94 While patent and trademark issues are significant to social networks; they fall outside the scope of protection of personal images. The tort of breach of confidence may provide protection in the absence of copyright protection, and confidential information captured under the Patent Act 1990 (Cth).95

Social networks have generated a range that span from pedophilia, through to identity theft, and fraud, as well as defamatory content, and passing off.96 While these issues are important the focus of the thesis is on whether personal images on social networks are protected

---


95 Any information that is confidential is potentially protected under the law of confidence. It also is not simply restricted to technical or formal requirements that could be protected under the Patents Act 1990 (Cth).

96 See e.g. Hogan v. Koala Dundee Pty Ltd., (1988) 20 FCR 314, 329-30 (Austl.); Henderson v. Radio Corp. Pty Ltd., [1960] 60 S.R. (N.S.W.) 576, 603. The common law tort of passing off applies in situations where the use of a celebrity’s image has been used commercially. In particular, passing off has traditionally applied to the commercial misappropriation of celebrity images and commercial organisations. As the focus of the thesis is on individual images that are shared online, it is outside the scope of the thesis.
adequately under the existing legislative framework and to the extent it is not suggesting reforms.

The remainder of this thesis is divided into two parts. **Part I: Existing Legal Protection for Personal Images** examines the adequacy of existing legal protection for personal images uploaded on social networks in Australia. Chapter 2 examines the ways in which social network contracts regulate the use of personal images that are shared on social networks. After outlining the various terms of use that social networks adopt, the chapter examines the impact that these terms have on the ability for people sharing and exchanging personal images. The chapter shows how social networks contracts facilitate the misuse of personal images. The contractual terms provide little protection for people whose personal images are shared by the copyright owners (the people who captured the photograph).

Chapter 3 focuses on how Australian copyright law protects personal images shared on social networks. The chapter shows that copyright provides little protection for personal images unless the copyright owner and the subject are one and the same. Chapter 4 examines the way that Australian privacy law protects personal images that are shared online. Specifically, it outlines how Australia’s fragmented approach for protecting privacy interests applies to the sharing and exchanging of photographs of people on social networks. The chapter argues that privacy law in Australia is inadequate to protect against the misuse of personal images online. Chapter 5 examines the way that the law of confidence protects personal images when those images are shared online. In so doing, it argues that while the tort of breach of confidence may protect certain types of personal images that are sensitive or of an intimate nature; personal images that are captured and depict various information about the person captured in the photograph, such as them eating and drinking, will not be protected under the law of confidence.

**Part II: Solutions** sets out some possible solutions to the problems with the legal protection of personal images in Australia identified in Part 1. Chapter 6 examines whether the recommendations of the Australian Legal Reform Commission in the 2014 ALRC Report would fill some of the gaps in the legal protection highlighted in the thesis. Chapter 7 evaluates whether adopting image rights in Australian law would provide adequate protection when personal images are shared online. Chapter 8 examines whether Australian law ought to adopt a right to be forgotten.
1.5 Existing Scholarship On Social Networks, Image Rights And The Law

The thesis grew out of a realisation that there was very little literature about the role the law does and should play in protecting personal images on social networks in Australia. While there has been a lot written on the legal status of social networks, there is an important gap in the literature regarding the standing of personal images on social networks in Australia. There is limited scholarship that explores how personal images are protected within a social network that exists outside of third-party copyright. While there has been scholarship that has considered commercial copyright infringement by people within a social network, it has not examined a person-to-person infringement of amateur copyright.

When reflecting upon the role played by the law of confidence in protecting personal images that are shared online, the existing scholarship tends to focus on images that reveal confidential or private information. As will be shown, the law of confidence has a limited application when images are shared on social networks. While the law of confidence may protect personal images in some situations, the protection is limited.

There is also little literature that examines the way that Australian privacy law protects personal images that are shared on social networks. The sharing and exchanging of people’s images on social networks poses challenges for privacy law to prevent the misuse of personal images. Consequently, the sharing of personal images on social networks has also highlighted concerns over the use and control of the use of the personal image.

There is also limited scholarship in relation to the impact that social network contracts have on the use of personal images. In particular, existing scholarship has focused on the way

---


98 For example, YouTube and Viacom third-party copyright infringement where people upload and reshar third-party copyright content; see generally Daniel Gervais, above n 1 ; 843 Gervais states that ‘the right to make private use of copyrighted material is considered fundamental in several EU copyright statutes and may have a constitutional basis in a number of other legal systems’; see further Julie E Cohen, ‘A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace’ (1996) 28 Connecticut Law Review 981; Mary Wai San Wong, above n 97.
that social networks use people’s information. Because the focus is on personal information, this scholarship has overlooked the protection of the use of personal images on social networks.

The scholarship looking at intellectual property and social networks has tended to focus on the use of third-party copyright on social networking sites.99 For example, Elkin-Koren argues that it is the fundamental ingredient of the means of producing and communicating content to the masses that enabled individual users to connect with each other.100 This primarily stemmed from the interactivity of digital networks as a result of the Internet, subsequently enabling a revamping of the production and distribution of creative works.101 Third party content was present before the internet or the phenomenon of digital networks as people were creating content in various forms of taking family pictures (or just pictures), telling stories, playing music and recording events (family) but disseminating the content was restricted.102

The scholarship in the United States is more extensive, as legal scholars became concerned that the development of photographic cameras were intruding into people’s privacy.103 Legal scholars Warren and Brandeis were concerned with the protection of people’s privacy as photography and photographic equipment evolved.104 Arguably, Warren and Brandeis attempted to protect image rights under the tort of privacy with the first landmark case to explore the right to privacy: Marion Manola v Stevens & Myers.105 Miss Manola was a theatre actor who objected to a photographer taking secret pictures of her in tights from his box for advertisements. The question, in this case, ignited scholars to consider ‘the rights of circulating portraits’.106 This played a pivotal role when questioning whether the law would recognise and protect the right to privacy.107 However, it was subsequent scholars who played a pivotal role

---

99 Niva Elkin-Koren, above n 1, 3–4,7. The author suggests that when people create content it is ‘often associated with the buzzword Web 2.0 which refers to social networks, media sites, collaborative initiatives and a variety of works created, remixed and exchanged by individual users’.

100 Ibid.
101 Ibid.
102 Ibid.
104 Ibid.
105 NY Supreme Court (15, 18, 21 June 1980), New York Times.
in establishing four different torts for protecting privacy in the United States.\(^\text{108}\) The right of privacy provides the right to be let alone, to live a life of seclusion and to be free from unwanted publicity.\(^\text{109}\) It protects four aspects of personality, which relate to a person’s name, history and image (likeness), and a common law protection of personal diaries, letters and eavesdropping.\(^\text{110}\) Despite the extensive scholarship centering on image rights in the United States, there is little clarity when considering how image rights are protected when used, shared and exchanged on social networks in Australia. This is because there are no known image rights upon which people can rely to protect their image, or subsequent use or misuse, when those images are shared online. The lack of image rights in Australia reflects limitations of Australian law to provide adequate protection for the use of personal images when those images are misused.

### 1.6 Overview of Social Networks

Social networks allow users to network and communicate with other users. There are many different types of social networks, which have different facets and tools for a user to share and exchange personal images, including Google+, Windows Live, MySpace, Bebo IMBD, Flickr, LinkedIn, Tumblr, YouTube, Photobucket, Twitter, Facebook, Pinterest and Instagram.\(^\text{111}\) While these social network platforms vary significantly in appearance, they all have a number of core features. These are profile, contacts, content/information and control (or access to control). For the purpose of the thesis, social network sites are taken to mean:

> Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.\(^\text{112}\)

---


\(^{110}\) Ibid.


\(^{112}\) See Danah M Boyd and Nicole Ellison above n 2, 211. While this definition has been widely accepted, it does not reflect the crucial role that personal information plays within a social network; nor does it
There are a number of key characteristics of a social network site. One key characteristic is the user’s profile. The profile influences how people communicate information, and how they interact and engage with other people within the social network. A profile contains information about users including their name, age, marital status, gender, likes and dislikes, education and friends/contacts. It may also include the names of other people users are connected to or wish to be connected to. Each person who is on a social network completes a profile, thus revealing information about themselves. This is irrespective of whether a person is creating content about themselves or another person. The information can take various forms, including images, videos, audios, written comments, posts, written information (such as likes, dislikes, about me) and combinations thereof.

A second feature of social networks is that they connect people. The networking function has a dual purpose of supporting the social network and allowing the user to establish connections with other users. This provides a link between one user and another user or multiple users. This is done by way of a ‘notification of request’, which may be accepted or ignored by the user. Accepted requests are added to a user’s contact lists, which may or may not be visible. The networking function also facilitates the sharing of information/content created by the users to their contacts on the social network. Profiles may contain links to a user’s friend’s profile. Through the profile function, users can view other users’ friends lists.

---

113 See generally Alessandro Acquisti and Ralph Gross, above n 1, 36.

114 This is not an exhaustive list; a more exhaustive list is provided in Chapter 2.

115 See Privacy Act 1988 (Cth), s 6(1) which defines personal information as: ‘Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.’ Contrast this definition with the ALRC’s view that the definition should be broader, or any combinations of written text, images, videos, posts, tags, links, etc.

116 See generally Leucio Antonio Cutillo, Mark Manulis and Thorsten Strufe, above n 25, 503.

117 Ibid.

118 Ibid.

119 Ibid.

120 Ibid.

121 See also Rebecca Wong, Social Networking: A Conceptual Analysis of a Data Controller [2009] 14(5) Communications Law 142, 143-4 <http://works.bepress.com/rebecca_wong/9>; ‘Data’ is the common term for how information is stored digitally: Privacy Act 1988 (Cth) NPP 9 (Schedule).
For example, Facebook’s ‘People You Know’ feature allows a user to view other users who are connected to their friends’ profiles. Twitter has follower lists and following lists showing who the person follows. Each social network has its own version of these features. All social networks provide a profile for people to create and allow the person to show their contacts, friends or followers.

Another key feature of social networks is that they facilitate the exchange of information. This is done by way of blogs, posts, emails, chat, uploading of videos, and images, wall-to-wall (Facebook) private messaging and notes. The most common way of communicating information is by a photograph and post. A post is a block of information comprised of written text, images, videos and links. This forms part of the main thread of the profile. Here the person, along with their contacts, can comment and interact with one another by depicting their own self as well as other users through posts, comments, image and video sharing. They can also link their own content to other users via features such as ‘tag’ or ‘like’ or ‘dislike’. The tag feature means that the person identifies another person through their content (and vice versa). Personal images that are shared on a person’s profile are stored on a social network. When people share personal images on a profile page, other information about a user may also be revealed such as the user’s identity, name, age, and address. It may also contain information of all of the user’s connections on their network and the information exchanged within the social network by all users.

Another key feature of social networks is the privacy settings that allow users to control who accesses their images. The privacy settings of a social network commonly determine how people’s profile information and personal images are shared with their friends and other users in the network. The privacy settings provide different levels of access to people’s images when uploaded on a profile page. From the privacy settings, people can also control whether their profile (along with its contents) is visible to and accessible by other users, and whether third

122 Facebook’s wall-to wall feature allows where a user to post a comment on another user’s wall.
123 This is not an exhaustive list. See Danah M Boyd and Nicole Ellison, above n 3, 213.
124 And any combination of written text, image, videos, or links.
125 Tagging is a feature better known in Facebook.
126 See generally Leucio Antonio Cutillo, Mark Manulis and Thorsten Strufe, above n 25, 503.
127 See further for an overview of general discussion about identity, James Grimmelman ‘Saving Facebook’ [2009] 94 Iowa Law Review, 1137, 1152; Alessandro Acquisti and Ralph Gross, above n 1, 36–58.
128 See generally, Leucio Antonio Cutillo, Mark Manulis and Thorsten Strufe, above n 25, 503.
129 Ibid.
parties have access to their content and posts. This is turn allows users to have some control over their profile within the network.

A social network’s contract terms also regulate the network’s privacy settings, which allow users to restrict access to their images. As will be shown, people’s ability to control their images depends on the network’s settings. When a user’s profile is restricted, control may be overridden by the social network’s default settings, which are public. This occurs, for example, in Facebook’s graph search because people’s information on their profile can be viewed publicly if their privacy settings are not changed. However, even if a user did restrict their individual privacy setting, they would still have very little control over the use of their images. This is because when a person uploads and shares an image on a profile page, that image is also subject to the privacy settings of third parties such as contacts/friends. One of the consequences of gaining access to a social network service is that people involuntarily relinquish control over their personal images because the contract terms are mandated by the social network.

One of the problems that I faced in developing the research question was the vast number of social networks that exist today. To make the project manageable, three social networks were selected: Facebook, Twitter and Instagram. The social networks were chosen in order to illustrate the different problems that arise when personal images are exchanged, used and shared within each network. These social networks were chosen because they each illustrate different problems that occur when personal images are shared, exchanged and used online.

The first social network that was selected was Facebook. It was selected because it demonstrates the problems that arise when users share, exchange and use images with their contacts. Facebook was launched in February 2004 and in January 2016 has more than 1.71 billion users. Facebook offers its users the ability to create a personal profile, add other

---

130 Ibid.
131 Ibid.
users as friends, receive automatic notifications when they update their profiles, exchange messages, have instant messaging, join common interest groups, and like fan pages that comprise workplace, organisations, schools or colleges.\(^{134}\) Users must register prior to using the site and use real names and information; they must also be at least 13 years old.\(^{135}\) Facebook has staked its claim to the number one position in the social network arena. This is due to its attractiveness for users to engage in a range of online communications such as chat, apps, games, uploading and sharing images, notes, videos and tagging.\(^{136}\) Facebook is the number one ranked social network with an estimated traffic of a billion people per month.\(^{137}\) Facebook was selected because it demonstrates the problems that occur when people upload images on their profile pages. In particular, it exemplifies the problems that arise when third parties reuse images that have been uploaded and shared by people on their profile pages.

The second network that was chosen was Twitter. Twitter was chosen because it highlights the problems that arise when users share personal images and third parties reuse those images. Twitter was launched in 2006 and currently has 1.3 billion registered users.\(^{138}\) It is a social networking and micro blogging service that allows users to send and receive short text-based messages up to 140 characters.\(^{139}\) The messages that are sent and received are called


\[\text{Facebook: http://www.facebook.com.}\]

\[\text{Ibid.}\]


\[\text{Adrianus Wagemakers, ‘There is a Possibility That the Quality of Twitter’s Users is Deteriorating’, (3 August 2015), Business Insider Tech http://www.businessinsider.com/twitter-monthly-active-users-2015-7?r=UK&IR=T.}\]

‘tweets’, and are publicly visible by default although the users can restrict the messaging delivery to their friends. The functionality works based on ‘following’: a user may follow another user without any reciprocity. Twitter’s function of establishing connections is similar to Facebook’s friends and friending; Twitter users ‘follow’ or have ‘followers’. A user creates a public profile, which has the user’s full name, location, web page and a short biography, and the number of tweets of the user. Users must register before they can post a tweet, follow or be followed.

The third social network that was chosen was the photo-sharing social network Instagram. Instagram is an image-sharing and hosting social network site that provides filters for ‘images’ and then allows people to share them on other social networks. Instagram was selected because it highlights the problems that arise when a third party uses personal images. Instagram enables users to capture an image on their mobile phone and then, using a filter, to enhance the image and share it via Instagram. Users can share their personal images via Facebook. Users on Instagram can upload photograms, share photos and follow other users. Recent new Instagram features are that users have a web profile, which contains biographical information, personal details, and personal images. Instagram was chosen because of its popularity, and because it allows people to share images across different social media sites, such as Facebook and Twitter.

---

142 See Twitter, It’s What’s Happening, https://about.twitter.com/company.
143 Instagram’s popularity has increased with over 30 million users in April 2012 and has been acquired by Facebook in 2012; Instagram, FAQ, https://www.instagram.com/about/faq/; see also Instagram, Instagram for Android – Available Now (3 April 2012) http://blog.instagram.com/post/20411305253/instagram-for-android-available-now.
144 Instagram, FAQ, https://www.instagram.com/about/faq.
Chapter 2
Terms of Use, Personal Images and Social Networks

2.1 Introduction

Contracts of service play an important role in shaping how personal images are used on social networks. Before a person is able to access a service, they must first accept the social network’s terms and conditions. When a person accepts a network’s terms of service, a contractual relationship is formed with the network provider. A social network’s contract is recorded in their terms of service, which are standard non-negotiable terms. Social network contracts usually contain a data/privacy policy along with provisions that stipulate how information (including images) is used by the network. This chapter examines the role that social network contracts play in regulating the use of personal images that are shared online.

In order to review the role that contractual terms play in protecting personal images, a range of different types of social network contracts was reviewed. This review revealed a number of things. First, while most social networks deal with similar issues, the name given to the contractual terms sometimes varies between different social networks. The review also revealed that while the language may differ between different social network contracts, most deal with similar issues such as privacy, content, variation, termination, disputes, disclaimers,

---

1 Click wrap contracts are the preferred vehicle for website owners to regulate access and use of online content. See ProCD Inc v Zeidenberg 86 F 3d 1447 (7th Cir 1996), where the United States court held that click wrap (shrink wrap) agreements were valid and enforceable contracts. See generally, Dale M Clapperton and Stephen G Corones, ‘Unfair Terms in “Click Wrap” and Other Electronic Contracts (2007) 35 Australian Business Law Review 152.

2 The industry term for an online contract is ‘terms of service’ or ‘terms of use’ or ‘terms’. Despite the different terminology, they are used interchangeably and are binding on parties who sign up to online services. Twitter uses the term ‘terms of service’ – see Twitter, Twitter Terms of Service (30 September 2006), https://twitter.com/tos?lang=en; Instagram uses ‘terms of use’ – see Instagram, Terms of Use (19 January 2013) <https://help.instagram.com/478745558852511>; Facebook’s terms are referred to in its Statement of Rights and Responsibilities – see Facebook, Statement of Rights and Responsibilities (30 January 2015) <https://www.facebook.com/legal/terms>.

3 The following are some of the standard terms that are contained in a social network: Privacy; Content; Amendments/variations; Termination; Disputes; Entire agreement; Indemnification; Disclaimer of warranties; and Jurisdiction.
intellectual property and data collection. In order to critically examine the impact that the contracts of service have on the use that is made of personal images online, the thesis will focus on those clauses that impact on how images are used. These relate to licensing, collection, use, disclosure and termination.  

Social network contracts regulate how personal images are shared online in a number of different ways. The first is that the contract will allow a network to use and reuse personal images that have been shared online. This occurs when a network is given a very wide licence to use, reuse and sub-licence personal images. As personal images are protected under copyright, the network must have permission to use and disseminate the images on the network. The second is when a network collects personal images. This occurs, for example, when a network collects personal images for marketing and advertising purposes. The third is where a network uses personal images that have been shared online. This occurs when a network encourages people to share images of other people on their network. For example, Facebook’s contract encourages people to share images of other people on their profile pages. Networks also encourage people to reshare or exchange personal images they do not own on the network. The fourth is when a network shares or discloses personal images – for example, when a network shares personal images with third-party affiliates for commercial purposes such as advertising. When this occurs, people’s images are exploited without any compensation to the person whose image is misused.

In looking at the role played by social networks in shaping how personal images are used online, the thesis focuses on three social network contracts: Facebook, Instagram and Twitter. These were selected for a number of reasons. The first is because they are the most popular networks that people use to share personal images. The second is because, while each of

4 While there are separate clauses that pertain to ‘content’ and ‘disputes’, I have addressed the ‘content’ clause under the licensing term. This is because the focus of the thesis is on the way that the use of personal images is regulated by social network contract.

5 This contractual term may contradict the network’s privacy settings. This may contradict people’s customised privacy settings for example a person has strict privacy settings, but people are still able to upload and share images of them. Instagram’s privacy terms are contradictory to the network’s features where personal images that are set to ‘private’, are still used and may be reused by third parties. This is similar to Twitter’s contractual terms and features where other users and third parties may misuse personal images that have been shared publicly.

6 See further Ebiz MBA, ‘15 of the Top Social Networking Sites’, eBiz (October 2106) <http://www.ebizmba.com/articles/social-networking-websites > . The site lists Facebook, Twitter and Instagram in the top 10 sites. Facebook ranked first, Twitter ranked second and Instagram ranked seventh.
these three networks has similar characteristics, they differ in terms of the ways in which personal images are shared and accessed online. The reason for this is that the networks have different settings that have ramifications for the way each network is able to use personal images shared online. A network has features that allow users to choose settings that enable the images that users share online to be viewed either publicly or privately (by restricting the images to a selected audience). The network’s settings may affect how the network and third parties use images that are shared online. Facebook was chosen because it is a semi-private network that allows people to choose various settings when sharing and exchanging personal images with their contacts; this means that a person can control access to their images. In contrast, Twitter was chosen because it is by default a public network; this means that anyone can view and access personal images that are shared on the network without restriction. Instagram was chosen because it is a semi-public network, which also allows people to choose limited settings when sharing personal images online. Where this occurs, they retain some ability to restrict access to personal images when shared online; however, this is very limited.

2.2 Licensing and Ownership of Personal Images

As most of the material that is uploaded, used and reused on social networks is protected by copyright, it is essential that the sites obtain permission to use images that are shared online. Typically, social network contracts include a licensing clause that facilitates the network’s use

---

7 Facebook has various privacy settings from which people can choose to share their images; when people share their images with their friends, and the images are reused, the image shared is subject to a third party’s privacy settings. Notably, Twitter and Instagram have limited privacy settings – public or private.

8 Twitter’s privacy settings are set to default or limited privacy settings. This is also the case with Instagram.

11 The content may be a combination of videos, images, audio or descriptive information, or just some of these types of content. It includes personal information that is provided by the user along with any combination in which it is expressed. The creation of images, videos or audio, along with the descriptive information that a user provides, falls under the definition of works in which copyright subsists in and is protected under the Copyright Act 1968 (Cth). The creation of a profile automatically demonstrates how personal information is authored and contributed by the person, which can take various forms of copyright due to the nature of copyright subsisting in works that may be created by amateurs. See Copyright Act 1968 (Cth), ss 10, 31(1), 32. Although there is argument about whether short text messaging is protected under copyright, I argue that it is not only the short text messaging but the combination in which it is expressed – for example, Twitter is a short text messaging which alone may not be protected by copyright however, the combination of the tweet with an image or audio would arguably be protected by copyright.
of personal images. The licensing clause plays a critical role in determining how the network is able to use the images that people share online. The permission is given at the time of joining a social network and is non-negotiable. This is important because, without a licence, the network is unable to use personal images and may be liable for infringement of copyright. Without a licensing clause, a social network would not be able to use personal images, including to publish or disseminate personal images on the network. There are significant ramifications in relation to the control networks can execute over personal images when people give a licence to a social network. The following section will look at the licensing clauses used by Facebook, Twitter and Instagram, and the impact they have on the way images may be used.

2.2.1 Facebook

Facebook’s Statement of Rights and Responsibility (SRR), Clause 2 states how the network treats personal images and any other information that people share online. Interestingly, this

---

10 There are two types of licence: exclusive or non-exclusive licences, which are either express or implied. Express licences enable the copyright owner of the photograph to grant an exclusive or non-exclusive licence over their photograph. The effect of an exclusive licence is that it gives the licensee (the person who has permission to use the licence over the photograph) the exclusive right to use the copyright work; see also Copyright Act 1968 (Cth), s 10, which states that ‘exclusive licence means a licence in writing, signed by or on behalf of the owner or prospective owner of copyright, authorizing the licensee, to the exclusion of all other persons, to do an act that, by virtue of this Act, the owner of the copyright would, but for the licence, have the exclusive right to do’, and ‘exclusive licensee’ has a corresponding meaning; see also Copyright Act 1968 (Cth), s 196(4).

11 The social network needs people’s agreement in order to use their images because images are considered to be content protected under copyright law. Chapter 2 discusses in detail how photographs are subject matter protected under copyright, and the copyright issues that arise with respect to ownership of photographs. As mentioned previously, only a creator or copyright owner has the right to share, disseminate and publish their images on a social network. A copyright owner can assign or license their copyright to a social network.

clause is contradictory. According to Facebook, all users retain ownership of their content.\textsuperscript{13} However, the contract contains qualifying sub-clauses that provide Facebook with a non-exclusive sublicense to their content and information. As sub-clause 2.1 provides:

For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and, application settings: you grant us a non-exclusive, transferable, sublicensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.\textsuperscript{14}

The effect of this sub-clause is to provide Facebook with a licence to use personal\textsuperscript{15} images royalty free. The licence term also provides Facebook with a ‘non-exclusive, transferable, sublicensable, royalty-free, worldwide’ licence over all the content, such as photographs and videos, posted by users on Facebook. This means that the network can use a person’s images without their permission. Essentially, Clause 2 provides that when people post images on the network, the images will be accessed in accordance with their privacy settings and with any applications that the user has used and/or is using.

Importantly, the licensing clause does not end if the user deactivates their account. If a person’s images are shared and then reshared with others, the licence is still in effect. This is because when a person terminates their social network account, the contract provides that the ‘IP licence ends when you delete your IP content unless your content has been shared with others and they have not deleted it’.\textsuperscript{16} The reality is that if a person’s photograph is reshared or reused by another user, the licence still operates.

\textsuperscript{13} See Facebook, Statement of Rights and Responsibilities Clause 2 (30 January 2015) <https://www.facebook.com/legal/terms> which states: ‘You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings’; see Van Alsenoy et al., above n 12.


\textsuperscript{15} For the purposes of the thesis, a user is a person who subscribes to a social network. Social network contracts refer to people who join the network as ‘users’.

2.2.2  **Twitter**

Twitter’s licensing clause is incorporated in Clause 5, ‘Your Rights’. This clause refers to copyright ownership of the content provided by users. Specifically, Twitter’s content term states:

> You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).\(^{17}\)

This clause varies slightly from the Facebook contract insofar as it explicitly states that the network is able to use any content that a person posts on the network. This includes any personal images that are shared on the social network. Clause 5 provides that the licence includes the right for Twitter to make:

> Content submitted to or through the Services available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use.\(^{18}\)

Twitter states that ‘all content whether publicly posted or privately transmitted is the sole responsibility of the person who originated such content’.\(^{19}\) This means that users are responsible for any possible infringement of copyright. The effect of this content term is that it also allows third parties and affiliates to use people’s images that are shared on the network. Twitter’s licence clause states that Twitter (along with third party affiliates) can use people’s images without compensating the people whose images are used. This means that people’s images can be reused, distributed, published or broadcast by third parties; this includes the network’s partners and other people who subscribe to the network. Like Facebook, Twitter’s licence for the use of images does not end when the contract ends. This is highlighted in the termination clause which states that certain clauses operate after a contract ends. For example,

---


\(^{19}\)  Ibid *Clause 4 Content on the Services*. 

---
Twitter can still make use of the content, even when people retain ownership of the images that they post on the service.

2.2.3 Instagram

Instagram’s licensing clause states:

Instagram does not claim ownership of any Content that you post on or through the Service. Instead, you hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub- licensable, worldwide license to use the Content that you post on or through the Service, subject to the Service’s Privacy Policy, available here http://instagram.com/legal/privacy, including but not limited to sections 3 (‘Sharing of Your Information’), 4 (‘How We Store Your Information’), and 5 (‘Your Choices About Your Information’). You can choose who can view your Content and activities, including your photos, as described in the Privacy Policy.20

While Instagram’s licence clause is similar to Facebook’s, there is more detail about how the content clause affects other standard clauses. For example, Instagram’s licensing clause operates subject to Instagram’s privacy policy, and the way that the network shares and stores personal images. As Instagram’s licence terms state that a person will give the network a ‘non-exclusive licence fully paid and royalty-free, transferable, sub-licensable, worldwide license to use’ personal images, the extent of the use depends on other terms in the social network contract.21 The licensing clause enables Instagram to publish and disseminate personal images that are shared on the network. This means that the network can use and publish any images that people share and upload. However, Instagram’s licensing clause is subject to other contractual terms – for example, in relation to privacy. Unlike Facebook and Twitter, Instagram’s termination clause is silent regarding whether the network is able to continue to use personal images.


21 Ibid including but not limited to sections 3 (‘Sharing of Your Information’); 4 (‘How We Store Your Information’); and 5 (‘Your Choices About Your Information’). You can choose who can view your content and activities, including your photos, as described in the privacy policy.
What is the Effect of the Licensing Clause on the Use of Personal Images?

The social network contracts examined above all use non-exclusive transferable, worldwide, royalty-free, sub-licensable licences to allow them to reproduce, communicate and publish the content that is shared by users on the network. This has important ramifications for how third parties are able to use personal images that are shared online. The consequences of a user granting a network a non-exclusive licence that is transferable and sub-licensable is that it allows the network to license the photograph to third parties for advertising and marketing purposes.\(^22\)

There are a number of problems with the licencing clauses used by Facebook, Instagram and Twitter. From the perspective of the person sharing images, the licence term facilitates the potential misuse of those images. This use potentially results in users losing their ability to control the use of the content that they share online. This means that when a user shares images on Facebook and those images are reshared, they will not be able to prevent third parties or Facebook from reusing those images. This is the case even if a user terminates their Facebook account.

2.3 Collection of Images

The network’s contract terms examined also allow the network to collect images that people share. A network collects the images that are shared in two situations: the first is when a person uploads and shares their images on their profile page; the second is when third parties share and upload images of other people online. In each situation, the effect is the same: the contract allows the network to collect the images that are shared online. This is the case even when the access to the images is restricted.

2.3.1 Facebook

Facebook’s SRR briefly outlines the network’s terms of service for users. Facebook’s privacy clause states that their users’ privacy is important to them.\(^23\) It also provides a link to Facebook’s data policy, which authorises how the network collects, uses and shares personal images that


\(^23\) See Facebook, *Statement of Rights and Responsibilities* (30 January 2015), [https://www.facebook.com/legal/terms](https://www.facebook.com/legal/terms) which briefly outlines the network’s terms of service for users to accept; however, within these terms users are expected to have read Facebook’s DP, which is provided as a link to click on in clause 1 of the Statement of Rights and Responsibilities privacy policy.
are shared online. Facebook’s data policy explains how Facebook generally collects information (including personal images) when people share images and when third parties share images of other people. The contract allows Facebook to collect the ‘content and other information that users provide when they use their services’.

The content collected by Facebook includes the information that a user has provided when signing up to the site, including their name, gender, email address, date of birth, photograph and/or phone number. This also includes subsequent information that the user has chosen to share, such as posting their status, status updates, the uploading of photos, sharing a story, likes, tag or comments on another user’s post or story. Essentially, Facebook will collect images that result from any interaction between the user and their networks and connections.

Facebook also collects metadata when users post photographs or videos on their profiles, such as the date, time and place the photographs were taken. Facebook also collects information when users access the service on different devices such as computers, mobile devices, tablets, amongst others.

---

24 See Facebook, Data Policy 1. What Kinds of Information Do We Collect? (29 September 2016), <https://www.facebook.com/full_data_use_policy>. The new DUP states that ‘We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.’; See Van Alsenoy et al., above n 12.

25 See Facebook, Information We Receive and How it is Used, Facebook Data Use Policy (29 September 2016), https://www.facebook.com/full_data_use_policy; see more recently the new Data Use Policy, Facebook, Data Policy 1. What Kinds of Information Do We Collect? (29 September 2016) <https://www.facebook.com/full_data_use_policy>; see also Van Alsenoy et al., above n 12.

26 See Facebook, Data Policy 1. What Kinds of Information Do We Collect? Your Networks and Connections (29 September 2016) <https://www.facebook.com/full_data_use_policy>. Here, Facebook states: ‘We collect information about the people and groups you are connected to and how you interact with them, such as the people you communicate with the most or the groups you like to share with. We also collect contact information you provide if you upload, sync or import this information (such as an address book) from a device.’ See also Van Alsenoy et al., above n 166. Facebook also collects information that other people provide when they use the service. See Facebook, Data Policy 1. What Kinds of Information Do We Collect? Your Networks and Connections (29 September 2016) <https://www.facebook.com/full_data_use_policy> where the DP states: ‘Things others do and information they provide. We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you, or upload, sync or import your contact information.’ In the previous DUP, Facebook provided more detail about the types of information it collected about users.
phones or tablets. When a user accesses their Facebook account, the network collects information that includes IP addresses, phone numbers, internet browser, pages that a user visits, operating systems, location and internet services. Facebook also collects information about its users from their affiliates and advertising partners, customers or third parties that help them to deliver advertisements and monitor their users’ online activities. In addition, Facebook collects information whenever users use the network or look at another person’s profile or timeline, use the graph search, like or search for a page, uses or clicks on pages within the network, clicks on people’s profiles or make purchases.

The consequence is that Facebook collects a vast amount of information from and about users from various sources. This enables Facebook to target and suggest services and features. Facebook’s contract allows it to collect personal images and use those images for advertising and marketing purposes, which increases the network’s revenue. The collection term also allows the network to exploit people’s images because the images are kept indefinitely until the network has no further use for them. This means that Facebook can retain images that have been collected indefinitely, even if those images are deleted or when a contract ends. In addition, Facebook’s collection term allows the network to obtain more information than people voluntarily provide, including people’s usage patterns, such as when they visit pages or check-in to places.

---

27 See Facebook, Data Policy 1. What Kinds of Information Do We Collect? Your Networks and Connections (29 September 2016) <https://www.facebook.com/full_data_use_policy>. Generally, the whole section outlines the information that Facebook collects from the user, what other people say about the user, how the user interacts with their connections, and networks and in particular, information about the device the user is utilising to access the service. Further, Facebook also collects information from third party websites and apps that use their services (specifically when a user visits other websites). Compare with the old Data Use Policy, Information We Receive and How it is Used (29 September 2016) <https://www.facebook.com/full_data_use_policy>; see Van Alsenoy et al., above n 12.

28 Facebook, Data Use Policy: Information We Receive and How it is Used (29 September 2016) <https://www.facebook.com/full_data_use_policy>.
2.3.2 Twitter

Twitter’s contract also allows the network to collect images when people use its service.29 Twitter’s contract governs the collection of personal images that are shared online.30 The contract provides that people consent to the collection of their images by their use of the Twitter service. This is different from Facebook because, from the outset, Twitter explains that users consent to the collection of their images by the service. Twitter’s contact outlines how the service will handle user’s personal images when they collect users’ information through various services such as various websites, SMS,31 APIs,32 email notifications, applications, buttons, widgets, ads and commerce services, and from partners and other third-party affiliates.33

Twitter’s contract states that the network is by default a public social network and designed to be shared with the world at large. As a result, the images that are collected by the network are publicly available. This means that photographs that users share, for example via tweets, following, lists and other public information, are essentially public. Twitter also collects any information that accompanies the images that are shared – for example, the metadata accompanying the Tweets, the time and location, along with users’ following lists and Twitter pages.34 While Twitter states that its service is by default a public network, users have the option

29 Clause 2 of Twitter’s terms of service agreement states that any information provided by users is subject to its privacy policy. Like Facebook, Twitter’s terms of use provide an external link to their ‘Privacy Policy’, which users are considered to have read and accepted at the time of subscribing. The clause effectively states that any information provided by users to Twitter is subject to their privacy policy; see Twitter’s Privacy clause 2, which states: ‘Any information that you or other users provide to Twitter is subject to our Privacy Policy, which governs our collection and use of your information. You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information, including the transfer of this information to the United States, Ireland, and/or other countries for storage, processing and use by Twitter. As part of providing you the Services, we may need to provide you with certain communications, such as service announcements and administrative messages. These communications are considered part of the Services and your account, which you may not be able to opt-out from receiving.’ Twitter, Twitter Terms of Service (30 September 2016) <https://twitter.com/tos?lang=en#content>.

30 Ibid Clause 2, Privacy.

31 Short messaging service.

32 API means Application Programming Interface.


34 Twitter, Twitter Privacy Policy, Information Collection and Use, Tweets, Following, Lists and Other Public Information (30 September 2016) <https://twitter.com/privacy>: ‘Most of the information you provide to us is information you are asking us to make public. This includes not only the messages you
to make their personal images private through the account settings. However, a person’s public information, such as public tweets, is searchable and transmitted through Twitter’s APIs to its third parties and services. As Twitter is a service that is public by default, people are aware that all information is public unless the user has selected otherwise in their privacy settings. The contract includes information that the user has shared, such as images, videos and links through Twitter.35 The clause allows users the choice of revealing their location information in their account settings. These terms provide users with the choice of ‘opting in’, as opposed to Facebook’s ‘opting out’. A differentiating point with Twitter is that users have the options of retaining more control over their information.

Twitter’s collection clause also allows the network to collect additional information that a user may provide on their Twitter page, such as their biographical details, location, website and photographs. Users can also provide mobile numbers for receiving SMS messages and to receive information from Twitter about services and marketing. A user’s privacy settings control how other users can contact them, whether it is by mobile phone number or email.36 Twitter states that any additional information provided in its ‘additional information’ clause is entirely optional.37 Twitter’s collection term also allows the network to collect images, which are shared for commercial purposes such as allowing third parties access to the images on the network.

2.3.3 Instagram

Instagram’s contract of service also allows the network to collect personal images.38 The network collects personal images that are shared online because the images that are shared are:

Subject to the Service’s Privacy Policy, available here http://instagram.com/legal/privacy, including but not limited to sections 3 (‘Sharing of Your Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information.’

‘For example, your public Tweets are searchable by many search engines and are immediately delivered via SMS and our APIs (http://dev.twitter.com/pages/api_faq) to a wide range of users and services. You should be careful about all information that will be made public by Twitter, not just your Tweets.’ See Twitter, Twitter Privacy Policy, Information Collection and Use, Tweets, Following, Lists and Other Public Information (30 September 2016) <https://twitter.com/privacy>

35 Ibid.
36 Ibid.
37 Ibid.
Like Facebook and Twitter, Instagram collects various types of information including information that people share, whether directly or by third parties. Instagram’s collection term also allows the network to collect images that have been shared, including additional information, whenever a person uses the service. For example, the network collects information about a person’s interactions on the service, such as when they use features to find friends, or by collecting log file information. In collecting people’s images, Instagram’s contract allows the network to use third-party analytics to gain further information about people’s use of the service. This means that the network collects more information about people than they provide. For example, Instagram collects information when people view images. Instagram also collects metadata about the user’s photograph, such as how, when and who collected the photo and how it was formatted. Interestingly, users can add metadata to their photographs by including a hashtag (marking key words when posting photographs) or geotags, which marks the location to the photograph posted. When Instagram collects metadata, the

---


40 The types of information collected are the information that users provide to Instagram directly when subscribing to an Instagram account. This will include profile information such as profile pictures as well as user content such as photos, videos and comments that users post to the service. There are also communications between Instagram and the users in relation to service-related information, such as updates, verifications and/or technical or security notices.

41 Each time users log into their Instagram accounts, log file information is automatically reported by users’ browsers – including each time they visit a web page or app. Instagram also collects and records log file information, such as: ‘When you use our Service, our servers automatically record certain log file information, including your web request, Internet Protocol (“IP”) address, browser type, referring/exit pages and URLs, number of clicks and how you interact with links on the Service, domain names, landing pages, pages viewed, and other such information. We may also collect similar information from emails sent to our Users which then help us track which emails are opened and which links are clicked by recipients. The information allows for more accurate reporting and improvement of the Service.’ Instagram, *Privacy Policy* (19 January 2013)< http://instagram.com/legal/privacy>.

42 Instagram uses third-party analytic tools to collect information sent by users’ device to Instagram, such as web pages users visit, add-ons and other information that ‘assists’ in improving the service.

43 Ibid.
contract allows the network to use cookies and other technologies like pixels and web beacons to collect information about how users use Instagram. The contract allows the network to provide information to third parties such as advertisers and affiliates, to enable them to serve advertisements or services to users’ devices that also use cookies. These identifiers can transmit information to third parties about how users browse and use Instagram in order to send users advertisements or content.

The effect of the collection clause in a network’s contract is that any time that people share or upload images online, the network will be able to collect those images. The network will be able to collect personal images that users share even if the images are subject to the network’s privacy settings. Social networks have different settings that relate to users’ privacy. The settings allow users to restrict access to their images; however, the user cannot restrict the network’s collection or access to those images.

A network such as Facebook has various privacy settings that allow people to restrict access to their images, which has consequences for the network’s collection of images. Facebook provides four different settings for users to share their personal images. A Facebook user can choose from: ‘public’, ‘friends of friends’, ‘friends only,’ or ‘only me’. There are different consequences for each setting. For example, when a person selects a public setting, anyone who is on the network can access this information (along with third parties). This extends to third parties who are not on Facebook by doing an internet search for the person’s name. When a person chooses restricted settings such as ‘friends of friends’, the setting allows third parties to access the users’ images. This contrasts to situations where a person selects ‘friends only’ or ‘only me’. When a user has highly restricted settings such as only allowing their friends to access their personal images, it may still result in third parties collecting the image. This is because when a person chooses ‘friends only’ to share their images, the shared images will be subject to the respective friends’ privacy settings. This often results in restricted images being accessed and used by third parties.

Twitter’s privacy settings are more limited than Facebook’s, as there are only two privacy settings: private or public. From the outset, Twitter states that some of the information the people provide, such as name and username, and profile page, is publicly available on the network.44 Twitter users have two options to select: public or protected. The protected option

---

44 See Twitter, Twitter Privacy Policy, Information Collection and Use, Tweets, Following, Lists and Other Public Information (30 September 2016) <https://twitter.com/privacy>. This clause states: ‘When you create or reconfigure a Twitter account, you provide some personal information, such as your name,
restricts access to the user’s followers. This means that the user’s tweets are ‘protected’ and cannot be searched, retweeted or quoted. Despite the settings, the privacy policy still enables Twitter’s third parties and affiliates to access people’s images. Instagram has similar privacy settings to Twitter: people can only choose public or private settings. However, all images will still be searchable or visible if other people have reshared them. Even though Facebook provides different levels of privacy settings, the network can collect the images despite the restrictions. Essentially, when people restrict access to their images, the collection term still allows Facebook and its affiliates and advertisers to use restricted images.

2.4 Use of Images

The three network’s contracts that were examined all contain terms that stipulate how the networks are able to use upload images. These include sharing the images with their affiliates for advertising and marketing purposes, and allowing third parties to use images that are shared online.

2.4.1 Facebook

Facebook’s Data Policy allows the network to use ‘all of the information’ it has to help it ‘provide and support’ its services. In particular, the policy allows Facebook to use personal images in the following ways:

- to provide, improve and develop services

username, password, and email address. Some of this information, for example, your name and username, is listed publicly on our Services, including on your profile page and in search results. Some Services, such as search, public user profiles and viewing lists, do not require registration.’


See Twitter, Twitter Terms of Service (30 September 2016), https://twitter.com/tos?lang=en, where Clause 10: Ending These Terms states that ‘in all such cases, the Terms shall terminate, including, without limitation, your license to use the Services, except that the following sections shall continue to apply: 4, 5, 7, 8, 10, 11, and 12’.

This is discussed in detail in the Facebook’s Data Policy.

This part of the Data Policy states that Facebook is ‘able to deliver our Services, personalise content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you’re connected to and interested in on and off our Services. We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friend tag you in a picture by comparing your friend’s pictures to information we’ve put together from your profile pictures and the other photos in which you’ve been tagged. If this feature is enabled for
to communicate with you\textsuperscript{49} \\
\begin{itemize}
\item to show and measure ads and services.\textsuperscript{50}
\end{itemize}

Facebook obtains a vast amount of information about users from various sources. This enables it to target and suggest services and features to users. In its Data Policy, Facebook states that that it uses the information it collects about users to ‘provide, improve and develop services’. In particular, the Data Policy states:

\begin{quote}
We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you’re connected to and interested in on and off our Services. We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friend tag you in a picture by comparing your friend’s pictures to information we’ve put together from your profile pictures and the other photos in which you’ve been tagged. If this feature is enabled for you, you can control whether we suggest that another user tag you in a photo using the ‘Timeline and Tagging’ settings.\textsuperscript{51}
\end{quote}

\textsuperscript{49} In this clause, Facebook can use people’s information to ‘send you marketing communications, communicate with you about our Services and let you know about our policies and terms. We also use your information to respond to you when you contact us.’ Available at Facebook, \textit{Data Policy} (29 September 2016) \<\texttt{https://www.facebook.com/about/privacy}\> ; see Van Alsenoy et al, above n 12.

\textsuperscript{50} See Facebook, \textit{Data Policy} (29 September 2016), \<https://www.facebook.com/about/privacy/\> ; see Van Alsenoy et al, above n 166.

\textsuperscript{51} Emphasis added: see Facebook, \textit{Data Policy} (29 September 2016) \<https://www.facebook.com/about/privacy>. Compare this with Facebook’s old policy, which stated that: ‘We also put together data from the information we already have about you, your friends, and others,
Facebook’s Data Use Policy states that Facebook can use the information that it receives about users through the features and services that the user and their friends use. It also provides that Facebook can also use information received through its partners, advertisers and developers that build applications on Facebook and the websites that users use. People’s images are prone to misuse by the network’s contract because it actively encourages their users and their friends to ‘tag’ them in pictures that the user’s friend has shared with the user in it.\(^5^2\) Facebook’s data use policy explicitly states that it may use the information that it receives about its users by ‘suggesting that your friend tag you in a picture that have uploaded with you in it’.\(^5^3\) In effect, the user not only gives Facebook a licence to use their images and videos; they also give the network a licence to use their information. Facebook acknowledges this in its data use policy under ‘I Information we receive and how it is used’.

### 2.4.2 Twitter

Twitter’s ‘use’ term allows the network to use personal images in various ways – for example, to tailor content to people. This is usually done when people share images, by tailoring and customising content, including ads.\(^5^4\) Twitter also collects information when people share their location, and uses information including log data to ‘improve’ the service. Twitter’s contract also provides the various ways that the network will collect and use any images that are shared, so we can offer and suggest a variety of services and features. For example, we may make friend suggestions, pick stories for your News Feed, or suggest people to tag in photos. We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you in which you might be interested. We may also put together data about you to serve you ads or other content that might be more relevant to you. When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services, like keeping your last GPS coordinates to send you relevant notifications. We only provide data to our advertising partners or customers after we have removed your name and any other personally identifying information from it, or have combined it with other people’s data in a way that it no longer personally identifies you.’ See Facebook, *Data Use Policy: Information We Receive and How it is Used* (29 September 2016), <https://www.facebook.com/full_data_use_policy>. See Van Alsenoy et al, above n 12.

Facebook has a ‘tagging’ feature that enables users to ‘tag’ other users in photographs that are uploaded and shared. Facebook, *Data Policy* (29 September 2016), https://www.facebook.com/full_data_use_policy#howweuse.

\(^5^2\) Ibid.

\(^5^3\) Ibid.

such as widget data, log data, location information, third-party affiliates, links and cookies. Twitter members are given more control over how the network monitors their usage. For example, people have the option of opting out by using a ‘do not track’ browser so that the network’s third parties do not have access to how users interact on the service.

2.4.3 Instagram

Instagram’s contract of service allows the network to use personal images in a similar way to Facebook and Twitter. For example, Instagram’s contract allows the network to use personal images to improve its service by using those images for marketing and advertising purposes.

What is the Effect of the Use Clause for the Use of Personal Images?

Social networks can use the images that are uploaded and shared on the network by sharing and disclosing the images to third parties. A network’s privacy/data policy enables a network to share and disclose personal images that are collected on the network. For example, when people share personal images on a profile page, the network is able to share and disclose those images to third parties. The use clause is essential to a contract because it allows the network to share users’ images with third parties. Third parties play a crucial role in Facebook, Twitter and Instagram’s contractual terms because the networks share users’ images with their third parties and affiliates for advertising and marketing purposes. For example, Twitter, Instagram and Facebook all use personal images for commercial purposes, such as when they allow a commercial entity to use personal images that have been shared online for advertising or marketing purposes. Essentially, the social network enables third-party advertisers to access its users’ pages to endorse their products through their ‘Sponsored Stories’ feature. This highlights the misuse of personal images that may occur when a network’s third party affiliates use personal images that have been shared.

2.5 Sharing and Disclosing

The social network contracts examined all contained clauses that enabled the social networks to share and disclose the images that users uploaded on their profile pages. When people join a

55 Ibid.
56 *Angel Fraley et al v Facebook Inc* CA No 511-01726. Facebook allowed developer applications access to people’s images in the sponsored stories feature. Facebook was sued for misusing its users’ profile pictures, information and likenesses because the network allowed users’ information to be exploited by advertisers to market their product.
social network, they agree that the social network can share and disclose a user’s personal images. The following section discusses the ways in which a network’s contract allows the network to use personal images when the images are shared online by sharing them with third parties and advertisers.

2.5.1 Facebook

In Facebook’s contract, the sharing/disclosure term allows the network to share the information (including personal images) the network collects with various third parties. The sharing and disclosure term provides that users can:

share and communicate with people they choose. For example, Facebook allows users to choose the audience who can access/see what users share. Users can select the audience when they share personal images, for example, they can select a custom group of individuals, all of their friends or a member of a group (if the user belongs to any). In the event that a user has a public profile then any information that is shared with a public audience will be ‘Public information’. This will include any information in a user’s public profile or content that is shared on Facebook pages or other public forums. Generally

---

57 Facebook, Data Policy: 2. How is This Information Shared? People You Share and Communicate With (29 September 2016) <https://www.facebook.com/full_data_use_policy#howweuse>. This clause states that ‘when you share and communicate using our services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your friends, or members of a group. Likewise, when you use messenger, you also choose the people you send photos to or message.’ See Van Alsenoy et al, above n 12.

58 Facebook, Data Policy: 2. How is This Information Shared? People You Share and Communicate With (29 September 2016) <https://www.facebook.com/full_data_use_policy#howweuse>. This clause states that ‘public information is any information you share with a public audience, as well as information in your public profile, or content you share on a Facebook page or another public forum. Public information is available to anyone on or off our services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV.’ See Van Alsenoy et al, above n 12.

59 Facebook, Data Policy: 2. How is This Information Shared? People You Share and Communicate With (29 September 2016) <https://www.facebook.com/full_data_use_policy#howweuse>. This clause states that ‘Public information is any information you share with a public audience, as well as information in your public profile, or content you share on a Facebook page or another public forum. Public information
public information (which includes personal images) are available to any person on or off the Facebook service and can be accessed by any person is any information you share with a public audience, as well as information in your Public Profile, or content you share on a Facebook Page or another public forum.\textsuperscript{60} Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV.\textsuperscript{61}

When members share and communicate with other people in their network, other users can download and reshare the content, whether or not the users are logged on to Facebook.\textsuperscript{62} Facebook also allows other people who use their service to share images and information about users with their connections. This is the case, for example, when a person shares a photograph of another person, mentions or tags another person at a location in a post, or shares information about a person that has been shared with them.\textsuperscript{60} Facebook encourages users and their friends to
share photographs and information about each other in various ways. One way that Facebook allows images to be shared and disclosed is via its ‘Tag’ feature. Tagging is a special type of link to a user’s timeline. Facebook’s ‘Tag’ feature is part of the Photos application, where users may ‘tag’ other users (friends) in a photograph. Facebook’s contract states that a tag ‘suggests that the tagged person add your story to their timeline. In cases where the tagged person isn’t included in the audience of the story, it will add them so they can see it. Anyone can tag another person in online images. Once a person is tagged in an image they are ‘visible’ (such as in News Feed or in search).’ For example, a user may upload photographs containing several friends and tag their friends within that photograph. Once a user is tagged, a notification goes to the user that they have been tagged, and provides a link to the photograph in which they are tagged. When users tag people in photographs, their images are disclosed to everyone who has access to those images. Facebook’s facial recognition technology uses facial recognition to identify people in photographs on its website. It also restricts the user’s control over how their image will be used and shared because the tagging itself does not restrict the image of the user from being re-shared or exchanged; it simply means that they can remove the ‘tag’. It does not provide any control over the image being shared, exchanged and tagged.

Facebook’s contract also allows the network to share and disclose an image when the use of the image is for commercial purposes. The clause states:

We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the

---

64 Wikipedia, List of Facebook Features (7 October 2016), <http://en.wikipedia.org/wiki/Facebook_features>


67 Ibid.

information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.69

Facebook’s contract also allows advertisers and third parties to access and use images that are shared on social network. Clause 9 of Facebook’s contract provides that the network is able to use and disclose personal images to third parties for commercial purposes.70 Consequently, the sharing and disclosure term allows Facebook to exploit personal images that are shared online. In particular, Facebook’s contract allows the network to use images uploaded on the network by sharing users’ images with Facebook’s third party affiliates for advertising, other commercial content and sponsored content.71 As was noted above, clause 9 of the Facebook


70 See Facebook, Facebook Clause 9.1 Facebook Statement of Rights and Responsibilities Advertising (30 January 2015) <https://www.facebook.com/legal/terms> which states: ‘You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.’; see Van Alsenoy et al, above n 166.

contract allows the network to share personal images with advertisers to sell and market their products for payment, without any compensation to the user whose image is being used.

2.5.2 Twitter

Twitter’s sharing and disclosure clauses state that the network may share or disclose personal images at their user’s ‘direction’, for example, when a person authorises third-party applications to access their account. As with Facebook, other people can disclose and share images of a user. This will occur when a third party mentions, ‘tags’ or shares images of a person. In terms of sharing users’ personal images, Twitter’s contract states that they may share a user’s personal image with third parties and affiliated service providers; this however, is subject to confidentiality obligations under Twitter’s privacy policy, and is conditional on the third parties using users’ personal data on Twitter’s behalf. A specific clause states that Twitter can share and disclose users’ non-private and non-personal data, such as public user profile information, tweets, following lists and followers.

2.5.3 Instagram

Instagram’s contract of service explicitly states that it will not ‘rent or sell’ users’ images to third parties outside of Instagram or affiliates without users’ consent, except ‘as noted’ in their policy. This is very different to both Facebook and Twitter’s policy of using people’s information because unlike Instagram, Facebook and Twitter’s contracts do not have any provisions about selling or renting users’ images. In contrast, Instagram states that it will not ‘rent or sell’ users’ information, which contradicts its Terms of Use Policy Rights clause 1: ‘Instagram does not claim ownership or any content that users post through the service.’ This is also contradicted in Instagram’s privacy policy clause, which outlines what happens in the event of change of control of the Instagram company. Facebook’s contract of service enables

---

72 The use of the word ‘consent’ means that the user must agree to the terms.
73 Ibid, Twitter’s privacy settings will control whether a person can be tagged on the service or not.
74 Ibid, Twitter’s terms of service, privacy policy.
75 Ibid, Followers and following lists are the people to whom the user is connected and/or chooses to follow.
76 Ibid, Clause 3. Sharing of Your Information (19 January 2013), http://instagram.com/legal/privacy, which states: ‘We will not rent or sell your information to third parties outside Instagram (or the group of companies of which Instagram is a part) without your consent, except as noted in this Policy.’
the network to assign its rights and obligations in connection with ‘a merger, acquisition, or sale of assets, or by operation of law or otherwise’, which is similar to Instagram’s terms of use. Clause 18 of the Instagram contract explicitly states that if Instagram sells or transfers part or whole of Instagram or its assets to another entity, ‘users’ information such as name, email address, users’ content and any other information collected through the service may be among the items sold or transferred’. However, users ‘will continue to own their user content’. This means that people will be able to use the content; however, their information may be sold or transferred if Instagram is sold.

Instagram has a similar ‘use’ clause to Facebook and Twitter. Clause 2 of the Instagram contracts states that parts of the Instagram service are supported by advertising revenue and may display advertisements or promotions and users hereby agree that Instagram may place such advertising and promotions on the Service or on, about or in conjunction with your content. The manner, mode and extent of such advertising and promotions are subject to change without specific notice to users.

*Effect of the sharing and disclosure on personal images*

Consequently, the effect of the sharing and disclosure term is that it allows networks to facilitate the use and misuse of personal images. This occurs in a number of different ways. The first is that the network may use images of third parties who are not members of the network, for example when a member uploads and shares an image of a third party who is not a member of the social network. When this occurs, the image that is captured and shared by the user may be subsequently used by the network without the permission of the person’s photographed. The second is that third parties can use personal images that are uploaded for advertising and

---


marketing purposes. This occurs when the network feature third-party applications that users may utilise to enhance the use of the service.\footnote{For example, this occurs when third party applications require more permissions and access to user’s information.} For example, the contract terms of the networks allow third parties, websites and affiliates to receive personal images that people post or share on the network.\footnote{See Facebook, Data Policy: 2. How is This Information Shared? People you Share and Communicate With (29 September 2016) <https://www.facebook.com/full_data_use_policy#howweuse> . This clause states: ‘When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.’; see Van Alsenoy et al, above n 12.} This allows the network to share users’ images with third parties and customers. The third is that people’s images are commercially exploited because this allows the network to give advertisers the use of people’s photographs to sell and market their product for payment, without any compensation to the user whose image is being used. The effect of this is that a network can use personal images without having to compensate people for the use of those images.

2.6 Termination

All of the social network contracts reviewed had standard termination terms. Generally, the termination clauses specify what will happen to a user’s images in the event that the user terminates their account. These provide that when the contract ends, certain clauses such as the licence clause will still operate. For example, Facebook’s terms of use states that the content, special provisions, and a clause termed as ‘other’ (which provides for miscellaneous clauses relating to the enforceability of the contract), advertising and dispute clauses still operate even if a user deletes or deactivates their Facebook account.\footnote{Facebook, Statement of Rights and Responsibilities: Clause 14; Terms of Use Clauses 2.2, 2.4, 3–5, 9.3, 14–18 (30 January 2015) <https://www.facebook.com/legal/terms> ; see Van Alsenoy et al, above n 12.} This is also the case for Twitter, where when a user terminates their account, the content and ‘Your Rights’ clauses will still operate.
The termination clause used by the social network reinforces the rights given to the network when users license their personal images to the network. Generally, the termination of a social network contract would result in the termination of the copyright licence; however, as highlighted above, this is not the case with Facebook, Instagram and Twitter contracts. From a user’s standpoint, this creates a problem in that it means a user is unable to prevent the misuse of their images once the images are shared online. It also means that even if a user terminates a social network contract, the licensing clause still operates so as to allow third party use of personal images – for example, to allow other people to reshare a person’s images online.

2.7 Conclusion

Contracts are critical to the scope and operation of social networking services. These allow the social networks to use the personal images that users upload to the sites. Social network contracts also allow networks to collect personal images and to share them with third parties.

One of the most important clauses in a social network contract is the licensing clause, which allows social networks to use images. When users give a licence to a social network, they give the network control over the images that they share online. This also allows the network to reuse those images for purposes other than those provided for in the licensing clause. The control that social networks have over the images uploaded by members is reinforced by the contractual clauses that deal with the collection, use and sharing of images. These clauses allow the network to control the use of images that are shared on the network. The termination terms found in the social network contracts also strengthen the control that networks are able to exert over images that are shared online. This is because the termination clause allows the network to use personal images (along with their other content) after the contract ends.

As we will see, the contractual provisions undermine the ability of legal scheme (or sphere?) such as copyright to assist in preventing against the misuse of images online.
Chapter 3

Copyright, personal images on social networks

3.1 Introduction

Over the last two decades or so, various web technologies and platforms—such as blogs, wikis, user-created sites, self-publishing sites, social bookmarking sites, content-sharing and social networking sites—have helped to create an environment in which personal images are routinely uploaded, shared and reused on the internet. The participative culture sparked by Web 2.0 in the late 1990s created a situation in which amateur creations began to populate the web on an unprecedented scale.1 The widespread online distribution, sharing, reuse and exchange of personal photographs created a number of problems for creators (and owners) of photographs, as well as for the people whose images are captured in those photographs. The aim of this chapter is to look at the potential role that copyright law might play in minimising or preventing this abuse. It also evaluates whether this protection is adequate.

When thinking about the role that copyright might play in preventing the misuse of personal images on social networks, it is important to distinguish between different interests. The first relates to the interests of people whose images are captured in those photographs; namely, the subjects in the photographs. Unlike the situation in some other countries, the subject of a photograph has no rights under copyright law in Australia.2 The second relates to the interests of the person who creates a photograph (or the person who subsequently obtains rights in those creations). This form of creation is typically protected by copyright law and is discussed in detail in this chapter.

There is little doubt that the type of photographs at issue here are protected by copyright law in Australia. It is clear, for example, that photographs are copyright subject matter:

---


2 Subjects in other countries for example, in the United States, any image rights or rights to publicity tend to protect celebrities and other famous people from use of their image. See Pollard v Photographic Company [1888] Chancery Division (North J Vol KL) where a photographer was restrained from selling or exhibiting any copies of the plaintiff’s image; see also Mansell v Valley Printing Company [1908] 1 Ch 567; ‘Marion Manola v Stevens & Myers NY Supreme Court’, New York Times (15, 18, 21 June 1890).
photographs expressly fall under the definition of ‘artistic works’ as defined in section 10 of the Copyright Act 1968 (Cth).\(^3\) Photographs also satisfy the requirement that to be protected by copyright, they must be recorded in a material form,\(^4\) that is they must be reduced in ‘writing or some other material form’.\(^5\) The requirement that to be protected a photograph must have a sufficient connection to Australia will also be easily satisfied. This is because connection with Australia is satisfied either when the person who took the photograph is Australian or the photograph was taken in Australia.\(^6\) Thus, when an Australian citizen subscribes to a social network and shares their photographs on their personal profile page, they satisfy the requirement of connection to Australia. There is also little doubt that photographs will satisfy the requirement of originality in Australia.\(^7\) This is because the requirement for protection in Australia is very low, originality

---

\(^3\) Hereinafter referred to as the Copyright Act. See Copyright Act (Cth) 1968 ss 89, 90,91, and 92. Section 10 (1) (a) defines a photograph as including a digital photograph, xerography or processes similar to photography such as survey plans. Photographs were protected under the Fine Arts Copyright Act 1862; see Lionel Bently, ‘Art and the Making of Modern Copyright Law’ in Daniel McClean and Karsten Schubert (eds), Dear Images. Art, Copyright and Culture (Ridinghouse, 2002) 331; Mark J Davison, Ann L Monotti and Leanne Wiseman, Australian Intellectual Property Law (Cambridge University Press, 3rd ed, 2016) 223.

\(^4\) Copyright Act 1968 (Cth) s 22(1); see Davison, Monotti and Wiseman, above n 3, 228.

\(^5\) As photographs are reduced to a material form when they are in physical or digital form, digital photographs will satisfy the requirement of material form, as they are reduced in digital form: Copyright Act 1968 (Cth) s 22(1).

\(^6\) Copyright Act 1968 (Cth) ss 32(4); see also, s 10.

\(^7\) The final threshold criteria for copyright protection of photographs is that the photograph must be original: Copyright Act 1968 (Cth) s 32(1). Originality in copyright law is a key issue that has been subject to much discussion in recent times. See Sam Ricketson, Megan Richardson and Mark Davison, Intellectual Property, Cases, Materials and Commentary (LexisNexis, 4th ed, 2009) 166-7. The meaning of ‘original’ was clarified by the 2009 High Court decision of IceTV v Nine Network Australia (2009) 239 CLR 458 where the High Court stated that authorship plays a central role when considering the requirement of originality in copyright law. The view that ‘authorship’ and ‘original work’ are correlative was illustrated in IceTV v Nine Network Australia (2009) 239 CLR 458, 473 [34] (French CJ, Crennan and Kiefel JJ). Subsequently the decision of Telstra Corporation limited v Phone Directories Company Pty Ltd (2010) 273 ALR 725 also considered the requirement of originality. See Alistair Abbott and Kevin Garnett, ‘Who is the Author of a Photograph?’ (1988) 20(6) European Intellectual Property Review 204; Simon Stokes, ‘Graves’ Case and Copyright in Photographs - Bridgeman v Corel’ in Daniel McClean and Karsten Schubert (eds), Dear Images: Art, Copyright and Culture (Ridinghouse, 2002) 109; Melville B Nimmer, Nimmer on Copyright (Matthew Bender, 1965), para 2.130 states that any or ‘almost any photograph may claim the necessary originality to support a copyright merely by virtue of the photographers personal choice of subject matter, angle of the photograph, lighting and determination of
will be satisfied by little more than the opportunist pointing of a camera and the pressing of the shutter button. As a result, the most elementary forms of a photograph, such as snapshots, will meet the threshold of originality. Photographs that capture the same subject matter will qualify for copyright protection. Thus when two people capture the same image of a family on vacation, each photograph is considered to be original and protected under copyright. As each person has expended labour, skill and originality in determining when to press the button on their camera to capture that particular scene, the work will be protected.

As the precise time when the photograph is to be taken. See Kathy Bowrey, Michael Handler and Dianne Nicol, *Australian Intellectual Property: Commentary, Law and Practice* (Oxford University Press, 2010) 59–60.

Nicholas Caddick, Gillian Davies and Gwilym Harbottle, *Copinger and Skone James on Copyright* (Sweet & Maxwell, 14th ed, 1999) para 3.104; Bowrey, Handler and Nicol, above n 7, 59.

See *Feist Publications Inc v Rural Telephone Service Co* (1991) 499 US 340 [10]. In *Burrow-Giles Lithography Company v Sarony* 111 US 53 (1884), the court emphasised the notion of author-photographer that was previously developed in *Nottage v Jackson* 11 QBD 627 (1883). The court, at 55 and 61, considered the question of human labour, specifically whether the efforts were deemed worthy of copyright protection and not merely ‘mechanical reproduction’. Having regard to the specific portrait of Oscar Wilde, the court focused on labour noting: ‘In regard to the photograph in question … it is a useful, new, harmonious, characteristic and graceful picture, and that plaintiff made the same … entirely from his own original mental conception, to which he gave visible form by posting the said Oscar Wilde in front of the camera, selecting and arranging the costume, draperies, and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade suggesting and evoking the desired expression and from such disposition arrangement or representation, made entirely by plaintiff he produced the picture in the suit.’ See Robert E Mensel, ‘Kodakers Lying in Wait: Amateur Photography and the Right to Privacy in New York 1885–1915’ (1991) 43 (1) *American Quarterly* 24.

See generally, Jane C Ginsburg, ‘No “Sweat”? Copyright and Other Protection of Works of Information After *Feist v Rural Telephone*’ (1002) 92(2) *Columbia Law Review* 338, 343-8. The originality requirement with respect to photographs is not stringent in Australia because originality according to the High Court is that the person who authors (captures) the photograph must have exercised some control over it and not have copied it from another work: *Telstra Corporation Limited v Phone Directories Company* (2010) 273 ALR 725.

Scholars have noted there is no distinction between photographs that are the result of pressing a button and other photographs that may be copies of other artworks or photographs. See Caddick, Davies and Harbottle, above n 8, para 3, ‘no reason of principle why there should be any distinction between the photograph which is the result of such a process and a photograph which is intended to reproduce a work of art such as another painting or another photograph’. Compare with Nimmer, who identifies two situations where questions of originality may arise. The first issue arises ‘where a photograph or other
can show that they have expended some degree of time, skill and labour in the capturing the photograph, the resulting photograph will be entitled to copyright protection.¹²

While there may be little doubt that photographs will be protected by copyright in Australia, there are still a number of hurdles that need to be addressed before copyright can be used to protect personal images. The first relates to the question of ownership: a matter which will play a role in determining how effective copyright law is in protecting a personal image that is uploaded online. The second relates to whether the unauthorised use constitutes an infringement of the owner’s rights in the photograph. These are examined below.

¹² See Caddick, Davies, Harbottle above n 8, para 3.104 who state that as long as the author has 'expended some small degree of time, skill and labour in producing the photograph (which may be demonstrated in by the exercise of judgment as to such matters as the angle from which to take the photograph, the lighting, the correct film speed, what filter to use, et cetera) the photograph ought to be entitled to copyright protection, irrespective of its subject matter'. See generally Bowrey, Handler and Nicol, above n 7, 59; see also Laddie, Prescott and Vitoria, Modern Law of Copyright and Designs (Lexis Nexis, 2nd ed, 1995) who also stated at para 3.104 that originality 'presupposes the exercise of substantial independence, skill, labour, judgment and so forth. For this reason, it is submitted that a person makes a photograph merely by placing a drawing or painting on the glass of a photocopying machine and pressing the button gets no copyright at all … It will be evident that in photography there is room for originality in three respects. First there may be originality which does not depend on creation of the scene or object to be photographed or anything remarkable about its capture, and which resides in such specialties as angle of shot, light and shade, exposure, effects achieved by means of filters, developing techniques … Secondly there may be creation of the scene or subject to be photographed … Thirdly a person may create a worthwhile photograph by being at the right place at the right time.'
3.2 Ownership

One factor that will influence a person’s ability to use copyright to protect against the misuse of their image captured in a photograph and uploaded online depends on who owns copyright in the photograph. While copyright will provide some protection where the owner and subject are the same person, the protection will be more tenuous in situations where the owner and subject are different people. Where the subject and owner are the same person the situation is straightforward. However, where copyright in a photograph is owned by someone other than the subject of the photograph, protection of the subject will depend on the goodwill of the copyright owner to bring an action on the subject’s behalf. Consequently, when personal images are misused on a social network, the effectiveness of copyright will depend on who owns copyright in the image.

3.2.1 Authorship

In thinking about who owns copyright in a photograph, a key principle of copyright law is that, with the exception of employees and commissioned works, the author is the first owner of rights in the image. In most cases, determining authorship is relatively straightforward; the person who takes the photograph will be the author and thus the owner of the resulting work. While in most situations authorship will present few problems, there are some situations, however, where problems will arise in determining who is the author of a work.\(^\text{13}\)

One situation where questions of authorship arise is where a person who owns a camera asks another person to take a photograph on their behalf: here the question arises as to whether ownership of the equipment gives them some rights over the resulting photograph. Another situation where problems arise is where a person directs, organises and orchestrates a scene but does not push the button; here the question arises as to whether the organiser can claim authorship of the resulting photograph. Questions also arise where an image is captured by automated or mechanical equipment. Another situation where questions of authorship arise is where it is difficult to locate or identify the owner of a photograph (‘orphan works’). Each of these situations will be addressed below.

\(^\text{13}\) When people take photographs of themselves, it is unlikely that questions of authorship will arise because it is clear who the author is as they are the person who captured their own image. People taking photographs of themselves are exercising skill, labour and effort in capturing the photograph.
3.2.1.1 Camera Ownership

One situation in which questions about authorship may arise is when a person gives a third party the equipment (e.g. camera or phone) to capture an image on their behalf. This would be the case, for example, when a tourist asks a stranger to use their camera to take pictures of them while on holidays. Under Australian law, as the third party is pressing the button (or shutter), they are prima facie considered to be the author of the photograph. This is regardless of the fact that the third party does not own the equipment used to take the photograph. As a result, the person who owns the equipment that is used to capture a photograph taken by a third party is unlikely to have a claim of the copyright in the resulting photograph.

Having said this, it is possible that the owner of the camera may still be able to claim copyright in a photograph taken on their camera by a third party. It could be argued, for example, that someone who asks another person to take a picture of them is potentially commissioning the photograph and, as such, may have a claim to authorship in the photograph. This will depend on whether when asking a third party to take a photograph on their behalf the camera owner is in fact commissioning the photograph. While ‘commissioned’ is not defined in the Copyright Act 1968 (Cth), Copinger suggests that it means ‘order’. According to Copinger, the meaning of ‘order’ goes beyond merely requesting or encouraging; there must be a mutual obligation to ‘create work and an obligation to pay’. For a work to be commissioned, it is essential that there be valuable consideration. This would suggest that where a person merely asks a third party to take a photograph of them, it would not constitute a

---

14 Generally, where a photograph is commissioned first ownership is provided to the photographer taking the photograph. For works created prior to 1998, the general rule was that the author, not the commissioner, held first copyright; this could be varied by an assignment under contract. There are exceptions to first ownership of commissioned photograph when the photographs are commissioned for a private or domestic purpose such as portraits and engraving see Copyright Act 1968 (Cth) s 35(5); so even if a person was commissioned to take photographs of another person’s wedding or family portraits or pictures on the street, the people who ask for the photograph to be taken are the rightful owners – see Douglas & Ors v Hello Ltd & Ors [2005] EWCA Civ 595 (18 May 2005).

15 See Caddick, Davies and Harbottle, above n 8, 275; see also Plix Products Ltd v Frank M Winstone (Merchants) [1986] FSR 63, 86, where the court held that ‘in s 9(3) of the Copyright Act 1962 (NZ) “commissioning” means more than requesting or encouraging. It means ordering and connotes an obligation to pay not just for the finished products if and when they are produced but for the very article in which the copyright resides irrespective of whether any of the finished products are purchased’.

16 See Caddick, Davies and Harbottle, above n 8, 275; see further Ultraframe (UK) Ltd v Fielding [2003] EWCA Civ 1805, 30.
commissioning. This is because there is no obligation to pay the third party to take the photograph.  

It could also be argued that when a camera owner asks a third party to take a photograph of them, the stranger gives the camera owner an implied licence to use the resulting photograph. The courts use an objective test to determine whether an implied licence has been given. An implied licence may be oral and arise because of the circumstances in which the camera is used. When a licence is gratuitous and informal, the photograph is supplied knowing that it will be used for a particular purpose – namely for the enjoyment and use of the person who requests it. Given that where a third party takes a photograph on another person’s behalf, the photograph is taken knowing that the photograph will be used by another person, there is little to no expectation of ownership of the photograph.

3.2.1.2 Directing, Arranging and Controlling a Scene

Another situation in which problems of authorship potentially arise is when a person directs, arranges and controls a scene, but does not press the button that captures that scene. A recent example of this arose at the 2014 Oscars when Ellen DeGeneres asked Bradley Cooper to use her phone to take a group photograph of her and other celebrities at the awards ceremony. DeGeneres arranged the scene but directed Cooper to take the photograph (by pressing the button on her camera-phone). When Associated Press wanted to share the now famous selfie the question arose: who had the rights in the photograph?

---

17 Copinger, 275, states that ‘while well-known personalities will often agree to their photograph being taken, even in a studio, without any commission by them being made, this is less likely to happen in the case of people in the ordinary walk of life, since in the latter case the photographer is unlikely to take the risk of no prints being ordered.’ See Caddick, Davies and Harbottle, above n 8, 275. See Sasha Ltd v Stonesco (1929) 45 TLR 350.

18 See Caddick, Davies and Harbottle, above n 8, 309; see also Express Newspapers Plc v News (UK) Ltd [1990] FSR 359 where it was arguable that there was ‘a trade custom between newspaper publishers that one newspaper was free to reproduce news stories appearing in another’.


20 See Caddick, Davies and Harbottle, above n 8, 309; Trumpet Software Pty Ltd v Ozemail (1996) 34 IPR 481, 500.

21 Trumpet Software Pty Ltd v Ozemail (1996) 34 IPR 481, 500; see Caddick, Davies and Harbottle, above n 8, 309.

22 See Elana Zak, ‘Ellen DeGeneres’s Epic Oscar Selfie Becomes Most Retweeted Tweet’, The Wall Street Journal (2 March 2014); Melville v Mirror of Life [1895] 2 Ch 531, where the court essentially examined the role of author who had not operated the photographic equipment. While the son had been operating
Copyright law in the United States suggests that there is scope for Degeneres to argue that Bradley Cooper was carrying out her direction and instruction in taking the photograph. In contrast, under Australian copyright law, where a person does not take the photograph but plays merely a role in staging and arranging the photograph, they will have no claim to authorship in the resulting photograph. Applying Australian copyright law to the Oscar selfie, even though Ellen Degeneres staged the photograph, the copyright owner would be the person who took the photo; namely Bradley Cooper.

### 3.2.1.3 Where There is No Human Involvement in the Creation of a Photograph

Problems of authorship also potentially arise when personal images are captured without human intervention. For example, when a photograph is taken using a self-timer or when a non-human (such as an animal or a machine) takes a photograph.

Self-portraits began to be used in the 1880s with the introduction of shutters and self-timers. The advancement of cameras created the ability to self-time. The camera itself is taking the photograph without a person needing to press the button to take the photograph. With the evolution of technology, people have been able to take self-portraits as well as group shots without actually pressing a button, by directing timers to automatically capture a photograph. When photographs are taken by self-timers, issues of authorship may arise because the photograph is taken without human labour, skill and effort. However, there is a potential

---


25 This view is also reaffirmed in the Oasis case; Creation Records Ltd and Others v News Group Newspapers Ltd [1997] EMLR 444.

26 See Nottage v Jackson (1883) 11 Q.B.D 627, 632; Burrow-Giles Lithography Company v Sarony 111 US 53 (1884) 59, 60.
argument that the person who sets the timer and positions the camera would be the author of the photograph.\textsuperscript{27}

Another situation where questions about copyright ownership of a photograph arise is where a non-human takes a photograph. The so-called ‘monkey selfie’ highlights the problem that arises in this situation. In the summer 2011, the photographer David Slater had been travelling in Indonesia taking pictures of a crested black macaque monkey when one of the monkeys took his camera and started to take several ‘selfies’ by pressing the button.\textsuperscript{28} The question here was whether there was an author of the monkey selfie. Under Australian copyright law, only humans qualify as a person under section 32(4) of the \textit{Copyright Act 1968} (Cth), which states that a qualified person is an Australian citizen, or Australian protected person or an Australian resident. Given this, an animal would not be the author of the photograph.

Another situation where authorship may be an issue is where a photograph is created automatically, for example by a traffic camera which records speeding infringements or by a CCTV.\textsuperscript{29} Reflecting of the close connection that exists between authorship and originality, the fate of an automatically generated work will depend on whether the work is original.\textsuperscript{30} As the Full court noted in the \textit{Telstra} decision, an automatically generated work would not quality for protection because it was not original.\textsuperscript{31} This was on the basis that originality requires independent human intellectual effort to generate the material work in question, something that

\textsuperscript{27} See generally \textit{Nottage v Jackson} (1883) 11 Q.B.D 627, 632; \textit{Burrow-Giles Lithography Company v Sarony} 111 US 53 (1884) 59, 60.

\textsuperscript{28} Steve Schlackman, ‘The Telegraph is Wrong About the Monkey Selfie’ (7 August 2014) \textit{Artslaw Journal} <http://artlawjournal.com/telegraph-wrong-monkey-selfie>.

\textsuperscript{29} A recent example illustrates how CCTV can capture personal images that can later be shared on the internet and social networks. The image of an airline flight attendant who was drunk and sleeping outside the airline employee accommodation was captured on CCTV and then shared by the vice president of the airline company to the employees. John Hutchinson, ‘Qatar Boss Shames ‘Drunk’ Air Stewardess by Emailing Photo of Her Slumped on Floor Outside Accommodation to Airline Staff’ \textit{Daily Mail} (17 March 2015) <http://www.dailymail.co.uk/travel/travel_news/article-2998774/Qatar-Airways-boss-shames-drunk-air-stewardess-emailing-photo-slumped-floor-outside-accommodation-airline-staff.html>.


\textsuperscript{31} \textit{Telstra Corporation Pty Ltd v Phone Directories Company Pty Ltd} [2010] FCAFC 149, [90], [101], [169]; Jani McCutcheon, above n 30, 925.
would not be present where a work was automatically generally by for example, CCTV. While the operation of a computerised process involves skill, judgement and labour, it would not meet the threshold of originality and as such, not likely to be protected by copyright.

3.2.1.4 Orphan Works

Another issue that is important here relates to situations where an author cannot be identified or located, that is so-called orphan works. A work is considered to be an ‘orphan work’ when a diligent search is conducted but the copyright could not be found. The inability to identify or locate the owner of a photograph poses problems because people who wish to use the image cannot attribute authorship or gain the copyright owner’s permission to use the image. In itself this is not really a matter of concern to the subject of a photograph. What is a potential problem, however, is when governments intervene to deal with the problems created by orphan works. This is the case, for example, in the United Kingdom where the British government introduced the 2013 Enterprise and Regulatory Reform Act. The Act aims to facilitate the use of orphan works for commercial purposes by allowing the images to be placed in collective licensing schemes. A person who carries out a diligent search may obtain a license to use an orphan

---

32 Telstra Corporation Pty Ltd v Phone Directories Company Pty Ltd [2010] FCAFC 149, [101]; Jani McCutcheon, above n 30, 925.
33 See generally, Susi Frankel, ‘The Copyright and Privacy Nexus’ (2005) 36 Victoria University of Wellington Law Review 507, 517-8. Frankel 517 argues that a ‘plaintiff could argue that the placing of the video camera and possibly even its operation involved skill, judgment and labour. These are the hallmarks of the test of originality for the subsistence of copyright. The counterargument would be that these skills alone are not enough because if they were it would allow a very low threshold of originality.’
34 If there was protection, it could be argued that as traffic light cameras and CCTV are government operated and owned, the Crown may have ownership of the photographs. See generally Stephen M McJohn, Intellectual Property: Examples and Explanations (Aspen Publishers, 2nd ed, 2006) 21. However, there is uncertainty as to whether this view would be successful as this issue has not been tested in Australia.
36 Enterprise and Regulatory Act 2013 (UK).
37 Andrew Orlowski, 29 April 2013, UK Gov Passes Instagram Act: All your pics belong to everyone now <http://www.theregister.co.uk/2013/0429/err_act_landgrab/>; see also Ethan Stallman ‘Twitter users stripped off rights to own snaps’, 29 April 2013
photograph for non-commercial and commercial purposes. In this situation there is little that the subject of an image can do to prevent the (mis)use of the photograph. Online social commentators have suggested that such schemes strip social network users of their rights to their photographs. Consequently, where the scheme applies, people will have a limited ability to prevent the misuse of their image. While Australian copyright law has not been reformed to deal with orphan works, photographs that have been uploaded and reshared by third parties may fall within the British scheme.

3.3 Exceptions to the author as first owner

As was noted above, the ability to use copyright to protect against the misuse of personal images placed on social networking sites will depend, in part, on who owns copyright in the photograph. As a general principle, the photographer as author is considered to be the first owner of the copyright in the photograph. There are a number of exceptions to this general principle that may affect the owner’s ability to use copyright to prevent the misuse of a personal image online. The most important relates to photographs created in the course of employment (particularly by journalists), and where a photograph is commissioned.

It is generally recognised that where a photograph is taken in the course of employment that the employer will be the owner of the copyright (however it should be noted that this may be modified contractually). To determine whether a photograph is owned by an employer it is important to consider two questions: the first is whether the creator of a photograph is an employee; the second is whether the photograph was created in the course of employment.

38 See generally, Eleonora Rosati, above n 38, 725-740.
39 Ethan Stallman, ‘Twitter users stripped off rights to own snaps’, 29 April 2013
40 Copyright Act 1968 (Cth) s 35(2); see also Davison, Monotti and Wiseman, above n 3, 239.
41 Copyright Act 1968 (Cth) s 35(6).
42 See Davison, Monotti and Wiseman, above n 3, 243.
43 Copyright Act 1968 (Cth) s 35(6).
44 See Davison, Monotti and Wiseman, above n 3, 244.
In thinking about whether an individual is an employee, a number of factors will be taken into consideration including the nature and scope of the creator’s duties, whether the creator was being paid, the hours of employment, and whether the creator is entitled to holidays. While in some cases, the fact that someone exercise control of another person is suggestive of an employer-employee relationship, this may not be the case when a person exercises a higher degree of skill and expertise in their duties.

It is also necessary to consider whether the photograph was created in the course of employment. This is important because the employer will not always own copyright in a work that is created by an employee. For example, an employee who takes a photograph while on a lunch break potentially retains copyright in the image. This is because:

the mere existence of the employer/employee relationship will not give the employer ownership of inventions made by the employee during the term of the relationship and that is so even if the invention is germane to and useful for the employer’s business. This is also the case even though the employee may have made use of the employer’s time and resources in bringing the invention to completion.

In determining whether a photograph was created in the course of employment, it is important to look at the terms of the relevant employment agreement and on the nature of the employment activities that the employee is expected to perform. As Moore J. noted in EdSonic v Cassidy the question of whether a work is created according to the terms of employment ‘is not the bare question of whether the author is employed under a contract of service, at the time a work is made but whether the relevant work is made in furtherance of the contract of employment with the employer.’ The key question is ‘did the employee make the work because the contract of employment expressly, or impliedly required or at least authorised the work to be made?’

---

45 See Insight SRC IP Holdings Pty Ltd v Australian Council for Educational Research Ltd (2012) 211 FCR 563; see Davison, Monotti and Wiseman, above n 3, 244.
46 See Davison, Monotti and Wiseman above n 3, 244.
47 See Redrock Holdings and Hotline Communications v Hinkley (2001) 50 IPR 565, 21 citing Denning LJ’s test in Stevenson Jordan & Harrison Ltd v MacDonald & Evans (1952) 69 RPC 10; see Davison, Monotti and Wiseman, above n 3, 244.
49 (2010) 189 FCR 271.
3.3.1 *Photographs Created by Journalists*

Questions of ownership also arise in relation to photographs created by journalists. Section 35(4) provides special rules for literary, dramatic or artistic works that are created for journalistic purposes.\(^{51}\) Where the work is created on or after 30 July 1998 both the publisher and the journalist have copyright in the photograph.\(^{52}\) In all other cases, the photographer will be the owner of the copyright.\(^{53}\)

3.3.2 *Commissioned Photographs*

Generally, where a photograph is commissioned, first ownership is given to the person who takes the photograph.\(^{54}\) Prior to 1998, the general rule for commissioned photographs was that copyright vested in the photographer. The person commissioning the photograph did not acquire copyright in the photograph unless the author agreed under contract. However, the law relating to commissioned works changed in 1998, specifically in relation to commissioned photographs, portraits and engravings.\(^{55}\)

Under the current law, where photographs are commissioned for a private or domestic purpose, ownership rests with the commissioner.\(^{56}\) For example, with wedding photographs and family portraits, the copyright rests with the commissioner as opposed to the photographer.\(^{57}\) This means that if a photographer was commissioned to take photographs of a wedding or a family portrait, the person who commissioned the photograph would be the rightful owner.\(^{58}\) This means that when a photographer is commissioned to take pictures, they

---

\(^{51}\) *Copyright Act 1968* (Cth) s 35 (4); Davison, Monotti and Wiseman, above n 3, 246.

\(^{52}\) There are special rules that apply to photographs created for publication in newspapers, periodicals or magazines; see *Copyright Act 1968* (Cth) ss 35(4) and 35(7). Copyright rests with both journalist and media proprietor for works that are created after 30 July 1998 and for works created prior to 30 July 1998, the media proprietor of the employed journalist will own copyright; see Davison, Monotti and Wiseman, above n 3, 245–6.

\(^{53}\) In such circumstances, these journalists are unlikely to fall within the exception provided under the *Copyright Act 1968* (Cth) s 35(4).

\(^{54}\) For works prior to 1998, the general rule was that the author held first copyright not the commissioner; this could be varied by an assignment under contract; see Davison, Monotti and Wiseman, above n 3, 245–6.

\(^{55}\) *Copyright Act 1968* (Cth) s 35(5).

\(^{56}\) Ibid.

\(^{57}\) Ibid s 35(7).

\(^{58}\) See *Douglas & Ors v Hello Ltd & Ors* [2005] EWCA Civ 595 (18 May 2005).
are unable to use those photographs on their website or other social network sites without the permission of the people who commissioned the photograph. It is important to note that commercial photographers often contract out of the commissioning provisions. Where this occurs, the photographer can upload and share the photographs that have been commissioned by third parties on social network sites.

3.3.4 Contract

When thinking about the effectiveness of copyright in protecting against the misuse of a person’s image, it is important to note that the law allows copyright in a photograph to be contractually transferred to a third party.\(^\text{59}\) As discussed in Chapter Two, people enter into a contractual agreement with the social networks and website companies when they subscribe to their services. Before a person can access the social network service they must accept the social network’s terms of use. Once a person agrees to the social network’s terms of use, they are bound by those terms. As was shown in Chapter Two, social network contracts typically contain standard licencing clauses that give the networks a licence the images that people upload on their profile page. The licence clauses also often give the network an irrevocable and non-exclusive licence to sub-licence the user’s image to third parties. The agreements also allow networks to continue to use the images even if a person withdraws their consent or deletes their account. As a result, a copyright owner will have little recourse against the social network or the network’s affiliates that they sub-licence to. Despite this, a copyright owner would still have a right of action against an independent third party who appropriates an image from a social network site.

3.4 Is Use of the Photograph on a Social Networks an Infringement?

A key factor that determines the effectiveness of copyright in controlling online misuse is whether the unauthorised resharing and reuse of the photograph on a social network constitutes an infringement. A copyright owner is given a number of rights by section 31 of the Copyright Act.\(^\text{60}\) The key rights are the right to reproduce, communicate, and publish the photograph.\(^\text{61}\) It

\(^{59}\) Copyright Act 1968 (Cth) s 35(3).

\(^{60}\) Copyright Act 1968 (Cth) s 31.

\(^{61}\) Ibid s 31(1)(b).
should be noted that these rights are subject to any contractual agreements which the copyright owner enters in. The owner of a photograph is given the right to reproduce the photograph in a material form. The right to communicate a photograph to the public essentially means that the owner can make the photograph available online. The owner of a photograph has the exclusive right to publish the photograph. A photograph is published if the reproductions of the photograph have been supplied to the public by sale or other means. Publication means that the public is able to visually read the work. The right to publish a photograph means that the owner can post, upload or share the photograph on the internet or allow third parties to do so. Photographs are published on social networks when a person uploads and shares the photograph with their contacts in the network. A photograph is also published when it appears on the network or on a person’s profile page.

In most cases the uploading, sharing or reuse of a photograph will constitute an infringement of copyright. A photograph that is reproduced, published or communicated to the public without the requisite permission will be a direct infringement of the copyright owner’s right. Copyright in a photograph will also be infringed when a third party (such as a friend of a friend) reshares or reuses the photographs shared on the person’s profile page, or when a third-party advertising site reuses the photographs.

While in most situations the reuse of an image online will be a clear infringement, the situation is less clear where someone uses photograph enhancing tools such as Photoshop to

---

62 For example, a reproduction of photograph is deemed to have occurred where the work is converted from hard copy (physical form) to a digital form: s 21 (1A), Copyright Act 1968 (Cth) this also would include computer programs, or works derived from the source code; see Davison, Monotti and Wiseman, above n 3, 240.

63 Copyright Act 1968 (Cth) s 10(1), defines communicate as ‘make available online or electronically transmit (whether over a path, or a combination of paths, provided by a material substance or otherwise) a work or other subject-matter, including a performance or live performance within the meaning of this Act’.

64 Copyright Act 1968 (Cth) s 29.

65 Copyright Act 1968 (Cth) s 29(1)(a).

66 Ibid s 29(3).

67 An example of third-party infringement is when Facebook was sued for allowing advertisers to use their users’ profile pictures, information and likenesses in order to promote and market their products see Angel Fraley et al v Facebook Inc (C A No 511-01726). This occurred through the sponsored Stories feature in Facebook; at that time, Facebook’s terms of use did not allow them to do this. These terms of use have subsequently been amended and are examined in Chapter 2.
distort or modify an image. In this situation to infringe, there needs to be a similarity between
the photograph and the infringing photograph. The similarity must not be relative to the idea
expressed, but to the way in which the work is expressed; to the material form of the work.68
Where a work has been altered, it must be shown that the defendant’s unauthorised act was
carried out in relation to a substantial part of the work.69 This will depend on the quantity and
quality that has been taken which in turn depends on the facts of the case.70 As there is no set
definition of ‘substantial part’ in the Copyright Act, it is done through the development of
various tests over time, which has enabled the courts to consider the meaning of ‘substantial
part.’ The various factors considered by the courts to determine the meaning of substantial part
relate to quantity and quality. In IceTV v Nine Network Australia Pty Limited the High Court noted
that the ‘quality of what is copied is critical.’71

3.5 Fair Dealing

While there are a number of defences to copyright infringement that are potentially relevant
where images are shared online, the most relevant is the statutory defence of fair dealing. While
fair dealing is important in so far as it allows third parties to utilise and build upon published
works, it also puts the interests of the subject at risk. Here, we see again that the law is called
on to balance the rights of the owner against the rights of the public to use the work.

If the defendant can show that the dealing was carried out for one of the permitted
purposes and the use is fair, it will not be copyright infringement. There is a two-step approach
when considering whether the defence of fair dealing will apply to the use of a personal image
captured in a photograph. The first is to consider whether the use falls within one of the
permitted uses. The second is to consider whether the use is ‘fair’.72

68 Copyright Act 1968 (Cth) ss 36(1), 36(1A); see Ricketson, Richardson and Davison, above n 7, 222, 224–
5, 238–9; see Davison, Monotti and Wiseman, above n 3, 278–9.
69 Ibid. The reasoning for this lies at maintaining a balance between creative freedom of creators and the
protection of original works as recognized in IceTV v Nine Networks Australia Pty Limited (2009) 239
CLR 458, 473, [30], 509, [155], 512, [170]; Hawkes & Son (London) Ltd v Paramount Film Service [1934]
Ch 593.
70 Quantity and quality are not considered in isolation; see further IceTV v Nine Network Australia (2009)
239 CLR 458, [30], [155], [170]; Hawkes and Son (London) v Paramount Film Service [1934] Ch 593,
604; EMI Songs Australia Pty Ltd v Larrikin Music Publishing Pty Ltd [2011] FCAFC 47 [57].
71 (2009) 239 CLR 458, 473, 509, 512, [30], [155], [170].
72 Copyright Act 1968 (Cth) ss 40–43.
For the fair dealing defence to arise, the dealing must fall within one of the permitted purposes, namely for:  
- research or study  
- criticism or review  
- reporting news  
- professional advice given by a legal practitioner or patent attorney, and  
- parody or satire.

The most relevant of these is where the use is for the purpose of criticism or review, reporting of the news, or for the purpose of parody or satire. These are discussed in turn.

### 3.5.1 Criticism or Review

The *Copyright Act* provides that fair dealing of a photograph will not be an infringement where the work is used for the purpose of criticism or review and the use is fair. Copinger defines ‘criticism’ as ‘the act or art of analysing and judging the quality of the literary or artistic work,’ the act of passing judgment as to the merits of something, or a critical comment, article or essay. In turn ‘review’ is defined as ‘a critical article or report as in a periodical, on some literary work, commonly some work of recent appearance; a critique.’ In Australia, criticism and review have been given dictionary definitions, essentially the purpose of criticism may be considered as ‘the critical application of the mental faculties,’ while review is viewed as the ‘results of a process’.

---

73 Davison, Monotti and Wiseman, above n 3, 318–20.
74 *Copyright Act 1968* (Cth) ss 40, 103C.
75 Ibid ss 41, 103A.
76 Ibid ss 42, 103C.
77 Ibid s 43(2).
78 Ibid s 41A.
79 Fair dealing for the purpose of research or study falls outside the scope of this thesis.
81 Kevin Garnet, Gillian Davies and Gwiym Harbottle, *Copinger and Skone James on Copyright* (Sweet and Maxwell, 2011) 567; see also, *De Garis v Neville Jeffress Pidler Pty Ltd* (1990) 18 IPR 292, 299.
82 Ibid, see also, *De Garis v Neville Jeffress Pidler Pty Ltd* (1990) 18 IPR 292, 299.
83 Garnet, Davies and Harbottle, above n 81. See also, *De Garis v Neville Jeffress Pidler Pty Ltd* (1990) 18 IPR 292, 299.
Whether the use of an image is for the purpose of criticism or review will depend on whether the criticism is balanced or strongly expressed. For the defence of criticism and review to apply the criticism or review must be of a ‘work’ or ‘performance of a work,’ which is construed broadly. Criticism or review is not restricted to the style or merit of the work but can also extend to thoughts, ideas or the doctrine of philosophy behind the work. Importantly, for the infringement to fall within the fair dealing of criticism or review, the review or criticism must be of the photograph and not for another purpose, such as education. It does not matter that there are dual uses so long as one of these critiques the photograph.

3.5.2 Reporting News

The Copyright Act also provides an exception to copyright infringement where the use of the photograph is for the purpose of reporting the news. One important preliminary question is whether using a photograph falls within the reporting of the news at all. This is because it may be argued that using a photograph of a person is not reporting the news per se, but rather using the photograph to illustrate the news. Copinger suggests that in the United Kingdom,
photographs are excluded from the ambit of the fair dealing defence of reporting news. This is because ‘the use of photographs in the context of news reporting could never be fair.’ In Australia, the use of images may fall within reporting of the news.

While in many cases it is relatively easy to determine when a use is made for the purpose of reporting the news, in some cases it may be difficult to determine whether the something is done for the purpose of reporting the news. This is particularly the case with ‘infotainment’ programs. This is made all the more difficult by the fact that the reporting of the news may be humorous. An example of the fragile line that exists between reporting the news and entertainment relates to the naked image of Prince Harry partying at a Las Vegas hotel on vacation that was published on an entertainment website and then reshared by online news sites. While it is unclear how the photograph was shared and by whom, it was clear that as the owner of the photograph, they had the right to publish, reproduce and communicate it. In this case, the subject of the photograph – a naked Prince Harry – had very little control over the use of his image.

3.5.3 Parody or Satire

If the dealing of a photograph is for the purpose of satire or parody and it is fair, it will not be an infringement. The defence of fair dealing for the purpose of parody or satire is one of the

---

91 Garnet, Davies and Harbottle, above n 81, 572.
92 Ibid.
93 See De Garis v Neville Jeffress Pidler Pty Ltd (1990) 37 FCR 99; see Davison, Monotti and Wiseman, above n 3, 314-5.
most important for the purpose of this thesis.\textsuperscript{97} Parody or satire is not defined in the Act, but has been said to support free speech, criticism and public debate.\textsuperscript{98} The parody defence may apply when all or part of the original photograph is reproduced.\textsuperscript{99} The courts may use an objective test when determining whether the use of a personal image falls within the parody or satire exception.\textsuperscript{100} Even though parody and satire have been used interchangeably,\textsuperscript{101} there are important distinctions that must be considered. For the exception to apply to personal images, the use of the image must be ‘genuinely for the purpose of parody or satire and be fair in all the circumstances.’ To fall within the scope of the parody defence, it is not enough to merely use humour, there must be some form of commentary for the use of the defence to apply.\textsuperscript{102} There are a number of factors that may be taken into consideration in working out whether the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{97} Copyright Act 1986 (Cth) s 41A.
\item \textsuperscript{98} Attorney-General and Department of Communications and the Arts, Proposed Moral Rights Legislation for Copyright Creators, Discussion Paper (1994) 3.66; see Davison, Monotti and Wiseman, above n 3, 315–16.
\item \textsuperscript{99} This is because ‘a parody is an imitation of a work that may include parts of the original. In some cases, a parody may not be effective unless parts of the original are included.’ See generally Parodies, Satire and Jokes, Information Sheet G083v05, Australian Copyright Council, (March 2017) \url{<http://www.copyright.org.au/acc_prod/ACC/Information_Sheets/Parodies__Satire_and_Jokes.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0ece4f4e>}; See also Fair Dealing: Information Sheet G079v06, Australian Copyright Council, (March. 2017) \url{<http://www.copyright.org.au/find-an-answer/(select “Fair Dealing: What Can I Use Without Permission (G079v06)”)}>.
\item \textsuperscript{100} Mariko A Foster, ‘Parody’s Precarious Place: The Need to Legally Recognize Parody as Japan’s Cultural Property’ (2013) 23(2) Seton Hall Journal of Sports and Entertainment Law 313, 328, where the author states that, ‘the court must conduct an objective assessment of how and why the material is used. In the case of parody or satire, the court will first determine whether the copyright user is genuinely using material for parody or satire. This is somewhat difficult because the legislation left parody and satire undefined, and Australian courts have not yet considered either term’.
\item \textsuperscript{101} Conal Condren, Jessica Milner Davis, Sally McCausland and Robert Phiddian, ‘Defining Parody and Satire: Australian Copyright Law and its New Exceptions: part 2-Advance Ordinary meanings’ (2008) 13(4) Media Arts Law Review 401, 406. There the authors state parody and satire ‘are so frequently work together that dictionary definitions and common usage often treat them as conjoined, even partly interchangeable.’
\item \textsuperscript{102} Fair Dealing: Information Sheet G079v06, Australian Copyright Council, (March. 2017), available at \url{<http://www.copyright.org.au/find-an-answer/ (select “Fair Dealing: What Can I Use Without Permission (G079v06)”)}>; see also, Mariko A Foster, above n 100, 327-28.
\end{itemize}
\end{footnotesize}
exception potentially applies, including whether the image is published, ‘the nature of the material, the nature of the use,’ whether permission has been granted by the copyright owner.\textsuperscript{103} While parody is not defined in the \textit{Copyright Act}, Spence suggests a definition that ‘tracks the ordinary usage of the term in a sufficiently broad range of contexts to render it useful for the purposes of legal analysis’.\textsuperscript{104} It is noted that any definition of parody must go beyond ‘dictionary definitions which restrict parody,’\textsuperscript{105} In line with this, Condren et al suggest that an ordinary meaning of parody be formulated:

which may then co-exist with, but remain distinct from, satire: parody is the borrowing from, imitation, or appropriation of a text, or other cultural product or practice, for the purpose of commenting, usually humorously, upon either it or something else.\textsuperscript{106}

As the Australian Copyright Council states, ‘the purpose of a true parody is to make some comment on the imitated work or on its creator.’\textsuperscript{107} In order to rely on a defence of parody, there would need to be commentary on the work or on the author of the photograph. In situations where television presenters comment on personal images in an entertainment show, the use may fall within the scope of the defence because the critique is a form of commentary.\textsuperscript{108}

While satire is also not defined in the \textit{Copyright Act} it has been suggested that satire that ‘may be defined, by extension from the definition of the satiric, as: those artistic expressions created in the satiric mode or idiom; the artistic results (usually humorous) of

\begin{flushleft}
\textsuperscript{103} See Mariko A Foster, above n 100, 328.
\textsuperscript{105} Ibid, there the authors state ‘any useful contemporary definition of parody must go beyond the dictionary definitions which restrict parody to a comic critique of its models and are shaped too much by narrowly literary concerns.’
\textsuperscript{106} Ibid.
\textsuperscript{108} Parodies, Satire and Jokes, Information Sheet G083v05, Australian Copyright Council, (March 2017) <http://www.copyright.org.au/acc_prod/ACC/Information_Sheets/Parodies_Satire_and_Jokes.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0ecf4ef>
\end{flushleft}
expression of such a critical impulse.' The Australian Copyright Council argues that the purpose of satire is:

to draw attention to characteristics or actions – such as vice or folly – by using certain forms of expression – such as irony, sarcasm and ridicule. It seems that both elements are required: the object to which attention is drawn (vice or folly etc.) and the manner in which it is done (irony, ridicule etc.).

Satire essentially requires two factors; the first is to draw attention to the form of the work, and the second is to use various forms of expression, such as sarcasm, ridicule or irony in order for the use to fall within the fair dealing. The use of personal images in social media and entertainment shows will usually fall within this fair dealing defence. This is because in most cases personal images are reused with satiric commentary or ridicule, for example in infotainment shows where intention of the commentary is to ridicule the subject in the photograph. As a result, in these cases the owner will not be able to prevent third parties from using the photograph.

3.5.4 Is the use fair?

The second factor that is required to determine whether the use falls within the fair dealing defence is whether the use is fair. In thinking about whether the dealing is fair, Lord Denning said:

[It is] impossible to define what is ‘fair dealing’. It must be a question of degree. You must first consider the number and the extent of the quotations and the extracts. Are they altogether too many and too long to be fair? Then you must consider the use made of them. If they are used as a basis for comment, criticism and review, that may be a fair

---

109 Conal Condren, et al, above n 101, 413; see also The Macquarie dictionary which defines “Satire” as: 1. the use of irony, sarcasm, ridicule, etc. in exposing, denouncing, or deriding vice, folly etc. 2. a literary composition, in verse or prose, in which vices, abuses, follies etc. are held up to scorn, derision, or ridicule. 3. the species of literature constituted by such composition. This definition is also used by the Australian Copyright Council, Parodies, Satire and Jokes, Information Sheet G083v05, (March 2017) <http://www.copyright.org.au/acc_prod/ACC/Information_Sheets/Parodies__Satire_and_Jokes.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0eceef4ef>


111 See Davison, Monotti and Wiseman, above n 3, 317. The authors suggest that while ‘it is difficult to determine how “fair” is to be judged’ what will be fair will depend on the circumstances of the case.
dealing. If they are used to convey the same information as the author, for a rival purpose, that may be unfair. Next you must consider the proportions…. But it must be a matter of impression.112

Justice Conti adopted a similar view when he said that ‘fair dealing involves question of degree and impression: it is to be judged by the criterion of a fair minder and honest person, and is an abstract concept’.113 The courts will consider ‘fairness’ objectively with respect to the relevant purpose. This means that the ‘purpose of criticism and review must be fair and genuine for the relevant purpose’.114 While section 40 of Copyright Act provides a list of the qualitative factors that may be taken into consideration when determining whether the use is fair, the list is specific to fair dealing for the purpose of research and study. For the other types of fair dealing, a variety of factors must be taken into account including ‘whether the work is published,’ ‘the degree which the infringing work competes with the exploitation of the copyright work by the owner and the extent of the use and the importance of what has been taken,’115 and ‘the amount taken, the motives and consequences of the dealing.’116

3.6 Can Moral Rights Can Prevent the Misuse of Personal Images?

In addition to the copyright given to the author of a photograph, Australian law also provides authors with moral rights. Moral rights are personal rights of the authors or creators of works. This means that authors will have moral rights regardless of whether they own copyright in the work. There are three different types of moral rights in Australian copyright law. These are the right of attribution of authorship,117 the right of integrity of authorship118 and the right to prevent false attribution.119 Moral rights will generally not protect the subject in a photograph where the image is uploaded and reused online. However, where the author and subject are the same person, moral rights may be used to prevent the misuse of the image.

---


114 Ibid 381, also affirmed on appeal TCN Channel Nine Pty Ltd v Network Ten Pty Ltd (2002) 118 FCR 417.

115 See Garnet, Davies and Harbottle, above n 81, 574-5.


117 Copyright Act 1968 (Cth) s 193.

118 Ibid s 194(1).

119 Ibid s 194(2).
Before looking at the rights in detail, it should be noted that there are two important limitations to the operation of moral rights. The first is that it is not an infringement of attribution or integrity if the treatment or act was ‘reasonable in all circumstances’. What may be ‘reasonable in all circumstances’ will depend on the conduct of the parties in the given circumstances. While the Copyright Act does not define ‘reasonable’, it does provide a number of factors that may be taken into consideration when determining whether the treatment is reasonable in all circumstances. One factor that may be relevant relates to the nature or type of work. Photographs created by professionals may be treated differently to works created by amateurs. Other factors that may be taken into account include the purpose (whether public or private or commercial or non-commercial), the manner and the context of the use. The Copyright Act does not provide ‘guidance as to how the reasonable factors are to be balanced against each other’. Thus it is left up to the courts to decide how to balance the factors which depend on the circumstances of each case.

The second limitation on moral rights is that authors are able to consent to acts that would be otherwise be an infringement of their moral rights. In many jurisdictions, moral rights are considered to be inalienable rights. While in these jurisdictions an author can assign their

120 Ibid ss 195AR (2), 195AS (2).
123 Copyright Act 1968 (Cth) ss 195AR(2)(c), 195AS (2) (c). See Davison, Monotti and Wiseman, above n 3, 341.
124 Copyright Act 1968 (Cth) ss 195AR(2)(d), 195AS (2) (d). See Davison, Monotti and Wiseman, above n 3, 341.
125 As a result, if the work is used for commercial gain or for a commercial purpose, it may not be reasonable: S Ricketson and C Creswell, The Law of Intellectual Property: Copyright, Designs, and Confidential Information (LBC Information Services, 2nd ed, 1999) 10.15, 10.175; see Davison, Monotti and Wiseman, above n 3, 341. As was shown in chapter two, a social network’s contract terms allow third parties to reuse and repost uploaded photographs. Given that social network sites comprise of individuals and companies to have an online presence; it may be the case that the court would also consider the community standards of the social network in the absence of an ‘industry’ code. The court may also take into account whether the image was used by an individual for private purposes; such as resharing or reposting the image on their personal profile page.
126 Davison, Monotti and Wiseman, above n 3, 340.
copyright in a work to a third party, they cannot transfer their moral rights.\textsuperscript{127} However, in Australia authors are able to consent to acts that would otherwise infringe their moral rights.\textsuperscript{128} When authors consent to acts that would be otherwise an infringement of their moral rights, they will be unable to rely on their moral right to prevent the misuse of the image.\textsuperscript{129} In order to consent to acts that would otherwise be infringing of an author’s moral rights, consent must be in writing.\textsuperscript{130} The consent must be ‘genuinely given by the author.’\textsuperscript{131}

It is important to note that social network terms of use do not usually contain provisions on moral rights. Despite this, one question that arises is whether an author consents to acts that would otherwise be an infringement of their moral rights when they sign up to a social network. This is because as the licence clause is very broad it may be deemed a waiver of their moral rights.\textsuperscript{132} While this is possible, it is unlikely that a court would construe the clause as a waiver because the clauses do not refer to acts that would be otherwise be an infringement of moral rights.\textsuperscript{133}

3.6.1 The Right of Attribution

The right of attribution provides authors with the right to be attributed as the creator of the work.\textsuperscript{134} This means that an author of a photograph should be attributed whenever the image is reused by third parties. The right to attribution is important because resharing a photograph on a social network potentially obscures the identity of the author. The author of an artistic work has the right to be identified as the creator of a work where that work is reproduced, communicated or exhibited to the public.\textsuperscript{135} In the event that a third party allows another person

\textsuperscript{127} Ibid 342.
\textsuperscript{128} W Rothnie, ‘Moral Rights: Consents and Waivers’ (2002) 20 Copyright Reporter 145; for further discussion, see Davison, Monotti and Wiseman, above n 3, 333–35.
\textsuperscript{129} Ibid 342-3, where the authors suggest this is because in situations where the author gives consent, the consent must relate to specific acts or omissions ‘or classes or types of acts or omissions.’
\textsuperscript{130} Davison, Monotti and Wiseman, above n 3, 342.
\textsuperscript{131} Ibid.
\textsuperscript{132} Ibid 343, the authors suggest that where ‘a broad consent is given, a waiver of moral right is effectively granted.’
\textsuperscript{133} This was highlighted in Monte v Fairfax Media Publications Pty Ltd [2015] FCCA 1633 which considered an infringement of moral rights when the plaintiff uploaded an image of his wife that was reused by a third party.
\textsuperscript{134} Copyright Act 1968 (Cth) s 193.
\textsuperscript{135} Ibid s 194(2); Snow v Eaton Centre Ltd (1982) 70 CPR (2d) 105 (Ontario High Court).
to use the work without attributing the author of the work, the use will be an infringement of the right to attribution. This is exemplified in *AFP v Morel,* which arose after Morel, a freelance photojournalist, posted eight photographs he had taken of the 2010 Haiti earthquake to his twitter account. Lisandro Suero copied the images and posted them on his own twitter profile which Agence France-Presse (AFP) found and disseminated to Getty Images (Getty US). Getty then used and shared the photographs widely without Morel’s permission. The court found that AFP and Getty failed to properly attribute Morel as the author of the images because the images were credited to AFP/ Getty/ Suero. The situation would be the same in Australia.

There is no prescribed method of identification: any method that is reasonable is sufficient. The core stipulation is that the author is clearly identified. Essentially, the author’s identity will be clear if it is included on the reproduction, copy or adaption of the work and that it is noticeable on the reproduction, adaption or copy of the work. In social media, photographs are not really credited to the author when those images are uploaded and reshared. This is because images that are posted online are often stripped of the author’s identity which make attributing the author of the image difficult. One question here is whether resharing images online without attribution would be reasonable in the circumstances. It is not usual practice to attribute the author when resharing an image on a social network like Facebook, as

---

136 *Copyright Act 1968 (Cth)* s 195AO.
137 10 Civ. 02739 (AJN) (S.D.N.Y Jan 14 2013).
139 *AFP v. Morel*, 10 Civ. 02730 (AJN) (S.D.N.Y. Jan. 14, 2013). The images had been licenced to third parties for commercial purposes for example, to CNN and Washington Post. Consequently, AFP and Getty were found to have infringed Morel’s copyright and he was awarded 1.2 million dollars.
140 *Copyright Act 1968 (Cth)* s 194(1).
141 Ibid s195AA; the case of *AFP v Morel* 10 Civ. 02730 (AJN) (S.D.N.Y. Jan. 14, 2013) in the United States provides an example of false attribution, which is an abuse of the photographer’s moral rights because in this case, from the onset of the infringement, AFP had originally attributed the photographs to Mr Suero. See David Becker, *Could the Morel v AFP/Getty Case Rewrite the Rules of Licensing Negotiation?* PetaPixel, (29 January 2014) <http://petapixel.com/2014/01/29/morel-v-afpgetty-case-rewrite-rules-licensing-negotiation>
142 *Copyright Act 1968 (Cth)* s 195AB.
there is a perception that images that are uploaded on a social network may be used without attribution. Consequently, it can be argued that because it is a common practice for ordinary people not to attribute who the author is when resharing an image, the use of the image may be reasonable.

### 3.6.2 The Right of Integrity

The second moral right is the right of integrity of authorship, which provides that authors have the right for their work not to be treated in a derogatory manner. When personal images are altered or distorted the author’s right of integrity may be infringed when an author is the subject of a photograph. In this situation, the right of integrity may prevent the misuse of the image. In contrast, when an author and subject of a photograph are different, the right to integrity will be of little assistance to a subject of an image. In this situation, the subject will depend on the goodwill of the author to bring an action on their behalf.

A key issue is whether there is a ‘treatment’ of the work. ‘Treatment’ of a work has been interpreted as ‘any addition to, deletion form or alteration to or adaptation of the work.’ A treatment of a work may arise where the image is used contrary to the way that the author intended the image to be viewed. Copinger suggests that ‘treatment’ that ‘covers a broad

---


145 Copyright Act 1968 (Cth) s 195AI (1), (2).

146 Copyright Act 1968 (Cth) s 195AK.

147 See Copyright Act 1968 (Cth) s 195AZB, where photographers are able to sue for infringement of their moral rights. In addition, they are also able to protect their reputation using alternative legal means such as defamation or passing off. This may pose difficulties regarding amateur photographers being awarded damages for infringement of their photographs on social networks. This is due to the commercial reality of not being able to demonstrate loss of income generated from the sharing of photographs on social networks.

148 See Garnett, Davies, and Harbottle, above n 81, 728. In particular, treatment does not apply to a ‘substantial part of a work but to any part of it’.

149 See for example, the image of a child posing with Hilary Clinton in the presidential campaign. The image was turned into various memes that contained vilification, and offensive captions. See Colby Itkowitz, ‘A Photo of a 4yr old with Hilary Clinton was used as a disgusting meme. Her mom fought back’, The Washington Post (1 December 2016) <https://www.washingtonpost.com/news/inspired-
spectrum of possible acts carried on a work, from the addition of a single word to a poem to the destruction of the entire work'.  

Another issue here is what is meant by ‘derogatory’. What is derogatory in this context depends upon whether the use is a ‘distortion or mutilation of the work or is otherwise prejudicial to the honour or reputation of the author.’ When a photograph is altered and/or is taken out of context (such as adding captions to the original photograph), the use may be ‘derogatory’. To some extent the question of whether a treatment is derogatory will depend on the nature of the work and the experience and skill of the author. This can be seen, for example, in Monte v Fairfax Media Publications, where the plaintiff sued for infringement of moral rights after the defendant reused an image that had been taken from the plaintiff’s wife’s social media account. Consequently, the defendant’s reuse of the image drew attention to the plaintiff’s wife’s escort business which was not known to her children or family, thus causing the plaintiff’s wife embarrassment and pain. Despite this the court did not find there was a breach of the plaintiff’s moral right because the plaintiff was not a professional photographer, but someone who had simply ‘captured’ the image. The court held that if Monte had been a professional photographer there would have been a breach of his moral right (either to integrity or attribution).

---

150 See Garnett, Davies, and Harbottle, above n 81, 728; Harrison v Harrison [2010] EWPCC 3, 60.
151 However, it is important that derogatory treatment relates to the treatment of the work; ‘the fact remains that whether or not a treatment is derogatory may often depend on how that treatment is used’: Garnett, Davies, and Harbottle, above n 81, 732.
152 Garnett, Davies, and Harbottle, above n 81, 729. Further, at 728, the authors state that for an infringement of a right to integrity, “the author must establish that the work has been subject to a ‘treatment’ and that such treatment is ‘derogatory’.” In thinking about what could be considered as a ‘treatment’ of a work, the authors state that ‘treatment’ means, in general, any addition to, deletion from or alteration to or adaptation of the work’. In particular, the authors note that the right of integrity does not apply to a ‘substantial part of a work but to any part of it’.
154 Ibid.
3.7 Conclusion

While Australian copyright law provides some protection against the misuse of personal images, the protection is limited. One of the key limitations is that the law only protects the form and not the subject matter of a photograph: that is, it does not protect the person whose image is captured in the photograph, only the person who takes the photograph. Consequently, subjects in photographs have no rights per se. Instead they must depend on the largess of the copyright owner to bring an action on their behalf.

The only protection available is to the creator of a photograph. As was shown earlier, there is little doubt that copyright subsists in most personal photographs. Despite this there are a number of limitations in relation to the protection provided to the people who create a photograph. A key concern is that the contracts of service that must be signed before a creator can upload images allow the network and its affiliates to reuse the images that are uploaded by the copyright owner. The content terms in social network contracts give a network a non-exclusive irrevocable licence to use and reuse and sub-licence all the images that have been uploaded and shared on people’s profile pages. The reuse of the image by the network (or its affiliates) may not be an infringement. In this situation, the only cause of action that a copyright owner may have is against an independent third party that copies and reuses an image from an online profile page. Even here, however there are limitations to the effectiveness of copyright law. One of the limitations is that third parties may be able to rely upon the defence of fair dealing. Where the defence applies, there will be no infringement of copyright. The upshot is that copyright law provides at best limited protection.

Moral rights provide authors with more effective protection for images that are uploaded and reused online. This is particularly the case in situations where the reused image has been distorted, or modified or altered. In such situations, the treatment of the author’s work may be derogatory and thus an infringement of a moral right. However, there are a number of limitations to the moral rights of the creators of photographs, which may limit their effectiveness in preventing the misuse of personal images reused online. One limitation is that moral rights will not apply to the subject of a photograph, and thus a subject has no right of action to prevent the misuse of their image. In most cases, the subject will depend upon the author of the photograph to bring an action on their behalf. Another limitation that may affect the ability of an author to enforce their moral rights is that the use of image may not be an infringement if the treatment is reasonable in the circumstances. As was noted earlier, copyright law provides some protection for the misuse of personal images that are shared online, however
this is limited. In particular, the chapter has highlighted that subjects in photographs are unable to personally prevent the misuse of their image and must rely on the creator of the image to bring an action on their behalf.
Chapter 4
Privacy, personal images and social networks

4.1 Introduction

The chapter evaluates the adequacy of Australian privacy law in protecting against the misuse of personal images shared on social networks. For the purpose of this thesis, Australian privacy law is construed broadly to include common law actions of trespass, nuisance, defamation, contract and equity, as well as the relevant state and Commonwealth legislation. It is also noted that privacy in personal images may be also be protected by the law of confidence. This is discussed further in Chapter 5.

As is noted below, the Privacy Act 1988 (Cth) (Privacy Act) provides limited protection for personal images shared on social networks in Australia. The problems with Australian privacy law were highlighted in a series of ALRC Reports written from the 1970’s through to 2014; the most important being that Australian law does not recognise a personal right to privacy, and that there is no nationally consistent approach for privacy protection of personal images. Instead, Australian privacy law is fragmented into statutory legal protection and common law. To remedy these problems, the ALRC made a number of recommendations, including the introduction of a new statutory tort of invasion of privacy, the expansion of the tort of breach of confidence to include private information and the addition of damages for...

---

1 Herein referred to as the Privacy Act or simply the Act.
4 Without doubt, Australian law has adopted England’s approach to protecting ‘privacy’ by using existing areas of law such as equity, the tort of breach of confidence, copyright and contracts, instead of developing a clear and definitive right to privacy: see for further discussion Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Report No. 123 (2014).
emotional distress. The ALRC also recommended that ‘Federal legislation should provide for a statutory cause of action for a serious invasion of privacy.’ To date, the Australian government has not implemented any of the ALRC’s recommendations. As a result, the protection for personal images on social networks remains fragmented under the common law and statutory legislation.

4.2 Common Law

Australian common law has been slow to protect personal images. In Australia, ‘there is no common law right not to be photographed’. As Dowd J said, ‘[a] person, in our society, does not have a right not to be photographed’. Without a right not to be photographed, personal images that are captured and shared on social networks are vulnerable to misuse. While there is limited protection for personal images, a person cannot prevent a third party from photographing them in a public place. There is no law against taking photographs of people from public places, even if a person is in a private place, unless the conduct of taking photographs amounts to stalking or ‘the intent is to “peep or pry” on an individual’.

The development of privacy law in Australia has been stagnant since the 1930s, when the landmark decision of *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) rejected the existence of a common law privacy right. As Latham CJ said in the

---


11 See, for example, the *Crimes Act 1900* (NSW) s 547C.

12 (1937) 58 CLR 479, 504–5. The *Victoria Park Case* signified the contention surrounding a right to privacy when the courts failed to establish a tort of privacy. This case proved to serve an unwavering perspective relating to privacy interests for decades later, as the case centred on privacy issues cloaked under the tort of nuisance and copyright over broadcasts. The plaintiff, the owner of the racetrack, tried to prevent the defendant from viewing and broadcasting the races and any information that was
decision, ‘however desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right of privacy exists’. It should be noted that this was not a unanimous decision. The dissenting judges believed that the common law of Australia ought to provide a new remedy that would defend the privacy of the individual from ‘serious, unwanted intrusion’.

Victoria Park had a stifling effect on the development of privacy jurisprudence in Australia. Indeed, it was not until the High Court considered privacy interests in the decision of Australian Broadcasting Corporation v Lenah Game Meats (Lenah) in 2001 that the issue was considered again by the courts. While there had been some hope that Lenah would

displayed at the track from the defendant’s adjacent property, where an elevated platform was built that allowed them to view and broadcast the races.

Victoria Park Racing and Recreations Grounds Co Pty v Taylor (1937) 58 CLR 479, 504-5, 496 (Latham CJ).


Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208; Australian Broadcasting Corporation (ABC) v Lenah Game Meats Pty Ltd [2001] HCA 63 (Gleeson CJ) 33: ‘Slicer J recorded that no issue of breach of confidentiality was raised’. See also Megan Richardson, ‘Whither Breach of Confidence: A Right of Privacy for Australia?’ (2002) 26 Melbourne Law Review 381, 388: ‘a difficulty with Lenah Game Meats viewed from a privacy perspective, is that the plaintiff did not argue its case for breach of confidence. If it had been maintained that the information about what went on in its abattoir was confidential, notwithstanding that some public access to the abattoir was permitted – in the same way that information about the plaintiff’s wedding was still regarded as confidential in Douglas v Hello! Ltd.’ See also Australian Broadcasting Corporation (ABC) v Lenah Game Meats Pty Ltd [2001] HCA 63, 64 (Gleeson CJ), citing ‘if by information, is meant the facts as to the slaughtering methods used by the respondent, such information was not confidential in its nature. But equity may impose obligations of confidence even though there is no imparting of information in circumstances of trust and confidence.’
recognise a general right to privacy, the High Court basically reiterated the existing position and held that there was no actual right to privacy in Australia.\(^{18}\) They did, however, suggest that there was a possibility that a tort of privacy might develop in the future.\(^{19}\)

---

18 Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199, 206–239 (Gummow and Hayne JJ) considered whether there was a right of privacy when they considered cases from the United States where right to privacy exists, but held that there was no such right in Australia, but could develop later on but in favour of natural persons not corporations. Further, Gummow and Hayne JJ stated that ‘privacy shouldn’t’ be used to protect information because it has value to the corporation if not disclosed to others’. In their judgment, Their Honours limited privacy to protection of information for natural persons as opposed to a corporation because there are ‘limits on the type of information that can be protected’. Lenah Games Meats Pty Ltd v Australian Broadcasting Corporation (2001) 185 ALR 1, 39, 55, 56, [189], [191]. Compare with the Victoria Park Racing and Recreations Grounds Co Pty v Taylor (1937) 58 CLR 479, 504–5; at 496, Latham CJ noted that ‘however desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right of privacy exists’.

19 Lenah Games Meats Pty Ltd v Australian Broadcasting Corporation (2001) 185 ALR 1, 39, 95 [335]. The court did suggest that there was a need for such a right – for example, when Callinan J suggested ‘a need for a relatively untrammelled form of protection against intrusion upon both private, and legitimate commercial interests, for all of ordinary people, celebrity and corporations; whether conducting lawful business activities, or doing things of commercial value, or going about their day-to-day affairs’. In his judgment, Callinan J signalled that it was time for consideration of a tort of invasion of privacy in Australia. Drawing upon Rich J’s dissenting view in Victoria Park, Callinan J acknowledged that Rich J’s view at that time resonated with modern society; further, in Lenah the judges stated: ‘Whatever development may take place in that field will be to the benefit not artificial persons and hence was not available to the respondent as a corporation.’: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd [2001] HCA 63 (15 November 2001); Hon. Justice IDF Callinan AC, ‘Privacy, Confidence, Celebrity and Spectacle’ (2007) 7(1) Oxford University Commonwealth Law Journal 1, 19. Until this happens, individuals whose privacy is at risk are forced to rely upon the piecemeal common law provisions along with state and federal privacy legislation, as highlighted in Victoria Park Racing and Recreations Grounds Co Pty v Taylor (1937) 58 CLR 479, 504–5. At 496, Latham CJ noted that ‘however desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right of privacy exists’; Re X [1975] Fam 47, 58; Malone v Metropolitan Police Commissioner [1979] Ch 344, 357–8; 10th Cantanae v Shoshana (1987) 79 ALR 299, 300; Kaye v Robertson [1991] FSR 62, 66, 70–1; Khorasandijan v Bush [1993] QB 727, 744; R v Central Independent Television [1994] Fam 192, 204; R v Khan [1997] AC 558, 581; Greg Taylor, above n 7, 237. See, Giller v Procopets [2004] VSC 113; Kalaba v Commonwealth [2004] FCAFC 326; Peter Bartlett, ‘Privacy Down Under’ (2010) 3(1) Journal International Media and Entertainment Law 145, 151, 172.
Until the courts develop a statutory or a common law tort of privacy, they will struggle to protect personal images under the common law. One possibility is the tort of trespass which will be actionable when a person interferes with another person’s body or property.\(^{20}\) Given that the tort of trespass requires a physical interference, it is unlikely that it will provide adequate protection for personal images that are shared on social networks. This is because when people take pictures of people and share them on social networks, there is no physical interference to the person’s image.\(^{21}\) Thus the tort of trespass to person or land will not provide adequate protection for personal images shared on social networks.

Another possible common law cause of action that may be relevant is the tort of nuisance. This tort may prevent the use of personal images when the images have been captured by interfering with another person’s use or enjoyment with their land or leads to physical harm.\(^{22}\) This may be the case, for example, when a third party takes photographs of a person in their home.\(^{23}\) One of the limitations of the tort is that an action for nuisance can only be brought by people who own the premises or hold the title over the premises where the tort occurs. Thus, only a person who owns the land has a right to sue; other parties cannot bring an action.\(^{24}\) As a result, when people take pictures of other people on private premises, it is unlikely that the tort of nuisance will provide any protection.

\(^{20}\) Collins v Wilcock (1984) 1 WLR 1172, where going about daily life may risk forms of physical contact when consent may be inferred – for example, public transport or walking on a busy street. See also Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123 (2014) Chapter 3: Overview of Current Law.

\(^{21}\) This also applies to an action for trespass to land, because only a person who has title over that land is entitled to sue, so in situations where a person takes a picture of a person at a wedding, or in hospital, there is no right under trespass to land to sue. See Kay v Robertson [1991] FSR 62; Douglas v Hello! Ltd [2005] EWCA Civ 595 (18 May 2005).


\(^{23}\) See Raciti v Hughes (1995) 7 BPR 14 837 where the plaintiffs were granted an injunction to prevent motion-triggered lights and surveillance cameras from targeting their backyard; see Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123 (2014), Chapter 3: Overview of Current Law.

Another way that the common law may prevent the publication of personal images shared on social networks is via the tort of defamation.\textsuperscript{25} The tort of defamation may be available as a cause of action when the publication of a personal image on a social network is damaging to a person’s reputation.\textsuperscript{26} In order to establish defamation, there are three key requirements that need to be established. The first requirement is that the plaintiff is identified as an individual.\textsuperscript{27} When a photograph of a person is published online, there is usually little problem in satisfying this requirement (although there may be problems in some cases, for example, where a person’s identity is obscured). The second requirement is that the image is published to a third party.\textsuperscript{28} Where a photograph is published online this requirement will be satisfied.\textsuperscript{29} The third requirement that needs to be satisfied is that there is a defamatory matter.\textsuperscript{30} What constitutes a defamatory matter is construed broadly and includes ‘hatred, contempt and

\textsuperscript{25} Prior to the Uniform Defamation laws, some states and territories indirectly protected private information in photographs if a defendant could not justify that the publication was in the public interest, or it was true – see Defamation Act 2005 (NSW); Defamation Act 2006 (NT); Defamation Act 2005 (Qld); Defamation Act 2005 (SA); Defamation Act 2005 (Tas); Defamation Act 2005 (Vic); Defamation Act 2005 (WA); Civil Law (Wrongs) Act 2002 (ACT) Ch 9; Defamation Act 2006 (NT) 2006.

\textsuperscript{26} See David Rolph, ‘Dirty Pictures: Defamation, Reputation and Nudity’ [2005] 10(7) Law Text Culture 101, 101-2; see generally, Andrew T. Kenyon, ‘Imputation or Publication: The Cause of Action in Defamation’ [2004] 27(1) University of New South Wales Law Journal, 100; Mirror Newspapers v Harrison [1982] HCA 50; (1982) 149 CLR 293, 295 (Mason J); Trkulja v Google (No 5) [2012] VSC 533 where the plaintiff’s name was associated with images and names of high profile criminal figures in the defendant’s search engine; Andrew Clarke, John Devereux, Julia Werren and Jennifer O’Reilly, Torts, A Practical Learning Approach (3rd ed LexisNexis Australia) 809.

\textsuperscript{27} See generally Andrew Clarke, John Devereux, Julia Werren and Jennifer O’Reilly above n 26, 811 where the authors state that the plaintiff must be able to show that the defamatory statement could be taken by others to refer to them, for example when a plaintiff’s name or image is used, whether the action will be successful will depend on whether or not the person is identifiable as an individual: Knupffer v London Express Newspapers Ltd [1994] AC 116, 124 where Lord Potter stated that ‘The size of the class, the generality of the charge and the extravagance of the accusation may all be elements to be taken into consideration but that none of them is conclusive’.

\textsuperscript{28} See generally Andrew Clarke, John Devereux, Julia Werren and Jennifer O’Reilly above n 26.

\textsuperscript{29} A publication may relate to different forms of media such as newspaper, magazines, television programs, internet communications for example blogs, tweets, online publications, YouTube clips, postings on Facebook and other social networking sites: see Andrew Clarke, John Devereux, Julia Werren and Jennifer O’Reilly above n 26, 812.

\textsuperscript{30} See Andrew Clarke, John Devereux, Julia Werren and Jennifer O’Reilly above n 26.
ridicule’ or statements that cause the plaintiff to be shunned and avoided. 31 One situation where a publication may be defamatory is where the photograph is of a person who is naked or where it exposes body parts. 32 This is because the exposure of a person’s genitalia may damage their reputation and expose them to ridicule. 33 As Gibson DCJ recently noted in relation to an action for defamation involving the publication of a photograph of a person’s genitalia:

the sting of the libel lay in being photographed in circumstances outside the normal, namely with disregard to the social taboos of nakedness and/or lack of dignity. In fact, even if the person photographed partially naked did not intentionally disrobe and/or permit the taking of the photograph, being photographed partially nude may be sufficient to be defamatory. 34

31 See Andrew Clarke, John Devereux, Julia Werren and Jennifer O’Reilly above n 26. See also, Ettinghausen v Australian Consolidated Press (1991) 23 NSWLR 443; Anderson v Gregory [2008] QCA 419, where the court held that the plaintiff was exposed to ridicule by a digitally altered photograph inferred meaning that the plaintiff had an eating disorder.


33 Australian Consolidated Press Ltd v Ettinghausen, unreported CA40079/93, CA (NSW) Gleeson CJ, Kirby P and Clarke JA, 13 October 1993, Ettinghausen v Australian Consolidated Press Ltd, unreported, SC (NSW), No 12807/91 Hunt CJ at CL, 11 March 1993, Ettinghausen v Australian Consolidated Press Ltd, (1991) 23 NSWLR 443. Shepherd v Walsh [2000] QSC 177, Shepherd v Walsh [2001] QSC 358, Shepherd v Walsh, unreported SC (Qld), No S49/96, Jones J, 8 May 2001. See David Rolph, above n 26, 101-2, 110, where Rolph argues that situations where the publications of photographs are defamatory involve the ‘concept of reputation as dignity.’ Further 124 where Rolph argues that the decision in Ettinghausen was ‘influential in legal terms. They encouraged others to use and his imputations formed the precedent for prospective litigants’ pleadings. Indeed, the central imputation in Shepherd v Walsh was explicitly based on the imputation of exposure to ridicule originally approved by Hung J.’ Rolph states, ‘it is perhaps paradoxical that plaintiffs who complain that a publication of a naked photograph exposed them to more than a trivial degree of ridicule seek to assuage the insult to their dignity by agitating the issue.’

34 Mossimani by his Tutor Karout v Australian Radio Network Pty Ltd [2016] NSWDC Gibson DCJ 23, stated this ‘was the case in McDonald v The North Queensland Newspaper Co Ltd [1997] Qd R 62, where a photograph of a footballer being tackled revealed his penis. There was no suggestion that he had permitted the photograph to be taken, as the sting of the libel was that his penis was showing.’ See generally for example, personal images depicting nudity, Australian Consolidated Press Ltd v Ettinghausen, unreported CA40079/93, CA (NSW) Gleeson CJ, Kirby P and Clarke JA, 13 October 1993; Ettinghausen v Australian Radio Network Pty Ltd [2016] NSWDC Gibson DCJ 23,
The online publication of a personal image may also be defamatory when the image is distorted or altered (photoshopped), where the image is uploaded along with accompanying text that is false or misleading, or where the context in which the image is displayed places the plaintiff in a bad light (by, for example, associating them with high profile criminal figures). In all cases, the plaintiff would need to show that the imputation or inference that is conveyed in the published photograph is capable of being defamatory, that is, that the publication gives rise to an inference that is damaging to the plaintiff’s reputation. In thinking about the fate of personal images published online, it is important to note that as Kirby J said, the standard for what may be defamatory may vary in accordance to current social standards:

In most circumstances, it ought not to be the case in Australia that to publish a statement that one adult was involved in consenting, private homosexual activity with another adult involves a defamatory imputation…. However, it would ignore the reality of contemporary Australian society to say that that day has arrived for all purposes and all people. At least for people who treat their sexuality as private or secret, or people who

---

35 Hanson-Young v Bauer Media Ltd (No 2) [2013] NSWSC 2029 (9 December 2013) where Senator Hanson-Young’s image was photoshopped on a lingerie model’s body posing at the entrance of a bedroom.

36 See Trkulja v Google (No 5) [2012] VSC 533. See for example, when a woman took a photograph of a man posing with a cut out of Darth Vader was uploaded on Facebook, along with accompanying text “Ok people, take a look at this creep. Today at Knox he approached my children when they sitting at the frozen movie in the children’s clothing section, he said “hey kids” they looked up and he took a photo, then he said I’m sending this to a 16 yr. old. I immediately removed the kids from that area and took them to security at the front so I then followed them and took his picture and he took off. Centre management were straight onto and so are the police, hopefully he is caught. Police said if he is a registered sex offender he will be charged, this happened at Knox, be safe with your kids’. The man however was a father taking selfie of himself (not the kids) to send to his own children as a daggy dad joke. See further detail Lisa Vass, ‘Creep’ shamed on Facebook was actually man taking selfie with Darth Vader’, 11 May 2015, Naked Security, <https://nakedsecurity.sophos.com/2015/05/11/creep-shamed-on-facebook-was-actually-man-taking-selfie-with-darth-vader/ >

37 Trkulja v Google (No 5) [2012] VSC 533.
have presented themselves as having a different orientation, such an imputation could, depending on the circumstances still sometimes be defamatory. 38

One of the key problems that a plaintiff faces in this context is that truth is a complete defence to defamation. This is important because when a person’s image is captured in a photograph and published on a social network, it is a true account and thus a potential defence to an action for defamation. Another problem that a plaintiff would face is that the courts seem to have set a high standard when it comes to proving defamation by way of a photoshopped photograph, this is particularly the case where the alteration is intended to be humorous.39 The restrictive attitude of the courts in this context can be seen in Mossimani by his Tutor Karout v Australian Radio Network Pty Ltd 40. This decision arose after a photograph taken of the plaintiff in a night club was uploaded on Facebook and subsequently reused and recirculated. The photograph showed the defendant embracing his girlfriend and people dancing in the background. The plaintiff had an unusual haircut, specifically a mullet. Following the publication of the image, a number of memes using the plaintiff’s image began to circulate on the internet. The plaintiff’s image was photoshopped and reused on a number of different photographs including Mount Rushmore, a pin the tail on the donkey, Pythagoras, a dollar bill, a horse, and a Joe Dirt movie poster.41 After the photographs went viral the images were republished in The Daily Mail and The Daily Telegraph. The plaintiff claimed that the publication of the photoshopped images were defamatory because they exposed him to ridicule and suggested that he was ugly and stupid. Gibson DCJ struck out the majority of the plaintiff’s claims because ‘even photoshopped images of the plaintiff would fall outside the imputations required for an image to be defamatory’.42 Gibson DCJ said that the images needed to be viewed in the context as a whole and that ‘the matter of complained of is commenting about his hairstyle

39 Hanson-Young v Bauer Media Ltd (No 2) [2013] NSWSC 2029 (9 December 2013)
Compared to Australian Consolidated Press Ltd v Ettingshausen (Unreported, Court of Appeal NSW, Gleeson CJ, Kirby P and Clarke JA, 13 October 1993) 15 (Kirby P); David Rolph, above n 26, 104-7.
40 Mossimani by his Tutor Karout v Australian Radio Network Pty Ltd (ACN 065986 987) [2016] NSWDC.
41 Mossimani by his Tutor Karout v Australian Radio Network Pty Ltd (ACN 065986 987) [2016] NSWDC
Gibson DCJ, 109.
being ridiculous, and this is not the same as saying that the plaintiff is ugly’.

Further Gibson DCJ said that none of the images ‘suggest physical ugliness on the part of the plaintiff let alone ‘hideous’ ugliness. The plaintiff has not been compared to Frankenstein or some other hideously ugly figure; his haircut has been criticised as ridiculous.’

As Gibson DCJ stated, while ‘the matter complained of publishes memes which portray the plaintiff in a humorous light, any defamatory meaning drawn from the publication as a whole would be so slight as to be de minimis.’

As a result, when personal images are reused or published in a humorous way, as in Mossimani, it is unlikely that they will be defamatory. This is an important limitation on the ability of the tort to be useful in protecting personal images online.

### 4.3 Statutory Protection

There are two sources of statutory law that protect personal images in Australia: Commonwealth and state legislation. In 1988, the Commonwealth government enacted the Privacy Act 1988 (Cth). The Privacy Act also fulfilled Australia’s international obligations.

---

43 Ibtd 108.

44 Ibid.

45 Mossimani by his tutor Karout v DailyMail.com Australia Pty Ltd (2016/210991); Mossimani by his tutor Karout v Nationwide News Pty Ltd (2016/210996); Mossimani by his tutor Karout v Australian Radio Network Pty Ltd (ACN 065 986 987) 13 unreported decision (Gibson DCJ).

46 Mossimani by his tutor Karout v DailyMail.com Australia Pty Ltd (ACN 166 912 465); Mossimani by his tutor Karout v Nationwide News Pty Ltd (ACN 008 438 828); Mossimani by his tutor Karout v Australian Radio Network Pty Ltd (ACN 065 986 987) (No. 2) [2016] NSWDC 357 Gibson DCJ held at 10 that: ‘the whole tenor of the matter complained of is that, to use the actual words of the publication, the plaintiff had become an “internet sensation” because of his “hair-larious” mullet hairstyle, which had resulted in “hilarious memes” and that the plaintiff’s friends (and, by inference, the plaintiff, although he said he “couldn’t care less”) were “loving the attention”. The highest that the matter complained of could be put is that the plaintiff’s hairstyle had provoked a sensational internet response, including humorous memes, a meaning which Mr Rasmussen acknowledged could not amount to a defamatory act or condition because it was so trivial as to have no defamatory content.’

47 The Privacy Act 1988 (Cth) was introduced as a result of the gaps in the law identified in a series of ALRC inquiries into the state of privacy protection: see Australian Law Reform Commission, Privacy Proposals, Report No 22 (1983); Australian Law Reform Commission, Unfair Publication: Defamation and Privacy, Report No 11 (1979); One of the consequences of the decision in Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479, 504–5 is that the courts held that there is no recognised right to privacy in Australia.
with respect to privacy. The Privacy Act contains privacy principles that relate to the way in which federal government departments or agencies and Australian corporations treat personal information. The Privacy Act did not affect any privacy laws of a state or territory. Each state and territory may have specific regulations managing personal information in relation to personal images. There is no prescribed manner of regulating personal information under state or territory law.

4.3.1 Commonwealth Privacy Legislation

The primary source of federal protection of privacy law in Australia is the Privacy Act 1988 (Cth). The Privacy Act regulates personal information that is handled by the Australian federal government and the private sector. The Privacy Act includes 13 Australian Privacy Principles (APPs) that govern and regulate the handling of personal information by federal government departments or agencies or Australian corporations.

In Australia, the Privacy Act provides protection for personal information in certain specific situations. The Privacy Act defines personal information as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable; whether the information or opinion is true or not; and whether the information or opinion is recorded in a

---


49 There are 13 Australian Privacy Principles (APPs) in Schedule 1 of the Privacy Act 1988 (Cth) that outline how government departments or agencies or Australian corporations manage personal information.

50 The Privacy Act 1988 (Cth) s 3 states: ‘It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.’


52 Some states have legislation while others have administrative policies – for example, Western Australia and South Australia: see Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, Report 108 (2008).

53 Australian government agencies (and the Norfolk Island administration) and all businesses and not-for-profit organisations with an annual turnover of more than $3 million are covered by the 13 APPs from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) which amended the Privacy Act 1988 (Cth).
material form or not’. 54 ‘Personal information’ potentially encompasses any information that identifies an individual, or their identity that is in recorded form. 55 Personal information also includes ‘sensitive’ information – for example, information that is about an individual’s race, gender, political opinions or religious beliefs. 56 There is little doubt that photographs of people would be classified as personal information and are thus potentially protected under the Privacy Act 1988 (Cth), s 6(1); this definition was amended in 2013, with the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Amending Act) which commenced in March 2014 and amended the definition of ‘personal information’ in the Privacy Act 1988 (Cth) as ‘personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) Whether the information or opinion is true or not; an
(b) Whether the information or opinion is recorded in a material form or not.’

Privacy Act 1988 (Cth) s 6(1) defines a ‘record’ to include (a) a document; or (b) an electronic or other device’. See further Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, Report 108 (2008) Chapter 69 Particular Issues Affecting Children and Young People, Taking Photographs and Other Images, where it states that ‘The Privacy Act protects personal information that is held, or collected for inclusion, in a “record”. A “record” is defined to include a photograph or other pictorial representation of a person. If an individual’s identity is apparent, or can reasonably be ascertained, from a photograph or other image, then the collection, use and disclosure of that image is covered by the Privacy Act. This extends to video images as well as still photographs.’

Privacy Act 1988 (Cth) s 6(1) defines sensitive as:

‘(a) information or an opinion about an individual’s:
   (i) racial or ethnic origin; or
   (ii) political opinions; or
   (iii) membership of a political association; or
   (iv) religious beliefs or affiliations; or
   (v) philosophical beliefs; or
   (vi) membership of a professional or trade association; or
   (vii) membership of a trade union; or
   (viii) sexual orientation or practices; or
   (ix) criminal record;
   that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates.’
Act. This is on the condition that the individual’s identity is apparent or can reasonably be ascertained from the photograph.57

The legislation only applies to government departments and agencies,58 and to Australian corporations (including non-for-profit organisations) (‘APP entities’).59 APP entities include Australian government departments and agencies as well as Australian corporations with a turnover of $3 million per annum.60 At first glance, it may appear that social networks

57 See further Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008), Chapter 69: Particular Issues Affecting Children and Young People, Taking Photographs and Other Images, which states: ‘If an individual’s identity is apparent, or can reasonably be ascertained, from a photograph or other image, then the collection, use and disclosure of that image is covered by the Privacy Act. This extends to video images as well as still photographs.’ The quality of protection of the Privacy Act for personal images that are shared online is limited, as is highlighted. This is because the scope of the Privacy Act does not apply to individuals, and as such personal images that are shared by people online fall outside the scope of the Act.

58 Privacy Act 1988 (Cth) s 6 definition of APP entities means an agency or organisation, see also the Australian Privacy Principles (APPs), as provided in Schedule 1 of the Privacy Act 1988 (Cth). The APPs provide for how Australian and Norfolk Island government agencies and all private sectors with an annual turnover of more than $3 million, and private health service providers must handle use and manage personal information. See also ‘organisations’ and ‘small business operators’ in section 6C section 6D, which may also have to comply with the APPs under the Privacy Act 1988 (Cth).

59 Privacy Act 1988 (Cth). The APPs guide Australian corporations that handle, collect and store personal information.

60 An entity that is not an APP entity (within the meaning of the Privacy Act) will be considered as a ‘small business’ if it has an annual turnover of less than $3 million dollars per annum: section 6D. There are notable exceptions with respect to ‘small business operators’ under section 6D (4): ‘an individual, body corporate, partnership, unincorporated association or trust is not a small business operator if he, she or it:

(a) carries on a business that has had an annual turnover of more than $3,000,000 for a financial year that has ended after the later of the following:

   (i) the time he, she or it started to carry on the business;

   (ii) the commencement of this section; or

(b) provides a health service to another individual and holds any health information except in an employee record; or

(c) discloses personal information about another individual to anyone else for a benefit, service or advantage; or

(d) provides a benefit, service or advantage to collect personal information about another individual from anyone else; or
are outside the scope of the Privacy Act because they are based overseas and not in Australia. However, the Privacy Act has an extra-territorial provision, which provides that a foreign entity\(^{61}\) will be caught by the Act if there is an Australian link.\(^{62}\) The Privacy Act potentially applies to any organisation that carries on business in Australia and the personal information is collected or held in Australia.\(^{63}\) This will mean that social networks like Facebook, Instagram

\(\text{(e)}\) is a contracted service provider for a Commonwealth contract (whether or not a party to the contract); or
\(\text{(f)}\) is a credit reporting body.’

\(^{61}\) Privacy Act 1988 (Cth) s 5B Extra Territorial Operation of This Act.

\(^{62}\) An Australian link is given the meaning under sections 5B (2) and 5B (3). See below. The Privacy Act 1988 (Cth) s 5B(1A) states: ‘This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator that has an Australian link. An Australian link is given the meaning under s 5B (2), which states: ‘An organisation or small business operator has an Australian link if the organisation or operator is:

- an Australian citizen; or
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; or
- a partnership formed in Australia or an external Territory; or
- a trust created in Australia or an external Territory; or
- a body corporate incorporated in Australia or an external Territory; or
- an unincorporated association that has its central management and control in Australia or an external Territory.’

\(^{63}\) Carries on business ‘generally involve conducting some form of commercial enterprise, systematically and regularly with a view to profit’: Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544 [38]. It may also apply to any small business operator that carries on business in Australia that is not described in s 5B (2). See s 5B (3), which states that ‘An organisation or small business operator also has an Australian link if all of the following apply:

- the organisation or operator is not described in subsection (2);
- the organisation or operator carries on business in Australia or an external Territory;
- the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.’

Power to deal with complaints about overseas acts and practices
There may be issues with s 5B(3)(c), which refers to personal information collected in Australia, however. The Office of the Australian Information Commissioner, APP Guidelines - Chapter B Key Concepts - B.22 Personal Information in Australia (March 2015) Australian Government, The Office of the Australian Information Commissionerhttps://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts explains that: ‘Personal information is collected ‘in Australia’ under s
and Twitter will be covered by the Act because they have registered offices in Australia and offer their social network services to Australians.64

The Privacy Act applies when an APP entity65 ‘holds, collects, or uses’ personal images.66 Under the Privacy Act, an APP entity is deemed to ‘hold’ a personal image if ‘the entity has possession or control of a record that contains the personal information’.67 The uploading of a personal image on to a social network page by an APP entity will constitute a ‘holding’. There are two situations in which an APP entity will ‘hold’ personal images on a social network. The first is when an APP entity uploads or shares personal images on their social network page. When this occurs, the APP entity is in possession of a personal image and consequently in control of the image it has uploaded. An APP entity does not need to ‘hold’ the personal images on its own information system because the scope of ‘holding’ extends beyond

5B(3)(c), if it is collected from an individual who is physically present in Australia or an external Territory, regardless of where the collecting entity is located or incorporated. An example is the collection of personal information from an individual who is physically located in Australia or an external Territory, via a website that is hosted outside Australia. This applies even if the website is owned by a company that is located outside of Australia or that is not incorporated in Australia.’ This was also highlighted in Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 218.


64 The Privacy Act applies to Australian government departments, agencies as well as Australian corporations with a turnover of $3 million per annum; see Privacy Act 1988 (Cth), s 6 where an ‘APP entity’ means an agency or organisation; also noteworthy is that, as an APP entity, the Privacy Act primarily provides for how personal information ought to be managed and protected.

65 Privacy Act 1988 (Cth) s 6 (1). The APPs guide Australian corporations that handle, collect and store personal information.

66 Privacy Act 1988 (Cth) s 6 (1).
a ‘possession to include a record that an entity has the right or power to deal with’\textsuperscript{68} a personal image. The second situation where an APP entity will ‘hold’ personal images is when the APP entity asks individuals to share their personal images on the APP entity’s social network site.\textsuperscript{69} The question that arises here is whether the APP entity has the right or power to deal with the personal image.\textsuperscript{70} An APP entity has the power to deal with a personal image by doing a number of different acts with the image, such as restricting or allowing access to third parties, or even removing the image from the social network page.

A second situation where the Privacy Act will protect personal images is when an APP entity ‘collects’ images that are uploaded on an APP’s social network page. The question here is whether the uploading of an image on a social network page is a ‘collection’ under the Privacy Act. Under the Privacy Act, an APP entity will only ‘collect’ personal images if it is ‘for inclusion in a record or a generally available publication’.\textsuperscript{71} An APP entity may collect personal images when it directly uploads a personal image on to its social network page. For example, when a corporation runs a photograph a competition and the winning entry is published on their social network page. Here the corporation is collecting personal images to be made available on a social network. An APP entity that has images directly uploaded onto its social network page will be deemed to have ‘collected’ personal images. When an APP entity asks people to


\textsuperscript{69} See, for example, Adrien Danjou, ‘The Australian Open is Getting Increasingly Creative on Social Media’, Digital Sport (18 January 2016) <http://digitalsport.co/the-australian-open-is-getting-increasingly-creative-on-social-media>. For example, #AusOpen has been identified as the official tournament’s hashtag, while #AOSelfie is a hashtag that tournament organisers will use to collect all the fan selfies during the event – all which are displayed on a digital wall in the tournament’s village.

\textsuperscript{70} See Office of the Australian Information Commissioner, The Guide to Securing Personal Information (January 2015) <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>, which states that ‘the term “holds” extends beyond physical possession to include a record that an entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, ‘holds’ that personal information.’

\textsuperscript{71} Privacy Act 1988 (Cth) s 6(1).
share their personal images on the APP entity’s social network page, the personal images are collected by the APP entity and are recorded on the network page. Consequently, personal images that are shared on an APP entity’s social network page will constitute a ‘collection’ under the *Privacy Act*.

A third situation where personal images will be protected under the *Privacy Act* is when an APP entity ‘uses’ personal images that are uploaded or shared on its social network page. While the term ‘use’ is not defined in the Act, the APPs suggest that an APP entity will ‘use’ a personal image if it ‘undertakes an activity with the information within the effective control’. When an APP entity uploads or shares a personal image on a social network page, the uploading of the image will be a ‘use’ of the image. The sharing of an image is a ‘disclosure’, which is another form of ‘use’. There are two situations where an APP entity will ‘use’ a personal image. The first is where an APP entity accesses and views a personal image that is shared on a social network site. This would be the case when an APP entity views personal images that have already been uploaded by individuals or third parties onto a social network such as Facebook.

---


73 See Office of the Australian Information Commissioner, The APP Guidelines Chapter 6 [6.8] (February 2014) <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information> states: ‘The term “use” is not defined in the *Privacy Act*. An APP entity “uses” information where it handles or undertakes an activity with the information, within the entity’s effective control.’ For further discussion of use, see Chapter B (Key concepts). Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another unauthorised access by an employee of the entity.


74 For example, when a person ‘likes’ a page on Facebook, their personal images (and information generally) may be accessed by an APP entity. This results in the entity having access to the images because when a person ‘likes’ a page on Facebook, they are connected to the entity’s social network page, which allows them to have access to and thus ‘use’ of the images: ‘Liking a Page means you’re connecting to that Page … When you connect to a Page, you’ll start to see stories from that Page in your News Feed. The Page
An APP entity will also ‘use’ a personal image where they upload an image on to a social network.75 When an APP entity uploads and shares a personal image, they disclose it on their social network page. The APP Guidelines suggest that while disclosure is separate from use, it is often considered alongside use.76 The Privacy Act does not define ‘disclosure’. A ‘disclosure’ of a personal image occurs when an APP entity makes an image ‘accessible to others outside the entity and releases the subsequent handling of the information from its effective control’.77 When an APP entity shares a personal image on their social network page, third parties may have access to the image.78 When personal images are placed and shared on an APP entity’s social network page, the images are ‘published’ because they are made available to the public. As a result, an APP entity gives third parties access to the personal images that have been shared on their social network page.79 Consequently, even accessing or sharing (disclosing) a personal image will constitute a ‘use’ of the image.

will also appear on your profile, and you’ll appear on the Page as a person who likes that Page.’ See Facebook, Questions You May Have (2016), <https://www.facebook.com/help/452446998120360>.

See Office of Australian Information Commissioner, APP Guidelines, Chapter B B.143 (March 2015), <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts>, where it states: ‘Generally, an APP entity uses personal information when it handles and manages that information within the entity’s effective control. Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another.’


See Privacy Act 1988 (Cth), Office of the Australian Information Commissioner, The APP Guidelines 6 – Use and Disclosure - 6.9 Schedule 1 (February 2014) <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>. ‘An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control. This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient.’ See OAIC,
There are a number of limitations on the scope of the Privacy Act. The first, and one of the most important for the purpose of this thesis, is that the Privacy Act does not apply to individuals who store, collect, use and disclose personal information for personal, family or household purposes for private purposes.\(^{80}\) As was noted above, the Privacy Act only applies to government departments and agencies and APPs. As a result, the Privacy Act would not cover personal images that are shared by people on social networks. This is because both parties are ‘individuals’; consequently, images that are uploaded, posted or reposted by individuals would fall outside the scope of the Act.

Another limitation arises because employee records\(^{81}\) and information captured and shared for journalistic purposes are excluded for the scope of the Privacy Act.\(^{82}\) As a result, personal images that have been uploaded by employees or used by journalists are not covered under the Privacy Act.\(^{83}\) Another important limitation of the Privacy Act is that it does not apply to images that are held in a public record, that is to images held in a ‘generally available

\(^{80}\) Privacy Act 1988 (Cth), ss 7B (1), 16E on information that is used, collected or disclosed for personal, family or household purposes. See also Office of Australian Information Commissioner, FAQ, Government Office of the Australian Information Commissioner, which provides that ‘the Privacy Act doesn’t cover individuals acting in a personal capacity. This means you generally can’t enforce a privacy right against an individual, though you may have actions against them under other laws. For example, while you may not be able to make a complaint under the Privacy Act about an individual who posts your personal information on a social networking site’. www.oaic.gov.au <https://www.oaic.gov.au/individuals/faqs-for-individuals/social-media-ict-identity-security/social-media>.

\(^{81}\) Privacy Act 1988 (Cth), s 7B(3) personal images will be subject to contractual arrangements between employer and employee; it is also noteworthy is that there is uncertainty about whether there is adequate legal protection for personal information of employees because the issue is dealt with outside privacy law. The Attorney-General had noted that this issue was important and worthy of privacy protection; however, he deemed that personal information of employees was protected under workplace relations legislation: Commonwealth, Parliamentary Debates, House of Representatives, 12 April 2000, 15749 (D Williams, Attorney-General); see Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, Report 108 (2008).

\(^{82}\) Excludes media organisations acting in the course of ‘journalism’ see further Privacy Act 1988 (Cth) s 7b (4a).

\(^{83}\) There are other areas of law such as breach of confidence which may protect personal images, this is highlighted in Chapter 5.
The key issue here is whether a personal image on a social network is a public record. ‘Generally available publication’ is defined to mean ‘a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public a) whether or not it is published in print, electronically or in any other form, and b) whether or not it is available on the payment of a fee’. This definition is broad enough to include anything that is shared or placed on the internet.

Whether a personal image that is shared on a social network is ‘generally available’ will depend on the social network in question. It will depend on the ability of the social network’s privacy settings to control access to the social network page. As noted in Chapter 2 social networks such as Facebook, Twitter and Instagram have privacy settings that allow people to restrict access to their images. One situation where a personal image on a social network may not be ‘generally available’ is when a person uses the privacy settings to restrict third parties from obtaining access to their images. In this situation the image will only be visible to the people who they are connected to within the social network. Here, the public cannot access the personal image on a social network. Problems arise however, when a third party reshares a personal image that is restricted. When this occurs, access to the image will depend on the third party’s privacy settings. One problem that arises when personal images are shared or uploaded on a social network is that an image can go from being restricted and ‘private’, and not publicly available, to being reshared and accessed by the public simply by resharing the image.

A second situation where a personal image that is shared or uploaded on a social network will not be ‘generally available’ is when a third party gives access to another person and they take a picture or a screen shot of the image. For example, when a third party has access to a personal image shared on a social network and they show the image to another person. When this occurs, the image may be on a social network but only be available to a select audience. As a result, a personal image that is shared on a social network but is restricted to a select audience will not be ‘generally available’.

---

84 The Privacy Act 1988 (Cth) s 6(1) defines ‘record’ to include:
   ‘(a) a document; or
   (b) an electronic or other device’
   but does not include:
   ‘(d) a generally available publication; or
   (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.’

85 Privacy Act 1988 (Cth) s 6(1): ‘generally available publication’.
Personal images that are shared on social networks will not be protected under the Commonwealth privacy legislation when the images are resharred by individuals (acting in a personal capacity as distinct from APP entities and government agencies and departments) and are publicly available. This means that when people upload their images and third parties resharre these images, the images will fall within the public domain. This occurs, for example, when personal images are found on Google Images or when people can search for photographs on social networks such as Twitter or Instagram without having a social network account.

Another limitation with the protection of the Privacy Act is that if a person consents to their image being held, collected or used by an APP, the Privacy Act will not apply. Consent has two purposes under the Privacy Act. The first is that it acts as an exception when an APP entity collects and uses personal images. The second is that consent authorises the use of personal images when an APP entity collects and uses personal images for marketing purposes. Consent may be given impliedly through the terms of use of a social network. This may occur when a person signs up to a social network and connects with an APP entity (for example, a bank or a store’s social network page). However, an APP entity would need to obtain the consent of an individual when using their image for a different purpose than those for which it is originally collected. This would occur, for example, when an APP entity has collected personal images for online competitions and subsequently uses the images in an advertising campaign.

4.3.2 State and Territory Privacy Legislation

As discussed above, the Commonwealth Privacy Act only applies to federal government department and agencies, and to APP entities that handle personal information. This leaves many gaps in the regulation of personal information in Australia. In response, the states and

---

86 See Privacy Act 1988 (Cth), Sch 1, APPs 3.3 (a), 6.1 (a).
88 For example, ANZ’s campaign to donate two dollars for every selfie shared on its #headbandforgood Twitter page.
89 Information Privacy Act 2014 (ACT); Privacy and Personal Information Protection Act 1998 (NSW); Health Records and Information Privacy Act 2002 (NSW); Information Act (NT); Information Privacy
territories have developed privacy legislation or administrative regimes to protect personal information. For example, Queensland, Victoria, New South Wales, the Australian Capital Territory, Tasmania and the Northern Territory have privacy legislation to regulate personal information. South Australia regulates personal information through an administrative instruction that requires compliance by the South Australian government departments and agencies, while Western Australia regulates personal information under the *Freedom of Information Act*.

State privacy legislation applies to state government public sector bodies. In some cases, state privacy legislation will also apply to private sector organisations. For example,

**Act 2009 (Qld); Personal Information and Protection Act 2004 (Tas); Privacy and Data Protection Act 2014 (Vic).**

90 *Privacy and Personal Information Protection Act 1998 (NSW); Information Privacy Act 2009 (Qld); Premier and Cabinet Circular No 12 (SA); Personal Information Protection Act 2004 (Tas); Privacy and Data Protection Act 2014 (VIC); Information Privacy Act 2014 (ACT); Information Act (NT).*


93 State and territory privacy legislation herein after referred to as ‘state’ privacy legislation.

privacy legislation in New South Wales, Queensland, the Australian Capital Territory and Victoria also applies\(^95\) to the private sector when the information relates to health information.\(^96\)


While the definition of personal information varies between states and territories, the definition is similar to that used by the Commonwealth Privacy Act: personal information is information about an individual whose identity is apparent or ascertainable, whether or not recorded in a material form. State privacy legislation, like the Commonwealth legislation, does not apply to individuals who handle personal images on social networks. However, like the Commonwealth legislation, state privacy legislation may provide limited protection for personal images that are shared on social networks.

State privacy legislation only applies to state public sector government agencies and departments that handle personal information. ‘Handling’ is a broad term, which is defined

---

97 For example, Tasmanian legislation defines ‘personal information’ as any information or opinion in any recorded format about an individual (a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and (b) who is alive or has not been dead for more than 25 years: Personal Information Protection Act 2004 (Tas) s 3; Victoria’s Privacy and Personal Data 2014 defines personal information as ‘information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include health information’: Privacy and Data Protection Act 2014 (Vic) s 3; New South Wales also defines ‘personal information’ as ‘information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion’; see Privacy and Personal Information Protection Act 1998 (NSW) s 4; Queensland’s (Qld) s 12 defines personal information as ‘information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion’.

98 See Privacy Act 1988 (Cth) s 6(1), which defines personal information as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable; whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not’.

99 Some states and territories also include biometrics and fingerprinting identification when defining personal information.

100 Privacy and Personal Information Protection Act 1998 (NSW); Information Privacy Act 2009 (Qld); Premier and Cabinet Circular No 12 (SA); Personal Information Protection Act 2004 (Tas); Privacy and Data Protection Act 2014 (VIC); Information Privacy Act 2014 (ACT); Information Act (NT). See Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, Report 108 (2008), http://www.alrc.gov.au/publications/2.%20Privacy%20Regulation%20in%20Australia/state-and-territory-regulation-privacy; see also Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Chapter 3: Overview of Current Law, Report 123,
as ‘collecting, holding, managing, using, disclosing or transferring’ personal information. The terms ‘collection, use, disclosure and holding’ were examined above in the context of Commonwealth privacy legislation. Given that is likely that these terms will have the same meaning in State legislation as under Commonwealth legislation, they will not be discussed again. Instead I will focus on those terms that have not yet been examined: the meaning of ‘transfer’ and ‘manage’.

While ‘transfer’ is not defined in state and territory legislation, if its ordinary meaning is applied, it will mean ‘to remove from place to another’. One situation where a ‘transfer’ may apply is when a state public organisation body collects, uses, holds and discloses personal images. One situation where a public sector organisation ‘collects, uses and holds’ personal images is when a state public school takes pictures of children and uploads or posts them up on its website or includes them in an electronic newsletter. However, it is noted that neither Victorian nor Queensland legislation defines ‘collects’ or ‘handles’.

Transferring and managing personal information are covered in Victorian and Queensland legislation. For example, the Privacy and Data Protection Act 2014 (Vic) s 20(2) provides for public sector organisations not to contravene information privacy principles with respect to collection, use, storage, transfer and managing of personal information; Queensland has a similar provision, Information Privacy Act 2009 (Qld) s 6, which states that ‘6 Scope of personal information under this Act applies to the collection of personal information, regardless of when it came into existence, and to the storage, handling, accessing, amendment, management, transfer, use and disclosure of personal information regardless of when it was collected’. While New South Wales only ‘manages’ personal information, see Information Privacy Commission, PPPIP Act, http://www.ipc.nsw.gov.au/ppip-act#.

The following state legislation does not define ‘transfer’; see Privacy and Data Protection Act 2014 (Vic); Personal Information Protection Act 2004 (Tas); Information Act (NT). The exception is Queensland, which has provisions for the transfer but does not actually define the term: Information Privacy 2009 (Qld) s 33 provides for the transfer of personal information outside of Australia.

See Cambridge Dictionary, which defines ‘transfer’ to move someone or something from one place, vehicle, person, or group to another’, http://dictionary.cambridge.org/dictionary/english/transfer.
occur is when a public sector organisation moves or shifts personal images from its information system to its social network page. Another situation where a public sector organisation might transfer personal images is when it outsources the holding of personal images to a foreign entity.\textsuperscript{105} When this occurs, the public sector organisation will need to comply with the information privacy principles incorporated into the relevant legislation.\textsuperscript{106}

A further situation where state privacy legislation will protect personal images is when a public sector organisation ‘manages’ personal images. ‘Managing’ is not defined in state privacy legislation.\textsuperscript{107} If an ordinary meaning is applied, a public sector organisation will ‘manage’ when they are ‘responsible for controlling or organising’ personal images.\textsuperscript{108} A public sector will ‘manage’ personal images when they upload them on to their social network page.\textsuperscript{109}

There are a number of situations where state privacy legislation will not apply to protect personal images. This includes situations where personal images shared on social networks are publicly available – for example, when personal images are shared and are visible to third parties, such as personal images that are found on Google Images or Facebook. Personal images that are visible without the requirement of having a social network account, subscription or

\textsuperscript{105} For example, a public sector organisation may ‘transfer’ personal information to an entity outside of Australia in some cases where it is necessary for the function of the public sector organisation: see Information Privacy 2009 (Qld) s 33, which provides for the transfer of personal information outside Australia.

\textsuperscript{106} Each state and territory that has privacy legislation must comply with the Information Privacy Principles; these are similar to the Commonwealth’s APP. See further Privacy and Data Protection Act 2014 (Vic) s 17. The Information Privacy Act 2009 (Qld) s 33 provides for the transfer of personal information outside Australia. Personal Information Protection Act 2004 (Tas); Information Act (NT).

\textsuperscript{107} Privacy and Data Protection Act 2014 (Vic) s 17 states that a public sector must do anything that would contravene IPP that is ‘collected, held, managed, used, disclosed or transferred by it in connection with the administration of the public register if that information were personal information’.

\textsuperscript{108} See Cambridge Dictionary, which defines manages as ‘to be responsible for controlling or organizing someone or something, especially a business or employees,’ <http://dictionary.cambridge.org/dictionary/english/manager>.

\textsuperscript{109} This will occur when a public sector organisation uploads personal images onto its social network page; the organisation is effectively controlling the images because the organisation chooses whether to allow or restrict access to the images on the social network page. Also noteworthy is that in Victorian privacy legislation, ‘managing’ refers to the administration of personal information see: Privacy and Data Protection Act 2014 (Vic) s 20.
profile fall within the meaning of being publicly available. When personal images are shared on social networks without restricted access, the images can be accessed by anyone. In this situation, the images are publicly available and will not be protected under state privacy legislation. State privacy legislation will also not apply when personal images are used for law enforcement purposes — for example, where state and territory law enforcement agencies search for personal images on social networks as a way of obtaining information in relation to criminal matters. State and territory privacy legislation will also not apply when the use of the image is in the public interest, or when the information is subject to freedom of information provisions.

4.3 Conclusion

The chapter has shown that the common law potentially provides some protection for personal images via the torts of trespass, nuisance and defamation. However, the protection here is restricted. For example, the tort of trespass is restricted by the fact that there needs to be a direct and physical interference to a person. The tort of nuisance will also provide limited protection for personal images because taking photographs of people is not considered to be an interference with a person’s use or enjoyment of their land. As noted earlier, the tort of defamation may provide a remedy when personal images that are published online are defamatory. As the case law suggests, the courts are willing to prevent the publication of naked images or images of exposed body parts. Defamation may also relied upon when a person’s name is associated with someone else’s image in a manner that is false or misleading. Despite this, there are a number of potential limitations to the use of defamation in protecting against misuse online: the most important being that ‘truth’ is a defence to defamation and the fact that the courts have set high standards in proving online defamation, particularly where an image is

---

110 See Information Act 2002 (NT) s 68. Information privacy principles will not apply to publicly available information; Privacy and Data Protection Act 2014 (Vic) s 12; Personal Information Protection Act 2004 (Tas) s 8; Information Privacy Act 2009 (Qld) Sch 1.

111 Personal Information Protection Act 2004 (Tas) s 9; Information Privacy Act 2009 (Qld) s 29.

112 For example, when a person goes missing, see Privacy and Data Protection Act 2014 (Vic) s 15.

113 See Information Privacy Act 2009 (Qld) Sch 1, public interest disclosure; see also Privacy and Data Protection Act 2014 (Vic) s 29.

114 Privacy and Data Protection Act 2014 (Vic) s 14; see Information Privacy Act 2009 (Qld) s 5.
photoshopped for humorous purposes. In situations where a person’s image has not been altered or distorted but published online, it seems that defamation will be of limited use.

Commonwealth privacy legislation also provides limited protection for personal images that are shared on social networks. However, upon closer examination there are significant problems with the Privacy Act. There are a number of factors that limit the operation of the Privacy Act in relation to personal images that are shared by people on social networks. One limitation is that journalists who use personal images for journalistic purposes are not covered by the Privacy Act.115 An important limitation is that the Privacy Act does not apply to individuals who share and exchange personal images on social networks, instead it only applies to government department and agencies and Australian APP’s.

State privacy legislation also provides limited protection for personal images when state government departments and agencies handle personal information. In some states, privacy legislation also extends to private sector organisations that handle health information. The majority of private sector health service providers will be caught under both state and territory legislation. While many organisations, government departments and agencies will fall within the scope of state privacy legislation, private organisations that share personal images on social networks fall outside the scope of the legislation. Despite the protection provided by state legislation, there are a number of gaps in the existing law. One problem is that state privacy legislation is inconsistent and fragmented. The lack of uniformity means that the level of protection available for personal images that are shared on social networks is uncertain and unclear. State privacy legislation is also limited insofar as it excludes protection for personal images that are ‘publicly available’. As a result, when people share images on social networks, there is a risk that those images will fall in the public domain.

While Australian privacy law provides some protection for personal images that are shared on social networks, the protection is limited and fragmented. It is clear that Australian

---

115 When people upload and share their personal images on social networks, journalists may use these images for journalistic purposes; this means that the use of the image would not be covered under the existing privacy legislation – see, for example, Jenni Ryan, ‘How a Darth Vader Selfie Showed the Worst Side of Social Media’, Mashable Australia (11 May 2015). <http://mashable.com/2015/05/11/darth-vader-selfie/#rYjWrQ8gikq3>; see also Lisa Vaas, “‘Creep” Shamed on Facebook was Actually Man Taking Selfie with Darth Vader’, Naked Security by Sophos (11 May 2015) <https://nakedsecurity.sophos.com/2015/05/11/creep-shamed-on-facebook-was-actually-man-taking-selfie-with-darth-vader>.
privacy law provides, at best, limited protection to prevent the misuse of personal images on social networking sites. This leaves a significant gap in the law.
Chapter 5
Breach of Confidence, Personal Images and Social Networks

5.1 Introduction

The sharing of personal images on social networks has blurred the line between public and private life. It has also created a situation where people risk having the images they have taken of themselves and uploaded onto social networks being misused. People are in an even more precarious position when third parties place their image on a social network site. This chapter evaluates whether the Australian law of confidence is adequate to prevent the misuse of personal images in these two situations.

One of the notable things about Anglo-Australian law is that there has been a reluctance to recognise a common law to a right to privacy. Rather, the law has developed specific legislation to deal with specific problems. The fate of personal images on social networks must be viewed in light of this. In Coco v AN Clark Engineers, Megarry J found that three elements must be satisfied for an action of a breach of confidence to succeed. These are as follows:

1. the information must have the necessary quality of confidence;
2. the information must have been imparted in circumstances importing an obligation of confidence; and
3. there must be an actual or threatened unauthorised use or disclosure of the information to the detriment of the confider.

When thinking about the role potentially played by breach of confidence in preventing the misuse of personal images on social networks, a number of questions arise. These are:

---

2 As evidenced by various intellectual property laws, such as copyright, trademarks, patents and breach of confidence.
3 Coco v AN Clark Engineers [1969] RPC 41. This case related to protection of confidential information in relation to trade secrets.
4 Coco v AN Clark (Engineers) Ltd [1969] RPC 41, 47 (Megarry J).
5 Lionel Bently and Brad Sherman, Intellectual Property Law, 4th ed. (Oxford University Press, 2014) 1142. See generally, Tanya Aplin et al above n1, 13; Coco v AN Clark (Engineers) Ltd [1969] RPC 41; Saltman Engineering Co Ltd v Campbell Engineering Co Ltd (1948) 65 RPC 203 (Court of Appeal); See
1. Is the personal image is capable of being protected?
2. Is there an obligation to keep the personal image confidential?
3. Does the use of the personal image constitute a breach of confidence?
4. Does the defendant have a defence to an action for breach of confidence?

These are discussed below.

5.2 Is the Personal Image Capable of Being Protected?

One of the key questions that arises when reflecting on the role that the law of confidence potentially plays in preventing the misuse of personal images is whether an image is in fact information that is capable of being protected. The concept of ‘information’ here is very broad: it includes information in various forms, including video, text, drawings and photographs. It also includes various types of information, such as commercial information, medical lectures, marital secrets, cultural and religious secrets of Aboriginal and Torres Strait Islander


Abernethy v Hutchinson (1824) 1 H & Tw 28; 47 ER 1313.

Argyll v Argyll [1967] Ch 302.
communities,\textsuperscript{10} and photographs.\textsuperscript{11} There is little doubt that personal images are capable of being protected under the law of confidence. While the scope and types of images capable of being protected is very broad, information that is trivial, immoral, vague or in the public domain will not be protected.

5.2.1 Are Personal Images Shared on Social Networks Trivial?

There is a general presumption that trivial information is not protected under the law of breach of confidence. The reason for this is that it is unlikely that equity would protect information unless the consequences of disclosure were serious.\textsuperscript{12} As Megarry J said, ‘I doubt whether equity would intervene unless the circumstances were of sufficient gravity; equity ought not to be invoked to protect trivial tittle-tattle, however confidential.’\textsuperscript{13} This has the potential to impact whether the information captured in an image and shared on a social network site is protected.

Whether personal images shared on social networks are trivial will depend on the specific type of information revealed in the image.\textsuperscript{14} Without question, many of the images that are exchanged and revealed on social networks – such as pictures of people eating, cooking or dancing – are trivial.\textsuperscript{15} Consequently, there is a risk that many of the personal images that are

\textsuperscript{10} Foster v Mountford [1978] FSR 582.


\textsuperscript{12} See Coco v AN Clark (Engineers) Ltd [1969] RPC 41, 48.

\textsuperscript{13} Ibid.

\textsuperscript{14} Certain types of information, such as addresses, phone numbers or email addresses may be considered ‘trivial’. This type of information may be capable of being protected if the use of the information poses a significant risk to the plaintiff. Consequently, there may be a serious risk of exposure to stalkers and being stalked if such details are revealed: Mills v News Group Newspapers [2001] EMLR 957.

\textsuperscript{15} See Sarah Thomas, ‘Fat Shamed Dancing Man to Party with Moby, Pharell Williams Support’, Sydney Morning Herald, 9 March 2015 <http://www.smh.com.au/entertainment/music/fatshamed-dancing-man-to-party-with-moby-with-pharrell-williams-support-20150309-13yqge.html>. Photographs of Sean ‘Dancing Man’ dancing were shared on social media site 4chan by the person who had taken them, mocking Sean dancing and making cruel comments about him. The photographs, which went viral, highlight that, despite the ‘trivial’ nature of a person being captured dancing, it may not be trivial to the person when their image captured is embarrassing or humiliating.
shared on social networks will fall within the category of trivial information, and thus not be protected.

While information that is trivial will not normally be protected by the tort of breach of confidence, it seems that exceptions will be made in a number of situations. The courts will protect information that might otherwise have been trivial if the publication of the information revealed in the image is ‘offensive to a reasonable person of ordinary sensibilities’. It seems that the courts are willing to protect personal images where the image relates to someone’s personal life. This is particularly the case with images of celebrities. This is on the basis that the publication of those images is intrusive into private life ‘in a peculiarly humiliating and damaging way’—for example, a photograph of Naomi Campbell coming out of a Drugs Anonymous meeting, images of the Douglas and Zeta Jones wedding and photographs of people engaged in sexual activities have been held to not be trivial and thus potentially

---

16 There is limited discussion of what is ‘trivial’ in relation to personal images in the leading cases: see Campbell v MGC [2004] 2 AC 457; Douglas v Hello! [2008] 1 AC 1.


18 Theakston v MGN Ltd [2002] EWHC 137 (Queens Bench) [62]; see also Douglas v Hello! [2001] QB 967 (Douglas (No. 1)) [165]; Keene LJ said: ‘The photographs conveyed to the public information not otherwise truly obtainable, that is to say, what the event and its participants looked like’; Douglas v Hello! (No. 3) [2005] EWCA Civ 595, [2005] 3 WLR 881 [106] where personal images are more than just the information that is revealed; Lord Phillips M.R said: ‘Nor is it right to treat a photograph simply as a means of conveying factual information. A photograph can certainly capture every detail of a momentary even in a way which words cannot, but a photograph can do more than that. A personal photograph can portray not necessarily accurately, the personality and the mood of the subject.’


20 Douglas v Hello! [2008] 1 AC 1, 81–3 [287]–[91]; compare with 87 [307]; In Douglas v Hello! the majority held the view that images of the Douglas and Zeta Jones wedding were not trivial despite the dissenting view of Lord Walker; Lionel Bently and Brad Sherman, above n 5, 1142, 1144; Douglas v Hello! Ltd [2000] 1 QB 967, where Sedley LJ stated (at 110) that ‘we have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right to personal privacy’.
It seems that this will be the case even when the image is taken in the public domain.

5.2.2 Are the Personal Images Vague?

Another limitation placed on information protected by breach of confidence is information that is vague. This limitation traditionally excludes general ideas and concepts from protection under breach of confidence. What is deemed to be vague information is difficult to determine. Anything that is a ‘bare goal, purpose or possibility, a mere speculative idea [is] not capable of being protected’. Vague information may constitute ideas that are too broad and lack an element of novelty. The restriction on vague information is unlikely to apply to personal images shared on social networks because the limitation typically applies to commercial knowledge rather than to images.

5.2.3 Are the Personal Images Shared on Social Networks in the Public Domain?

The law of confidence will not protect personal images that are in the public domain. This is because breach of confidence cannot protect personal images without an element or degree of

---


24 Ibid.

25 The issue of novelty and originality of information is used as a restrictive mechanism on information that may not be protected. This is reminiscent of the limitations of the novelty requirement imposed in patent legislation. Novelty is not an element that has been commonly referred to when applying the breach of confidence action to protect personal images. It has been used as an argument against the protection of vague information: see Lionel Bently and Brad Sherman, above n5, 1145; DeMaudsley v Palumbo [1996] FSR 447.

26 Attorney-General and Observer Ltd v Times Newspapers Ltd [1990] 1 AC 109, 282, where Lord Goff said: ‘The principle of confidentiality only applies to the extent that it is confidential. In particular, once it has entered what is usually called the public domain (which means no more than that the information in question is so generally accessible that, in all the circumstances, it cannot be regarded as confidential) then, as a general rule, the principle of confidentiality can no application to it.’
secrecy in the personal image. Regardless of how confidential the circumstances may be, there is no breach of confidence when something is already common knowledge.\(^{27}\) When personal images are shared on social networks, they potentially fall in the public domain\(^{28}\) (this of course would not apply where the source of the image is the defendant). This is because once an image is shared on a social network, it is published. As a result, it loses its secrecy and will be in the public domain.\(^{29}\) This potentially excludes most information revealed in images placed on social network sites from being protected by the tort of breach of confidence. Without doubt this is a serious limitation on the applicability of the use of breach of confidence in this area. Again, it is important to reiterate that this does not apply where the defendant places the image in the public domain.

While, in most cases, public disclosure of information will ensure that the information loses its quality of confidentiality, there are some circumstances where information in a personal image is made available to several people but the image will still be deemed confidential. That is, there are some situations where an image can be disclosed to people and

\(^{27}\) Coco v AN Clark (Engineers) Ltd [1969] RPC 41, 47.

\(^{28}\) EPP (Australia) Pty Ltd v Levy [2001] NSWC 482 [20] per Barret J (‘everything which is accessible through the internet as being in the public domain’).

\(^{29}\) The courts have construed the notion of public domain broadly in some cases such as when the information is discussed in public then it would be considered to be in the public domain; see Lennon v News Group Ltd and Twist [1978] FSR 573, 574-5; Theakston v MGN Ltd [2002] EWHC 137 (Queens Bench); [2002] EMLR 22, 68; see generally N A Moreham, above n 21, 612–13; William van Caenegem, Intellectual and Industrial Property Law, 2nd ed (LexisNexis, Australia, 2015) 216-217; see also in relation to the anonymous sources of breaches of confidence by anonymous contributors: Australian Football League v The Age (2006) 15 VR 419, [55] where Kellam J said ‘if speculation, gossip or even assertion from an anonymous source, thus being incapable of being verified or in any way held accountable, is to be regarded as the putting of information in the public domain, then the opportunity for unethical and the malicious, to breach confidentiality and then claim that there is no confidentiality is unrestrained’.

125
without losing its quality of confidentiality. The difficulty here is determining when this will occur.

One situation where an image may retain its confidentiality even if it is disclosed on a social network is when a person shares their personal image on a social network but states that the image is confidential and restricts access to a limited audience. When people share personal images on social networks, the network may offer custom privacy settings. As a person who shares their personal image can choose their own privacy settings; this can directly affect whether an image is made publicly available or whether it is only made available to a select audience and thus remains confidential. While social networks such as Facebook, Twitter and Instagram allow people to restrict access to their images, the level and degree of control that a person is able to exercise over the image depend on the network’s privacy settings and the selected privacy settings of each person and their connections who are part of the network. Even if a person chooses to restrict access to their personal images to a selected audience, the image can still fall within the public domain. This is because third parties who have access to the image can reshare the image on their social network pages. Consequently, when an image is shared on a public social network such as Twitter or Instagram, it is likely to become part of the public domain. As such, it is unlikely to be protected by law of confidence.

While people cannot avoid being photographed in public places, it does not follow that anyone ‘who takes or obtains such photographs can publish them to the world at large’. As the court said in von Hannover, people are not ‘free to publish images of others simply because they were in a public place at the time the images were obtained’, if the information captured

---

30 Wilson v Ferguson [2015] WASC 15, [57] (Wilson J): ‘The circumstances in which the defendant obtained the images of the plaintiff were such as to impose on the defendant an obligation of conscience to maintain the confidentiality of the images. The fact that the defendant emailed copies of the sexually explicit videos to himself from the plaintiff’s phone without her knowledge or consent would of itself ordinarily be sufficient to import an obligation of confidence. This was confirmed by the plaintiff’s reaction to being informed of what the defendant had done, and the defendant’s agreement to make sure nobody else saw the photographs.’

31 NA Moreham, above n 21, 612.

The use of personal images on social networks diverts from the historic view of Prince Albert v Strange (1849) 2 DeG & Sm 652; 64 ER 293 (Knight Bruce LJ), where multiple people knew the drawings were confidential and there was a degree of control over the physical form of the drawings.

33 Campbell v MGN Ltd [2004] 2 AC 457 at 474 (Lord Hoffman).

34 von Hannover v Germany App No 59320/00, 24 June 2004.
in the image relates to their private life. While there are situations where British courts will protect information in personal images that are captured in the public domain, the law in Australia is less certain. In particular, there is uncertainty as to whether Australian courts would protect information in personal images that are captured in the public domain when the information is about a person’s private life.

5.3 Is There an Obligation to Keep the Personal Image Confidential?

The extent to which the law of confidence will protect personal images when they are misused on social networks will depend on whether there is an obligation to keep the personal image confidential. In examining whether a person sharing a personal image has an obligation to keep the personal image confidential it is necessary to consider how the obligation arises.

When thinking about the role of breach of confidence in protecting the misuse of personal images on social networks, it is important to distinguish two situations. The first is where a confidential image is uploaded onto a social network. Here the question of confidentiality of the image will depend on the situation in which the image was created and the relationship between the parties. In this case, the confidentiality arises before the image is uploaded onto the social network. The second situation is where the confidentiality arises as part of the digital and legal relationships that exist on the social network. Here the confidential obligation might arise as a consequence of contractual relations between parties or because of the relationship between the person uploading the image and the people with whom the image is shared.

---

35 See von Hannover v Germany App No 59320/00, 24 June 2004, 77 (Judges Barreto and Zupancic), where Princess Caroline of Monaco tried to prevent images of her going about her daily life from being published. The court concluded that: ‘The public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public. Even if such a public interest exists... In the instant case those interest must, in the Courts view, yield to the applicant’s rights to the effective protection of her private life’; N A Moreham, above n 21, 609; Peck v United Kingdom (2003) 36 EHRR 41; JH v United Kingdom App No 44787/98, 25 September 2001; McKennitt v Ash [2005] EWHC 3003 (Queens Bench), 50 (Eady J) ‘in light of [von Hannover, Peck, and PG and JH] a trend has emerged towards acknowledging a “legitimate expectation” of protection and respect for private life, on some occasions, in a relatively public circumstances. It is no longer possible to draw a rigid distinction between that which takes place in private and that which is capable of being witnessed in a public place by other persons.’
An obligation of confidence may arise in four ways. In some situations, an obligation of confidence arises contractually. Another situation where an obligation of confidence arises is when the parties are in a special fiduciary relationship – for example, husband and wife. In some cases, the obligation may arise from the circumstances in which the image is obtained. In some (rare) situations, an obligation of confidence may arise even where there is no relationship between the parties; that is, where the parties are strangers.

5.3.1 Contractual Relationships

Personal images may be protected under the law of confidence where there is a contractual relationship between the parties. An obligation under contract may be express or implied. When someone commissions a photographer to take pictures of them, there is usually a contractual agreement that may give rise to an obligation of confidence. However, in situations where people take photographs of other people in public spaces, there is unlikely to be a contractual relationship. The question of social networks’ contract of services was discussed in Chapter 2.

5.3.2 Fiduciary Relationships

Another way in which an obligation of confidence may arise is by way of a fiduciary relationship. Fiduciary relationships are established categories where trust and confidence are imparted between the parties. Established categories of fiduciary relationships include doctor and patient, priest and parishioner, husband and wife, solicitor and client, and trustee and

37 Argyll v Argyll [1967] Ch 302.
38 Lionel Bently and Brad Sherman, above n 5, 1160; John Glover, above n 36, 611.
39 Pollard v Photographic Co (1888) 40 Ch D 345, 352 where the Chancery held that a photographer had breached an implied term in the photographer’s contract as well as an obligation of confidence that was placed in him by the consumer. The photographer had sold Pollard’s image on a Christmas card, see further David J Seipp, ‘English Judicial Recognition of a Right to Privacy’ (1983) 3(3) Oxford Journal of Legal Studies 325, 338. In Steddal v Houghton (1901) 18 TLD 126, the court held similar views to those in Pollard, when a husband tried to restrain publication of his estranged wife and children. Also, maintaining confidentially is particularly significant where the employee is privy to trade secret or sensitive commercial information, as highlighted in Maggbury Pty Ltd v Hafele Australia Pty Ltd [2001] HCA 70 (13 December 2001). Another example is when people enter into a contract for services with social networks.
beneficiary. It is accepted that people who are in a relationship but not married to each other will also fall within the scope of a fiduciary relationship. As Mitchell J said:

The case establishes that … the intimate nature of a personal relationship between two people may give rise to a relationship of trust and confidence such that, without express statement to that effect, private and personal information passing between those people may in certain circumstances be imbued with an equitable obligation of confidence.

In these instances, if an image was captured as part of a fiduciary relationship, if one of the parties uploaded the photographs on a social network, they would be bound by the obligation of confidence. It is unlikely that parties who are digitally connected on a social network will be treated as if they are in a fiduciary relationship. Social networks such as Twitter and Instagram allow anyone to follow them and access their photographs. Facebook allows access to personal images if the person has public settings. Facebook also allows strangers and third parties access when a person ‘likes’ a particular product or a group. It is unlikely that ‘friending’ someone on a social network gives rise to a fiduciary relationship.

5.3.3 From the circumstances

Another situation where an obligation of confidence may arise is from the circumstances in which image is taken. Speaking of sexually explicit images, Wilson J said:

The circumstances in which the defendant obtained the images of the plaintiff were such as to impose on the defendant an obligation of conscience to maintain the confidentiality of the images. The fact that the defendant emailed copies of the sexually explicit videos to himself from the plaintiff's phone without her

---

40 Boardman v Phipps [1967] 2 AC 46.
42 Ibid 51.
43 Traditionally, a fiduciary duty arises in circumstances where there is trust and confidence; see further La Forest J in Lac Minerals Ltd v International Corona Resources Ltd (1989) 61 DLR 14, 28, where he said that ‘not every legal claim arising out of a relationship with fiduciary incidents will give rise to a claim for breach of fiduciary duty’. However, it would be difficult to argue that a person who is connected to a third party on a social network is in a fiduciary relationship.
knowledge or consent would of itself ordinarily be sufficient to import an obligation of confidence. This was confirmed by the plaintiff’s reaction to being informed of what the defendant had done, and the defendant’s agreement to make sure nobody else saw the photographs.44

Consequently, a person that uploads and shares sexual or intimate photographs of a third party online will be under an obligation of confidentially.

5.3.4 Where there is no relationship between the parties: Strangers

The question of whether a stranger will owe an obligation of confidence when they obtain or access images depends on the conduct of the stranger and the capacity under which they were acting.45 There are three situations where a stranger receiving personal images may be under an obligation of confidence.

An obligation of confidence may arise when personal images are obtained by unlawful conduct, for example telephoto lens photography.46 Given that when third parties and strangers obtain personal images on social networks, they are usually acquired lawfully, no obligation is owed by third parties or strangers to a person whose image has been shared.47 This would be

---

44 Wilson v Ferguson [2015] WASC 15 [57] (Wilson J) [33] he states ‘the defendant’s conduct indicates that he was well aware that the images were regarded by the plaintiff as private and that he did not have her consent or authority to show them to any other person’; see also Giller v Procopets [2008] VSCA 236 where the defendant had video recorded sexual and intimate activity of the plaintiff and threatened to show it to the plaintiff’s friends and employer. While Giller v Procopets was about a sexually explicit video of the plaintiff, it could apply by analogy to photographs. The courts are willing to protect personal images that are of a sexual or intimate nature even if they are lawfully obtained: see Wilson v Ferguson where the plaintiff had disclosed and sent some images to the defendant.

45 The distinction between lawful and unlawfully obtained personal images depends on whether the image is used for the purpose for which the information is acquired: see Malone v MPC [1979] Ch 344, 376 where, in this case, the police were authorised to phone tap the claimant’s phone line, subsequently prosecuting him for handling stolen goods.

46 Douglas v Hello! Ltd. (No3) [2006] QB 125.

47 Peck v United Kingdom (2003) 36 EHR 41; PG and JH v United Kingdom Appl No 44787/98 (25 September 2001); McKennit v Ash [2005] EWHC 3003 (Queens Bench) 50 (Eady J), who stated that ‘in the light of [von Hannover, Peck and PG and JH], a trend has emerged toward acknowledging a “legitimate expectation” of protection and respect for private life, on some occasions, in relatively public circumstances. It is not possible to draw a rigid distinction between that which takes place in private and
different however, if the images were acquired by hacking into a social network (which would be treated in a similar way to illegal phone tapping) or by comparison, phone tapping unauthorised by police.49

A second situation where a stranger may owe an obligation of confidence is when the stranger is acting lawfully but nonetheless obtains the image surreptitiously.50 Historically, the UK Court of Chancery laboured under the principle that publication of confidential information that which is capable of being witnessed in a public place by other persons’; see NA Moreham, above n 21, 609. See also, Wilson v Ferguson [2015] WASC 15 (Mitchell J). The defendant had taken photographs and videos of the plaintiff by taking her phone and emailing them to himself without her knowledge, despite the plaintiff explicitly asking the defendant not to show the images and videos to anyone else; however, once the defendant had emailed the images, he subsequently shared them on his social network account.

48 For example, in August 2014, a collection of approximately 500 private celebrity photographs were posted online and subsequently resharred on social networks: Joanne Kavanagh and Dan Cain, ‘Not Too Snap Happy What is the Rhian Sugden Naked Photo Hack and What Other Celebrity Hacked Picture Leaks Have There Been?’ 16 May 2017 The Sun, <https://www.thesun.co.uk/tvandshowbiz/3102066/rhian-sugden-kelly-rohrbach-hacked-celebrity-naked-photo-leak/>

49 See Malone v Commissioner of Metropolitan Police [1979] Ch 344. An example of illegal conduct would be phone tapping by anyone other than the police, as stated in Francome v Mirror Group Newspapers [1984] 1 WLR 892, 900, Fox LJ stated that: ‘It must be questionable whether the user of a telephone can be regarded as accepting the risk of that in the same way as, for example, he accepts the risk that his conversation may be overheard in consequence of the accidents and imperfections of the telephone system itself.’ The issue of lawfully obtaining personal images has been contested in the United Kingdom: Peck v United Kingdom (2003) 36 EHRR 41; PG and JH v United Kingdom Appl No. 44787/98 (25 September 2001); McKennit v Ash [2005] EWHC 3003 (Queens Bench) 50 (Eady J), who stated that ‘in the light of [von Hannover, Peck and PG and JH], a trend has emerged toward acknowledging a “legitimate expectation” of protection and respect for private life, on some occasions, in relatively public circumstances. It is not possible to draw a rigid distinction between that which takes place in private and that which is capable of being witnessed in a public place by other persons’; see also NA Moreham, above n 21, 609.

obtained surreptitiously ought to be restrained. The question that arises is whether a person ‘surreptitiously’ acquires an image that is not shared directly by the person disclosing the image to a third party. This may occur for example, when a stranger searches a social network and acquires a person’s image without permission.

A third situation where a stranger may owe an obligation of confidence is when a stranger obtains a personal image and has knowledge that the image is confidential. When a stranger has knowledge that the personal image is confidential, there will be a duty imposed even when that image has been acquired lawfully. Whether a stranger has knowledge of the confidential personal image and thus owes an obligation of confidence is based on a question of reasonableness. This might occur for example, where a photographer takes photographs on a film set without an invitation and there are signs prohibiting the taking of photographs in the entrance to the studio. It is the lawful conduct that imparts an obligation of confidence based on whether the stranger has knowledge of the personal image.

5.4 Has there been a Breach of Duty?

The third factor that needs to be proved in an action for a breach of confidence is that the personal images were used in a way that breaches the obligation of confidentiality. There are various factors that determine the scope of the obligation and thus whether it is breached. These relate to how the personal image is given, whether the information in the image was sensitive,

---

51 Lord Ashburton v Pape [1913] 2 Ch 469, 465 (Swinden Eady LJ) ‘The principle on which the Court of Chancery has acted for many years has been restrain the publication of confidential information improperly or surreptitiously obtained or of information imparted in confidence which out not to be divulged.’

52 For example, on Facebook’s graph search function, third parties can search for images that have been uploaded and shared by people with their connections.

53 There is some debate whether the key issue is knowledge or the unlawful conduct as highlighted in Attorney – General v Guardian (No. 2) [1990] AC 109 at 281–2 (Lord Goff).

54 In Shelly Films v Rex Features [1994] EMLR 134, His Honour Mann QC noted that the lack of regard for the claimants’ signs stating ‘no photography’ and ‘access to authorised persons’ could only be considered as confidential. Compare with Francome v Mirror Group Newspapers [1984] 1 WLR 892 and Shelly Films v Rex Features [1994] EMLR 134; in Shelly Films it was distinguished from Francome with emphasis on the knowledge and not the illegality of trespassing and taking the photograph. This is also seen in situations where paparazzi photographers obtain images of celebrities and publish them in magazines: Douglas v Hello! [2001] 2 WLR 992.

55 Lionel Bently and Brad Sherman, above n 5, 1163; see Wilson v Ferguson [2015] WASC 15.

56 Ibid 1142.
and the extent of interest in the use of the personal image by the person providing the photograph.

The defendant must use the personal image imparted by the confider for there to be a breach of confidence. The personal image cannot be derived from another place or source. There is no requirement to examine the defendant’s state of mind as in criminal law. It is not necessary for a plaintiff to demonstrate that the defendant’s breach was a conscious or deliberate action.57 Consequently, the defendant will not be able to rely on arguments that they acted in good faith, that they were ignorant of the nature of confidentiality of the personal image or that they accidentally used of the image as a way of side stepping their liability for a breach of confidence.58 This is in contrast to the requirement for establishing the defendant’s obligation.59

It is unclear whether the plaintiff must suffer damage or harm before an action of breach of confidence can be initiated.60 Whether damage is a crucial element remains dependent on two factors: the type of personal image and the definition of damage/harm.61 Where breach of confidence relates to personal or private information in photographs, it has been suggested that there is no requirement to prove damage.62 A claimant need only prove that there has been an invasion of their private life, not that there has been a detriment.63 Essentially, the issue of detriment may be fashioned as an invasion of private life because the invasion is the detriment suffered by the claimant.64

In many cases, the misuse of a personal image is easily determined. Anything that is in contrast to the confider’s instructions about the use of the personal image will be deemed to be a breach. There are other circumstances where the misuse of the information needs further examination. These circumstances surround the actual information – for example, where the personal image used is different from the original personal image disclosed.65 The information

58 Weld-Blundell v Stephens [1919] 1 KB 520.
59 Lionel Bently and Brad Sherman, above n 5, 1072–5.
60 Ibid.
64 This was highlighted in McKennitt v Ash [2008] QB 73.
65 Memes encompass various subject matter, however for the purposes of this thesis, the term meme is in reference to personal images that have been adapted and modified with various phrases and spread on the internet. Memes are defined as ‘a cultural item in the form of an image, video, phrase, etc., that is spread
does not have to be identical to be breached, it can still be a breach if it appears in a different form.\(^{66}\) This raises the question of how different the information can be for it to constitute a breach. This is problematic when considering information that is personal because in these situations the degree of similarity does not have to be significant.\(^ {67}\) Any altered personal image raises the question of whether the extent of the image is different from the originally shared personal image. This essentially depends on whether the altered information is a continuation of the information from which the altered information is derived.\(^ {68}\)

5.5 Possible Defences

When personal images are misused on social networks, it is important to consider whether there are any potential defences to an action of breach of confidence. There are two main defences that are available to a defendant in an action for breach of confidence relevant here: consent and public interest.

5.5.1 Consent

The issue of consent is one that may absolve the defendant from any liability. Essentially, if the defendant can demonstrate that the plaintiff authorised or consented to the use of the personal image in such a way then they will not be liable. This arises through express licence agreements or contractual arrangements. This may not be an issue that arises when the nature of the information relates to personal images and there is no licence agreement or contractual arrangement in place. This may occur for example where two parties are in an intimate relationship with one another.\(^ {69}\) The issue of consent in relation to the use of personal images arises when considering the terms of use agreements as noted in chapter 2.

---

\(^{66}\) via the Internet and often altered in a creative or humorous way’: Dictionary.com, [http://dictionary.reference.com/browse/meme](http://dictionary.reference.com/browse/meme)

\(^{67}\) Lionel Bently and Brad Sherman, above n 5, 1072–5.

\(^{68}\) Ibid.


5.5.2 Public Interest

In the United Kingdom, the public interest defence is commonly used to safeguard genuine public interests in revealing information that may pose serious danger to the public.70 The British courts have attempted to apply a liberal approach of a breach of confidence action to protect personal images and privacy interests. However, application of the public interest defence has largely been in relation to trade secrets. In some instances, the courts have applied the public interest defence to accidently obtained information or surreptitiously obtained information.71 The position in the United Kingdom has favoured a much broader approach to the public interest defence and balancing the interests of the public, freedom of speech and confidentiality.72 The status of the public interest defence in Australia is less certain. At best, Australian courts have taken a narrow approach to the public interest defence.73 At worst, they have denied its existence. According to


71 Lord Ashburton v Pape [1913] 2 Ch 469 475 (Swinden Eady LJ); Argyll v Argyll [1965] 1 All ER 611. In Lord Ashburton v Pape, His Lordship Swinfen Eady suggested that any information obtained improperly or surreptitiously by anyone would be liable for a breach of confidence; see Megan Richardson, above n 6, 690.

72 While the European Convention of Human Rights provides the right to freedom of expression, it is independent from the public interest defence: see Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), Art 10; Lionel Bently and Brad Sherman, above n 5, 1187.

73 Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd [1987] FCA 266 (13 August 1987) [57] where Gummow J states ‘That principle, in my view, is no wider than one that information will lack the necessary attribute of confidence if the subject matter is the existence or real likelihood of the existence of an iniquity in the sense of a crime, civil wrong or serious misdeed of public importance, and the confidence is relied upon to prevent disclosure to a third party with a real and direct interest in redressing such crime, wrong or misdeed’; see Smith Kline and French Laboratories (Aust) Ltd v Secretary, Dept of Community Services and Health [1990] FCR 73, 111 where Gummow J states that:

(i) an examination of the recent English decisions shows that the so-called ‘public interest’ defence is not so much a rule of law as an invitation to judicial idiosyncrasy by deciding each
Kellam J, the ‘correct legal position is that there is no general public interest defence.’ Further he acknowledged that this issue is not ‘determined authoratively’ and that the ‘public interest must amount to more than a public ‘curiosity’ or public ‘prurience’.’

5.6 Conclusion

While the Australian law of confidence provides some protection for personal images placed on social network sites, this protection is very limited. One reason for this is that the law of confidence will not protect images that are in the public domain.

Another reason to the limited protection is that the law of confidence has not expanded to protect information that is about a person’s private life. While Australian law has attempted to expand the tort of breach of confidence to include private information to protect specific types of personal images such as those of an intimate nature – it has not developed in to protect personal images that are not intimate or of a sexual nature. The Australian law of confidence varies from its UK counterpart because there it does not extend or protect a person’s ‘private life’. As a result, the protection of a person’s private life is not strongly entrenched in Australian jurisprudence. It is clear that the law of confidence in Australia does little to prevent the misuse of personal images when those images are shared on social networks.

---

74 Australian Football League v The Age Company Ltd (2006) 15 VR 419, [74] Further, Kellem J at [75] stated: ‘It is true that the existence of, and/or the extent of, any public interest defence to a breach of confidentiality is by no means clear and settled in Australia.’

75 Ibid at 84. He cited Lord Wilberforce in British Fuel Corporation v Granada Television Limited [1981] AC 1096, 1168 ‘… There is a wide difference between what is interesting to the public and what it is in the public interest to make known.” at [94] This case also related to the disclosure of names of Australian football players who had tested positive to illicit drugs, the disclosure of the names would not have been in the public’s interest but merely to satisfy the public’s curiosity.


77 The United Kingdom, law of confidence incorporates Article 8 of the European Convention of Human Rights and thus provides a broader scope of protection than Australian law.
Part II

Possible Solutions
Part I of the thesis examined the legal protection for personal images uploaded and shared on social networks in Australia. This revealed that while Australian law provides some protection, the protection is very limited.

A number of issues potentially arise when images are uploaded on social networks. One occurs when a person takes and uploads their photograph and that image is reused and reshared online. Here, the law provides limited protection. For example, copyright protects against misuse of the image in some situations – such as when people take photographs of themselves and shares them on a profile page; however, in some situations when the use falls within the defence of fair dealing – notably where the image is used to report the news or the image is used for parody or satire purposes – the reuse of an image may not constitute a copyright infringement. Other areas of law, such as privacy, the law of confidence, and contract are also of little use. For example, privacy law will not prevent the misuse of a person’s image when that image has been reshared online. While there is some protection for personal images under the Privacy Act 1988 (Cth), the protection is inadequate. The reason for this is that the Privacy Act only applies to government agencies and departments, and to Australian corporations that collect, use and disclose images; the Privacy Act does not apply to individuals who collect, use and disclose personal images on social network sites. Another limitation of the Privacy Act is that personal images shared on social networks are not protected when journalists use them for journalistic purposes.

While in some cases the law of confidence potentially provides protection when a person shares their image online, this protection is limited. There are many problems here, the key one being that the law of confidence does not protect personal images that fall within the public domain. The problem here is that when people share and exchange personal images on social networks, the images fall within in the public domain. This means that they lose the condition of confidentiality; this is the case even if the images that are disclosed are private and access is restricted.

When images are reshared and reused are exacerbated by the fact that when a person enters into a social network contract, they often sign away many of their intellectual property rights. Social network contracts usually contain wide licence terms that enable a social network to use, reuse and sub-license their photographs. The consequence of this is that when a person becomes a member of a network, they give the network a very broad licence over the use of their images. This facilitates the misuse of personal images. These problems are made worse by the fact that social networks can alter the terms of service without allowing the users to negotiate the terms.
Another problem that potentially arises when personal images are shared online is when third parties distort or alter the images. This occurs, for example, when third parties turn photographs into memes. The legal protection here is limited. In rare cases, copyright may offer protection. When an image is reshared and reused without attributing the creator of the image, this may amount to a breach of the moral right to attribution.\(^1\) While this offers some protection, it is limited in that the only person who can bring an action for breach of attribution of authorship is the photographer.\(^2\)

Potential problems also arise when the circumstances surrounding the uploading of an image change. This may occur, for example, when a person uploads and shares an image on a social network page, but later changes their mind about uploading the image, or when the creator of the uploaded image dies. While a person is able to remove or delete images that they have uploaded on their own profile page, when they change their mind about sharing the image, they are not able to delete images that have been reshared by third parties, because those images are now stored on third-party profile pages. Problems also arise when a person who uploads images on a social network page dies. When a creator of an image dies, the copyright in the image will pass to the deceased person’s estate. However, the problem here is that when a person signs up to a social network, they effectively assign their copyright to the network.

Problems may also arise when third parties capture photographs of other people and upload those images onto social networks. In this situation, many of the problems outlined above apply. One additional problem that arises here relates to the very act of taking of the photograph and the uploading of that image. When this happens, there is no protection to speak of. When people take photographs of third parties and share those images online, the subject is not able to prevent the use of their image under copyright. Because copyright law protects the form of a copyright work and not the subject matter, copyright protection does not extend to the person whose image is captured in a photograph. This means that the subject of a photograph has no rights under copyright law. The lack of copyright protection for people whose images are captured in photographs and shared online means any protection for the subject of a photograph must be sought under other legal areas, such as the law of confidence, contract or privacy law.

---

One area that offers a potential remedy when a third party captures another person’s image in a photograph is breach of confidence. However, protection under the law of confidence is limited by the fact that any rights a subject has in an image will end when the image is placed in the public domain. This is the case even if the image is private or personal. Unlike in the United States, there are no image rights in Australia on which people may rely when they are photographed. One of the ramifications of this is that a person cannot prevent a third party from photographing them in a public or even a private place. Another ramification of not having any image rights is that a subject cannot control the use of their image or the information captured in the image after their photograph is taken.

While there is some protection for personal images that are shared online in Australia, this protection is limited. Part II of the thesis explores three possible areas that could potentially close the gaps that exist in the law in Australia. The first is a statutory tort of serious invasions of privacy. The second is the introduction of ‘image rights’ or a ‘right to publicity’ in Australia. The third option that is examined is a ‘right to be forgotten’. In exploring these three areas, Part II will argue that if adopted collectively, there is potential for these three areas to alter the legal protection that exists for personal images that are uploaded and shared online in Australia.
Chapter 6
Expanding Privacy Law

6.1 Introduction

There are a number of significant gaps in the legal protection available for personal images that are shared on social networks in Australia.¹ This chapter examines the potential role that a new statutory tort for serious invasions of privacy might play in protecting personal images shared online from misuse. Specifically, the chapter examines two proposals made by the ALRC in its 2014 report, Serious Invasions of Privacy in the Digital Era.² The first is that a statutory tort for serious invasions of privacy should be introduced. If enacted, the tort for serious invasion of privacy would cover two types of serious invasions of privacy:³ ‘intrusion upon seclusion’ and ‘misuses of private information’. The ALRC also recommended that in the absence of a statutory tort, the tort of breach of confidence ought to be expanded to include private information. The chapter will look at each of these proposals in turn. It will then examine whether the ALRC’s recommendations, if adopted, would protect personal images that are shared online. In examining the proposed reforms, it will be argued that while the changes would provide some improvements the reforms do not adequately address the gaps in the existing legal protection.⁴

¹ The Australian Law Reform Commission has made numerous recommendations for privacy reform over the years. For example, since Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479, the Commonwealth government has commissioned investigations that resulted in the enactment of the Privacy Act 1988 (Cth); see further Australian Law Reform Commission, Privacy, Report No 22 (1983), xxxvi, xxxvii and Chapters 9–11.
³ Ibid.
⁴ The Australian government has yet to make any significant responses to the ALRC’s recommendations. This is in contrast to New South Wales established a parliamentary inquiry. The Legislative Council’s Standing Committee Law and Justice has been conducting an inquiry.
6.2 A New Statutory Tort of Invasion of Privacy for Serious Invasions of Privacy

The current legal protection of personal privacy in Australia is piecemeal and fragmented. As noted previously, the avenue for redress for intrusions upon seclusion is limited to tortious actions such as trespass to property and trespass to person. The existing privacy law is also inconsistent. Even though the ALRC highlighted the problems in the law, there have not been any significant reforms to bridge the gaps in Australian law.

One of the ALRC’s key recommendations was that the Commonwealth government should enact a statutory tortious cause of action for serious invasions of privacy that would cover two new types of serious invasions of privacy: ‘intrusion upon seclusion’ and ‘misuse of private information’. These types of invasion of privacy are based on US privacy law.

---


7 See Australian Law Reform Commission, Unfair Publication: Defamation and Privacy, Report No. 11 (1979) 228; the report highlighted gaps in the law such as identification of sexual assault victims; identification and publication of addresses and name of a witness of murder; media photographs of two 15-year-olds who eloped; filming individuals in the street without their consent; and paparazzi taking photographs of a woman giving birth to quadruplets.

8 See further Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Report 123 (2014) 4, 4-1 and 4-2, which states: ‘Recommendation 4-1 A new tort in a New Commonwealth Act. Two Types of Invasions, Recommendation 4–1 if a statutory cause of action for serious invasion of privacy is to be enacted, it should be enacted by the Commonwealth, in a Commonwealth Act (the Act)’; See Recommendation 4–2 the cause of action should be described in the Act as an action in tort; Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Report 123 (2014), 5: 5.15, Recommendation 5-1.


10 US privacy law includes four different types of tortious actions: for breaches of privacy intrusion upon the plaintiff’s seclusion or solitude, or into their private affairs; public disclosure of embarrassing private facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; and appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness’. William L Prosser, ‘Privacy’ (1960) 48 California Law Review 383, 389. The ALRC confined an Australian statutory tort to the first two categories. In 1960, Prosser stated that the law of privacy comprised four ‘distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but
following sections examine the two types of tortious action for serious invasions of privacy. This section also considers whether the two types of tortious actions would be likely to prevent the misuse of personal images that are shared, uploaded and exchanged on social networks.

6.2.1 Intrusion Upon Seclusion

The first type of serious invasion of privacy recommended by the ALRC is ‘intrusion upon seclusion’.11 While intrusion upon seclusion is not specifically defined in the ALRC report, intrusion upon seclusion is based on American jurisprudence.12 In the United States, intrusion upon seclusion is defined as situations where a person:

intentionally intrudes, physical or otherwise, upon the solitude or seclusion of another or his private affairs or concerns is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.13

A number of questions arise when considering whether the proposed new tort would play a role in preventing the misuse of personal images on social networks. The first is whether the tort would apply to digital spaces; that is, whether the tort would apply to personal images that are shared on social networks. The second is whether uploading images on a social network page is an intrusion. The third is whether the tort would protect all types of information captured in personal images that are shared online.

______________________________
12 See generally William L Prosser, above n 10.
13 See American Law Institute, Restatement of the Law Second, Torts (1977), § 652B.
6.2.2 Is a Social Network Page a ‘Secluded’ Space?

According to the ALRC, the tort of intrusion upon seclusion involves unwanted physical intrusion into someone’s private space.\(^{14}\) It is clear that the tort applies to intrusions into private physical spaces of individuals. Typically, it applies when someone’s physical space has been interfered with, such as when people watch, listen, or record a person in their home. One issue that is unclear is whether a *secluded* space needs to be a *private* space. That is, would a photograph taken in a public space be protected? Would, for example, a park be considered to be a secluded place? While in most cases this would not be the case, one situation where a park may be a secluded place is when photographs are taken of homeless people. Even though a park is a public place, as homeless people have no specific private place, it may be treated as a secluded space.\(^{15}\)

Another question that arises is whether a social network page would be seen as a secluded space. While seclusion is not defined in the ALRC report, the meaning of the term is drawn from the United States *Restatement of Law, Torts* which states that:

> by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff’s room in a hotel or insists over the plaintiff’s objection in entering his home …\(^{16}\)

The intrusion itself makes

---


the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.\textsuperscript{17}

It is arguable that in some limited cases a profile page may be ‘a place of seclusion’.\textsuperscript{18} Social networks such as Facebook, Twitter and Instagram are public and semi-private networks which provide users with the ability to restrict access for users to their images. Even though Twitter allows people to share images publicly, there is some ability to restrict access.\textsuperscript{19} For example, Facebook’s privacy settings allow people to have a closed group or limit access to ‘only me’, ‘friends’, or ‘friends of friends’. When a person chooses the ‘friends of friends’ access setting third parties can access and view the images a social network page would not be a secluded space. However when a person has a profile page with restricted privacy settings such as ‘only me’ or a ‘closed group’, it could be argued that their profile page is a secluded space.\textsuperscript{20} Given that social networks allow users to create groups that are closed or ‘secret,’ a social network space may in limited situations be a secluded space.\textsuperscript{21} This will depend on the nature of the settings used.\textsuperscript{22}

\textbf{6.2.3 \textit{Is Uploading an Image on a Social Network Page an Intrusion Upon Seclusion?}}

The decision of what qualifies as an \textit{intrusion} upon seclusion depends on a number of different factors. Intruding on a secluded space may occur (in this context) in three situations. The first is in the taking of a photograph of a person. The second is in uploading the image. The third is when a personal image is viewed or accessed.

In addition to physical encroachment into someone’s private space, intrusion upon seclusion includes the act of watching, listening, or recording private activities or affairs.\textsuperscript{23} The

\textsuperscript{17} Ibid.
\textsuperscript{18} Ibid.
\textsuperscript{20} Adam Pabarcus above n 19, 406.
\textsuperscript{21} See Adam Pabarcus, above n 19, 401-403.
\textsuperscript{22} For example, Facebook users can access the profile page, even if the parties are not connected directly – for example, friends, or friends of friends. See generally, Adam Pabarcus above n 19.
taking of a photograph of a person engaged in a private activity, would be an intrusion, because the taking of a photograph of a person is a record. 24

The question of whether someone intrudes on another person’s secluded space when they upload a photograph of that person or when they view a photograph that is online may depend on the privacy settings that are selected. Arguably a person who uploads an image of a third party engaged in a private activity to an open site would be intruding on the third party’s private space because the photograph is a record of a private activity. A person who accesses an image that was uploaded on a public site by someone else would not be intruding on a secluded space, because there are no restrictions on the accessibility of the uploaded images. The position would be different however, when an image is uploaded to a closed site. A person who uploads an image of another person on a social network site that is closed would less likely to be an intrusion. The position would be different, however where a third-party hacks into a closed or restricted site and views images. 25 In this case, this would likely to be an intrusion.

6.2.4 Scope of Protection

Another issue that will impact upon the effectiveness of the tort of intrusion upon seclusion in protecting personal images that are shared online relates to its scope. It is clear that the tort will protect against the misuse of personal, private and intimate images. As the ALRC noted, recording private activities is ‘more likely to be a serious invasion of privacy’.26 While private and personal activities were not defined in the ARLC report, the terms ‘private’ and ‘personal’

24 N. A. Moreham, above n 14, 354-5. The author suggests that taking photographs of a person’s private activities or disseminating photographs of the private activities fall within the scope of intrusion upon seclusion.
25 See generally, Adam Pabarcus above n 19.
have been defined to include images that are ‘sexual or intimate’ in nature. This would also include images that capture people changing or semi-clothed.

While the tort will protect against the misuse of personal, private and intimate images, it is less clear whether the tort will cover images of ordinary, everyday situations such as photographs that capture people eating, sleeping, walking or laughing. Generally, the question of whether a non-sexual or non-intimate image will be protected will depend on whether there is a reasonable expectation of privacy when people are photographed. There are no specific rules that apply when considering whether ordinary images are protected under the tort; however, it appears as though the scope is narrower for personal images that are taken in public places.

6.3 Effectiveness of the Tort in Protecting Personal Images Shared Online

While the proposed tort of intrusion upon seclusion would address some of the gaps in the law, there are a number of issues that are not addressed. One problem that arises is that the proposed tort does not deal with situations where ordinary personal images are uploaded and shared on social networks – for example, when people’s images are captured in everyday moments such when they are sleeping or in embarrassing or intimate moments in their homes, at family gatherings, or public places.

---

27 See Giller v Procopets (2008) 79 IPR 489, Wilson v Ferguson [2015] WACA 15; Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Report 123 (2014), 5.2–5.3, 73; see also submission by Electronic Frontiers Australia, Submission 44 ‘posting of photographs, audio-recordings, and video-recordings of personal spaces, activities, and bodies for which consent to post has not been expressly provided by the participant.’


30 However, in the United Kingdom, some activities such as walking on a street or taking a child for a walk in the park may be protected as a private activity. See Campbell v MGN Ltd [2004] 2 AC 457; von Hannover v Germany App No 59320/00 (24 June 2004); Murray v Express Newspapers PLC [2007] EWHC 1908.


32 Australian privacy law contrasts with that of the United Kingdom because British common law expanded to include ‘misuses of private information’. The expansion of British common law of confidence was the
Another problem with the tort is that it is uncertain whether photographing people in public places would be protected. Currently, Australian law does not prevent people from being photographed in public places.\(^{33}\) Whether the proposed tort would protect personal images captured in public places would depend on whether there is a reasonable expectation of privacy.\(^{34}\) Without a reasonable expectation of privacy, it is unlikely that a tort of intrusion upon seclusion would be actionable. The upshot is that even if Australia adopted a tort of intrusion, it would still be inadequate to protect personal images online.

### 6.4 A Misuse of Private Information

The second type of serious invasion of privacy recommended by the ALRC is when there is a misuse or disclosure of private information, irrespective of whether that information is true or not. This mirrors the United Kingdom’s expanding tort of breach of confidence, as well as developments in other jurisdictions such as United States, New Zealand and Canada, which have recognised a tort for misuse of private information.\(^{35}\) In considering whether a tort of misuse or disclosure of private information would protect personal images that are shared on social networks, it is important to determine whether the misuse or disclosure of a personal

---

33 The ALRC acknowledged that Australian law was not in line with other jurisdictions such as the United Kingdom, Canada, the United States and New Zealand where images of people captured in public places have been protected.

34 Jonathan Morgan, ‘Privacy Confidence, and Horizontal Effect: “Hello” Trouble’, *The Cambridge Law Journal* [2003] 62(2) 444, 446 Morgan argues that there may be an expectation of privacy when in public just because people: ‘venture into the public, in order to further our private lives; we do not *ipso facto* relinquish all claims to a private sphere. Even tacit consent to being observed by other cannot automatically extend to their taking and a fortiori publishing photographs’; David Rolph, ‘Looking Again at Photographs and Privacy: Theoretical Perspectives on Law’s Treatment of Photographs as Invasions of Privacy’ in Anne Wagner and Richard K Sherwin (eds), *Law, Culture and Visual Studies* (Springer, 2014), 205, 224; see generally, D Feldman, ‘Privacy as a Civil Liberty’ (1994) 47(2) CLP 41.

35 The House of Lords were given the opportunity to examine a privacy claim based on breach of confidence in *Campbell v MGN Ltd* [2004] 2 AC 457, 464 (Lord Nicholls). While there was no question of extending the action of breach of confidence for an invasion of privacy for disclosure of private information, it was considered that breach of confidence may be misleading. In that decision, Lord Nicholls said that breach of confidence ‘harks back to the time when the cause of action was based on improper use of information disclosed by one person to another in confidence’.
image would be an invasion of privacy. There are three key elements for an action of a tort of misuse of private information. The first is that there must be private information. The second is that there must be a reasonable expectation of privacy in relation to the information in question. Third, the disclosure of the private information must be highly offensive to a reasonable person.

6.4.1 What is ‘Private Information’?

It is uncontested that photographs are not only information, but also a superior form of information. It was shown earlier that photographs fall within the definition of personal information. In particular, photographs capture all kinds of information that can be private and personal. The key question here is whether the information is ‘private’. According to the ALRC, ‘private’ information means ‘information as to which a person in the position of the plaintiff has a reasonable expectation of privacy in all of the circumstances’. Whether something is

36 The 2014 ALRC report, Recommendation 5–1 recommended that ‘private information include untrue information if the information would be private if it were true’. In particular, at 5.55 the ARLC states: ‘it should be stressed that for the plaintiff to have an action under the privacy tort in this Report, the other elements of the tort would of course have to be satisfied. The untrue information would have to be a matter about which the plaintiff had a reasonable expectation of privacy and the misuse would have to be serious.’ See also Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Report 123 (2014), 5, ‘Two Types of Invasion’, 5.36–5.55, <https://www.alrc.gov.au/publications/5-two-types-invasion/misuse-private-information>.

37 Hosking v Ruting (2005) 1 NZLR 1, where the court accepted a new tort of invasion of privacy by making private facts public. Further, at [117] Gault P and Blanchard JJ considered two requirements for a successful claim, based on the ‘existence of facts in respect of which there is a reasonable expectation of privacy’ and ‘publicity given to those private facts that would be considered highly offensive to an objective reasonable person’.

38 See David Rolph, above n 34, 224.

private will depend on the circumstances of the case.\textsuperscript{40} In \textit{ABC v Lenah Game Meats},\textsuperscript{41} Gleeson CJ said that the test for determining whether something is private depends on whether the disclosure of the information would be ‘highly offensive’.\textsuperscript{42}

In some situations, determining whether something is private will be relatively straightforward. For example, sexual or intimate images will fall within the scope of private information.\textsuperscript{43} It could also be argued that ‘private’ would include photographs that capture information that relates to a person’s health, finances, personal relationships or finances.\textsuperscript{44} While in these situations it is relatively easy to determine whether the image would be private, in other cases it may be difficult to determine. This is particularly the case in relation to


\textsuperscript{41} (2001) 208 CLR 199.

\textsuperscript{42} \textit{Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd} (2001) 208 CLR 199 [42] (Gleeson CJ), who stated that, ‘Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. \textit{The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.’ } Emphasis added.


\textsuperscript{44} \textit{Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd} (2001) 208 CLR 199, [42] (Gibson C J).
embarrassing or humiliating images captured in public. This is because it is difficult to distinguish between what is and what is not private. As Gleeson CJ said in *Lenah*:

There is no bright line, which can be drawn between what is private and what is not. Use of the term ‘public’ is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford.

### 6.4.2 Is There a Reasonable Expectation of Privacy?

The second requirement that needs to present for the proposed tort to apply is that there must be a reasonable expectation of privacy. As noted in by Lord Nicholls in *Campbell v MGN*, ‘the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy’. Given that Australian law has not developed to the same extent as the United Kingdom, in framing the proposed tort, the ALRC looked to the United Kingdom for guidance in order to determine what would constitute a reasonable expectation of privacy. The ALRC recommended a number of factors that Australian courts could take into consideration when determining whether a person would have a reasonable expectation of privacy including the nature of the information (whether it relates to intimate or family matters, health, medical or financial matters), the ‘means that used to obtain the private information or

---

45 For example people may consider a photograph to be private if they are photographed when they are drunk, in embarrassing or humiliating situations, such as when Todd Carney was photographed urinating and the image was uploaded online, or when Mitchell Pearce was filmed intoxicated: see Cameron Tomarchio, ‘World Reacts to Mitchell Pearce’s Dog Act’, *News.com.au* (28 January 2016) <http://www.news.com.au/sport/sports-life/world-reacts-to-mitchell-pearces-dog-act/news-story/60e1653fd0b2ff0b0a326aafddf08627>.

46 *Lenah Game Meats Pty Ltd* (2001) 185 ALR 1, 13 [42] (Gleeson CJ).

47 *Campbell v MGN Ltd* [2004] 2 AC 457, [21].


49 Ibid.
to intrude upon seclusion,’\textsuperscript{50} whether the intrusion occurred at the person’s home, the purpose of the misuse, disclosure or intrusion, the way that the private information was held or communicated, whether the private information was already in the public domain, the attributes of the plaintiff (for example age, occupation and cultural background) and the conduct of the plaintiff. \textsuperscript{51} The ALRC also suggested that the court should:

consider not whether the plaintiff subjectively expected privacy, but whether it would be reasonable for a person in the position of the plaintiff to expect privacy. The subjective expectation of the plaintiff may be a relevant consideration, particularly if that expectation was made manifest, but it is not the focus of the test, nor an essential element that must be satisfied.\textsuperscript{52}

As noted by Lord Hope in \textit{Campbell v MGN} the test for whether there is a reasonable expectation of privacy is whether the person sharing the personal image ‘knows or ought to know that there is a reasonable expectation that the information in question will be kept confidential’.\textsuperscript{53} Given that being able to restrict access to a personal image may warrant a belief that there is a reasonable expectation of privacy, even if the photograph is published on a social network. There may be a reasonable expectation of privacy when an image is shared online and access to that image is restricted. It could be argued that when a social network enables a person to control access to their personal images, there ought to be an expectation of privacy. This would depend on the social network’s privacy features (and whether a person has customised their access settings).

While there is a likely to be a reasonable expectation of privacy where the image relates to a person’s home life or family life,\textsuperscript{54} it is unclear whether there would be a reasonable expectation of privacy when people are photographed in semi-public places or where the images capture sensitive information such as religious information\textsuperscript{55} (such as when people are photographed attending mass or while praying in places of worship and the photographs are

\textsuperscript{50} Ibid.
\textsuperscript{51} Ibid.
\textsuperscript{52} Ibid 6.7.
\textsuperscript{53} \textit{Campbell v Mirror Group Newspapers Ltd} [2004] 2 AC 457, 480.
\textsuperscript{54} For example, in the United Kingdom, privacy protection extends to private information about a person’s family or private life.
\textsuperscript{55} While the term ‘serious’ was discussed previously, it includes images that capture sensitive or sexual activity: see further \textit{Wilson v Ferguson} [2015] WACA; \textit{Giller v Procopets} (2008) 79 IPR 489.
To the extent that this is a concern, it would appear that the effectiveness of the proposed tort in protecting personal images that are captured in public places would be limited.

### 6.4.3 Is the Disclosure of Private Facts Highly Offensive to a Reasonable Person?

The third requirement that must be satisfied to show a misuse of private information is that the disclosure of private facts is ‘highly offensive to a reasonable person’. The ALRC noted that the question of whether a disclosure of private information is highly offensive should be left to the courts to determine.\textsuperscript{57} Using an objective test would be in line with other jurisdictions such as the United Kingdom, New Zealand and the United States.\textsuperscript{58}

It should be noted that the ‘highly offensive’ test has been questioned in other jurisdictions; specifically in the United Kingdom, where the British courts suggested that the test could be confusing. Specifically, Lord Nicholls stressed that there were two reasons why the test should be used with caution:\textsuperscript{59}

First, the ‘highly offensive’ phrase is suggestive of a stricter test of private information than a reasonable expectation of privacy. Second, the ‘highly offensive’ formulation can all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which publication was a matter of proper public concern. This could be a recipe for confusion.\textsuperscript{60}

---

\textsuperscript{56} For example, information that relates to a person’s religion is deemed sensitive information under s 6(1) of the Privacy Act (Cth) 1988.

\textsuperscript{57} See also Australian Law Reform Commission, *Serious Invasion of Privacy in the Digital Era*, Report 123 (2014) 6.22, which states: ‘The ALRC considers that the offensiveness of a disclosure or intrusion should be one matter able to be considered by a court in determining whether there is a reasonable expectation of privacy. It is more reasonable to expect privacy, where a breach of privacy would be considered highly offensive. As discussed in Chapter 8, offence may also be used to distinguish serious invasions of privacy from non-serious invasions of privacy.’

\textsuperscript{58} Ibid 6.14.

\textsuperscript{59} *Campbell v MGN Ltd* [2004] 2 AC 457, [22].

\textsuperscript{60} Ibid.
6.4.4 Expanding the Law of Confidence to Include Private Information

In the event that a statutory tort was not enacted, the ALRC proposed that the Australian law of confidence should be expanded to include ‘private information.’ This would bring Australian into line with other jurisdictions such as the United Kingdom where the law of confidence has been expanded to include ‘private information’. This was done to ensure that British courts complied with the *European Convention of Human Rights* which protects a person’s private or family life. As Lord Hoffman said, ‘the right to control the dissemination of information about one’s private life’ is central to a person’s privacy and autonomy. In order to comply with Article 8 of the *European Convention of Human Rights*, the British courts expanded the law of confidence to include the misuse of private information to avoid establishing a new statutory tort. In so doing, the courts substituted the requirement of keeping information confidential with the requirement that the information should be kept private.

Private information protected by an expanded law of confidence would be breached in a number of ways. The first is where a person discovers information about a third party such as bank records, health information, reading a diary or hacking into a person’s email. Another way that information could be breached is where a person retains private information about a third party, such as retaining private records or information for their own future reference or ‘with a view to sharing the information with others (by building up a computer file or secret dossier). Private information would also be breached where a third party photographed the

---

64 See Tatiana Synodinou above n 63.
65 See Nicole Moreham, above n 14, 354 where she suggests that keeping things private is when ‘someone is finding out something about you against your wishes. He or she is learning that you have a sexually-transmitted infection, that you enjoy cross-dressing in private, that you run your home in a particular way, that you are having relationship difficulties, or that you are the anonymous author of a popular blog’.
66 Nicole Moreham, above n 14, 351, 355. The author suggests that there are ‘three sub-categories of invasions, such as finding out things about people they wish to keep private, keeping things private and
private activities of another person or disseminated the photographs of the private activities to third parties. Information may also be breached in situations where a person discloses private information about another person such as "by passing on gossip, uploading facts, photographs or other material to the Internet, or disseminating it in the media."\(^67\)

As misuse of private information is very broad, it would cover many of the different ways that private information may be misused online. It is clear that personal images that are shared online would fall within the misuse of private information because an intrusion of privacy would potentially occur at three particular junctures; at the time of taking the photograph, uploading the image and each time the image is viewed or accessed.\(^68\)

Expanding the tort of breach of confidence in Australia to include the misuse, disclosure or publication of private information would provide some protection where a personal image is private but not of a sexual or intimate nature.\(^69\) Even if the existing law of confidence was expanded it would not provide people with adequate protection to prevent the misuse of their disclosing private information by either sharing it on the internet or media or passing it on through gossip’; the ALRC also recommended that the Act include collecting and disclosing private information: ALRC, Serious Invasion of Privacy in the Digital Era, 5 Two types of invasions, Misuse of Private Information <https://www.alrc.gov.au/publications/5-two-types-invasion/misuse-private-information>.\(^67\)

Nicole Moreham above n 14, 351, 355.\(^68\)

As Lord Phillips of Worth Matraver MR said in Douglas v Hello! Ltd (No. 3) [2006] QB 125, 161–2: ‘Once intimate personal information about a celebrity’s private life has been widely published it may serve no useful purpose to prohibit further publication. The same will not be necessarily true of photographs. In so far as a photograph does more than convey information and intrudes on privacy by enabling the viewer to focus on intimate personal detail, there will be a fresh intrusion of privacy when each additional viewer sees the photograph and even when who has seen a previous publication of the photograph is confronted by a fresh publication of it.’\(^69\)

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199, [110], [132], [34], [39], [40], [55]. Citing the American Law Institute, Restatement of the Law of Torts (Second) (1977), 2d § 652A, Comment b. Gleeson CJ said that ‘equity may impose obligations of confidentiality even though there is no imparting of information in circumstances of trust and confidence. And the principle of good faith upon which equity acts to protect information imparted in confidence may also be invoked to “restrain the publication of confidential information improperly or surreptitiously obtained”. The nature of the information must be such that it is capable of being regarded as confidential. A photographic image, illegally or improperly or surreptitiously obtained, where what is depicted is private, may constitute confidential information’; see also Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Report 123 (2014) Breach of Confidence Actions for Misuse of Private Information, Recommendation 13-1, 265; Giller v Procopets (2008) 79 IPR 489; Grosse v Purvis [2003] QDC 151; Wilson v Ferguson [2015] WACA 15.
image. One reason for this is that there are still conceptual difficulties with an action for breach of confidence in Australia. This is because an image may be private but not be confidential.\(^70\) The exclusion of information that is about a person’s family or private life would leave a gap in the legal protection for personal images that are taken, uploaded and shared online. This is because the information would need to be ‘serious’. Another limitation is that once the information is published in the public domain, the action for breach of confidence would potentially fail.

Another important recommendation of the ALRC was that a remedy for emotional distress ought to be included as part of compensation for misuse of private information.\(^71\) This would overcome the fact that the law of confidence does not adequately provide damages for emotional distressed suffered by a person whose image has been misused – for example, when people are photographed in embarrassing settings and the images were uploaded and shared online. Although some state courts in Australia have awarded damages for emotional distress, the common law generally is uncertain about whether damages can be awarded for emotional distress when personal images are misused.\(^72\) If enacted such a provision would provide important redress for online misuse.

### 6.5 Conclusion

In examining whether the proposed reforms potentially fill in the gaps in the existing legal protection, it has been shown that a statutory tort for serious invasions of privacy would provide legal protection for two specific types of invasions of privacy: intrusions upon seclusion and misuse of private information. The proposed recommendations would have limited application to personal images shared on social networks. This is because the proposed reforms would not deal with the ubiquitous capturing and uploading personal image on social networks. As noted

---


earlier, the ALRC’s view on ‘serious’ invasions are likely to be limited to images that are of a sexual or intimate nature. Personal images captured in everyday situations would be vulnerable and unprotected. This is also the case if the image was captured in a private place, unless the image was of a sexual or intimate nature.\textsuperscript{73} Consequently, there is a gap in protection for personal images that are not considered to be ‘sensitive’.\textsuperscript{74} Even though many personal images that are captured and uploaded online are not sensitive, those images also need protection. This is because personal images that are embarrassing or humiliating may be captured in public or private spaces.

The taking and uploading of an image on to a social network may be an intrusion upon a person’s seclusion for two reasons; the first is that the information in the photograph may be private, the second is that the taking of a photograph is an invasion of a person’s physical privacy.\textsuperscript{75} There are a number of problems with the proposed statutory tort for serious invasions of privacy. The first is that it is uncertain whether many of the personal images that are captured and shared on a social network would be protected. The second problem is that the law has not caught up with a situation where images that are uploaded and shared online may be ‘private’ but still fall in the public domain. This occurs when personal images that are shared on social networks are shared online and go viral in seconds. When this happens, there is little that the law can do to prevent the misuse of personal images other than establishing a personal right to privacy (or images rights). Even if Australian law established a tort of invasion of privacy, this would not cover all the different instances where personal images are captured and shared online. It has been shown that Australian law does not protect people who are photographed in public places and people in Australia do not have a right not to be photographed. As people are photographed in various situations and in public or in private spaces; a statutory tort would be limited to situations where the image is sensitive or of a sexual nature. If the existing tort of breach of confidence were broadened to include a ‘misuse of private information’, the law of confidence would not provide adequate protection for personal images shared on social


\textsuperscript{74} Maynes v Casey [2011] NSWCA 156 (14 June 2011) [35]; see Saad v Chubb Security Australia Pty Ltd [2012] NSWSC 1183 [183]; Gee v Burger [2009] NSWSC 149 (13 March 2009) [53]; Dye v Commonwealth [2010] FCA 720 [290], where Katzmann J refused leave to the plaintiff to amend her pleadings to include such a claim, on various grounds, and Doe v Yahoo! 7 Pty Ltd [2013] QDC 181 (9 August 2013) [310]–[311].

\textsuperscript{75} See Nicole Moreham, above n 14, 354-6. See Adam Pabarcus, above n 19, in relation to a private social network page being a secluded place.
networks. This is because when applying the criteria for an action of breach of confidence to personal images that are shared on social networks, the images tend to fall within the public domain. This is very similar to the way the existing common law protects personal images.

Given that an Australian statutory tort is modelled on US privacy law, a more appropriate recommendation would have been to incorporate two further types of invasions to cover the use and misuse of people’s images. For example, the ALRC should have included serious invasions of ‘publicity which places the plaintiff in a false light in the public eye’ and an ‘appropriation for the defendant’s advantage, of a plaintiff’s name or likeness’. It would seem that these two types of serious invasions of privacy would be more appropriate to the misuse of personal images on social networks, such as when people’s images are distorted. In thinking about possible solutions to close the gap in legal protection for the misuse of personal images on social networks, a statutory tort ought to be broadened to incorporate a right to publicity or image rights to capture the various situations where personal images are used and misused. These are examined in Chapter 7.

---

76 See further William L Prosser, above n 10, 389.
Chapter 7
An Australian Right to Publicity?

This right might be called a ‘right of publicity’. For it is common knowledge that many prominent persons (especially actors and ball-players), far from having their feeling bruised through public exposure of their likeness, would feel sorely deprived if they no longer received money for authorising advertisements, popularising their countenances, displayed in newspapers, magazines, busses [sic], trains and subways. This right of publicity would usually yield them no money unless it could be made the subject of an exclusive grant which barred any other advertiser from using their pictures.

Judge Frank in Haelan Labs

7.1 Introduction

This chapter examines the potential role that a right to publicity might play in protecting personal images that are shared online in Australia. While a number of jurisdictions have a right to publicity that protects personal images, Australia does not currently have such a right. Taking the United States law as a potential role model, the chapter will consider whether an equivalent right of publicity, if adopted in Australia, would help to prevent the misuse of personal images that are shared online.

---

1 Haelan Labs Inc v Topps Chewing Inc 202 F 2d 866, 868 2d Circ, cert denied, 346 US 816 (1953).
Image rights have been protected under the law of torts in the United States since the 1890s. The tort of a right of privacy is currently broken down into four categories and includes a right to publicity. These categories are:

1. intrusion upon the plaintiff’s seclusion or solitude or 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, and
4. appropriation for the defendant’s advantage, of the plaintiff’s name or likeness.

This chapter focuses on the last of the four torts protected under the tort of privacy in the United States: the appropriation of a person’s likeness or name, which is often referred to as the right of publicity or publicity rights. The US right of publicity allows people to prevent the appropriation of the commercial use of their identity, likeness or name. In 1953, in *Haelan Labs, Inc v Topps Chewing Gum, Inc;* Judge Frank said:

in addition to and independent of that Right of Privacy … a man has a right in the publicity value of his photograph, i.e., the right to grant exclusive privilege of publishing his picture … Whether it be labeled a property right is immaterial; for here, as often elsewhere, the tag ‘property’ simply symbolizes the fact that courts enforce a claim which has pecuniary worth.

---


There are two notable things about the US right of publicity that should be noted at the outset. The first is that the right only applies to natural people; it does not apply to corporations and similar entities. The second is that while, in theory, the right applies to both celebrities and non-celebrities, as a result of case law in the 1950's the right is now effectively limited to celebrities. As Bass has said; ‘although technically the right of publicity protects everyone, courts have primarily focused on celebrities because celebrities have greater incentives to litigate claims for commercial exploitation of their identities than non-celebrities’. The following section examines the criteria required for a right of publicity. In examining the right of publicity, the chapter will argue that if Australia did adopt a right to publicity, it could potentially fill in some of the gaps that exist in Australian law, as highlighted earlier in the thesis.

7.2 What are Publicity Rights?

There are four elements that must be satisfied for a claim of a right of publicity. These are:

1. that the plaintiff’s identity has been used,
2. for the defendant’s advantage, commercial or otherwise,
3. without the plaintiff’s consent, and
4. there is a resulting injury.


To fully understand the scope and operation of the right of publicity the four elements that need to be satisfied are examined below.

7.2.1 The Use of the Plaintiff’s Identity

The first element that must be satisfied for the right of publicity to apply is that the plaintiff’s identity must have been used. It can be argued that when someone photographs a third party, the person who captures that image is making use of the person’s image. As a photograph of a person falls within the definition of personal information, and as a photograph identifies a person, the taking of a person’s photograph would constitute ‘use’ of the person’s identity. Sharing personal images of people online is also using a person’s identity because the photograph identifies the person on the social network.

7.2.2 The Use Must Constitute an Advantage, Commercial or Otherwise

The second element that must be satisfied is that the use of a person’s image constitutes an ‘advantage, commercial or otherwise’. While this element is construed broadly, American jurisprudence since the mid-1950s has demanded that the use of a person’s image must be for a commercial purpose such as endorsing a product or brand. In this context, the appropriation of a person’s name or likeness is linked to the commercial value of a person’s identity. Tan argues that there is a presumption ‘that a plaintiff’s identity has an economic value – especially for celebrities – when it has been used by a defendant in a commercial context’; indeed, it would be futile for an advertiser or a trader to appropriate an identity that had no market value since


13 See generally, Alain J Lapter, above n 12, 272; Daniel Nemet-Nejat, above n 6; Anna E Helling, above n 12, 14.


15 See Pavesich v New England Life Insurance Company 122 Ga 190, 50 SE 68 (1905); Roberson v Rochester Folding Box Co 171 New York 538 (1902).
such an appropriation would not be providing any discernible benefit’.16 The reason that a right of publicity has been construed in economic terms is that in the United States post-1900s, people initiated claims seeking ‘economic compensation for the use of an individual’s likeness’.17 The commercial focus of the right of publicity ignores the non-monetary considerations that arise when people’s images are used in a non-commercial context.18 This is particularly important when personal images are misused on a social network given that it is often difficult to attribute economic value to a person’s image when they are not a celebrity.19 While some states, such as California, recognise these limitations and allow non-celebrity plaintiffs to recover damages for mental anguish apart from economic harm, this is not widely used.20

7.2.3 The Use of the Image is Without a Person’s Consent

When people take photographs of third parties, there is no requirement that they must obtain the consent of the person being photographed. While there is no law in the United State against taking photographs of people, a person will need to obtain consent if the photograph is used or published for commercial purposes.


17 Alison C Storella, ‘It’s Selfie Evident: Spectrums of Alienability and Copyrighted Content on Social Media’ (2014) 94 Boston University Law Review 2045, 2069; Samantha Barbas, ‘From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption’ (2013) 61 Buffalo Law Review 1119, 1119–21, where the author states that between the early 1900s and the 1950s ‘several states formally reworked the tort (of appropriation) so that it no longer principally compensated dignitary and emotional injuries but rather economic harms’.


20 See CAL. CIV. CODE § 3344(a) (West 2012). California courts permit recovery for private persons under the California right of publicity statute.
Social networks encourage and facilitate the sharing of images of third parties in their terms of use. Often, because images are shared on personal social network pages, it is unlikely that the subject will be asked for their consent to the use of their image – especially if their image is captured in a public place. As was noted in Chapter 2, social network contracts commonly deal with the use of personal images. When a person joins a social network, it can be argued that they give their consent to the use of their images. Where this is the case, a person would not be able to rely on a right of publicity when a social network uses those images for commercial purposes. This issue was considered in *Fraley v Facebook*, where Facebook argued that people give consent to the network to use the profile images when they agree to the network’s terms of use. However, the court found that the terms of use at that time did not explicitly give the network consent to use its user’s names and likenesses to disclose the services or products that the users had liked or used. The court also found that some of the plaintiffs in *Fraley* had consented to the network’s terms of use before the network introduced the ‘Sponsored Stories’ feature. Judge Koh dismissed Facebook’s claim that the plaintiff’s consented to the use of their images because the plaintiffs were:

likely to be deceived into believing [they] had full control to prevent [their] appearances in Sponsored Story advertisements while otherwise engaging with Facebook’s various features, such as clicking on a ‘Like’ button, when in fact members lack such control.

This situation may be different as a result of subsequent changes in Facebook’s terms of use.

### 7.2.4 The Use of the Image Results in Injury

In order for a United States right of publicity claim to be successful, the use of the image must result in an injury to the person whose image has been used. While it is relatively easy for a celebrity to prove economic harm, it is often difficult for non-celebrities to prove economic harm in the use of a person’s image. Social networks have challenged the traditional stereotype

---

21 *Fraley v Facebook* 830 F Supp 2d 785 (ND Cal 2011).
22 Ibid.
23 Ibid 803, 804–6.
26 See generally Anna E Helling, above n 12.
of celebrity because ‘anyone can be a star’. This is because in today’s digital world, anyone with a social network profile is a public figure. Social networks allow ordinary people to attain a quasi-celebrity status because many people have many followers or friends which affirms their online popularity. The problem that arises for non-celebrities in a right of publicity claim is that while a misuse of a person’s image will often result in emotional distress, harm or damage to their reputation, it may not result in economic harm. For example, when a photograph of an intoxicated person is published on a social network it may result in that person being embarrassed and cause damage to their reputation if the image but not lead to any economic damage. The problem is that US law has been reluctant to recognise emotional harm as a cause of action. One reason for this is that there is a concern that recognising emotional harm for an unauthorised use of a person’s image might lead to ‘bad faith claims’. As a result, US courts have held that there will be no legal redress unless the harm was objectively measurable (such as an injury to reputation). However, the US courts have rejected this concern because ‘the law does not take cognizance of and will not afford compensation for sentimental injury’. As Judge Henry Bischoff said:

perhaps the feelings find as full protection as it is possible to give in moral law and responsive public opinion. The civil law is a practical business system,

---

29 Social networks like Twitter, Facebook and Instagram allow people to have connections and followers, with some going over 1,000 connections. In some cases, people can reach up to 100,000 followers.
30 Even if a non-celebrity is successful in a right of publicity claim, ‘damages due to lack of a commercial value to his celebrity harms [would] be wholly non-economic in nature, given the lack of any marketable value for image’ see KJ Greene, above n 9, 538; Alison C Storella, above n 17, 2072; Brian D Wassom, ‘Uncertainty Squared: The Right of Publicity and Social Media’ (2013) 63 Syracuse Law Review 227, 242–4, who states that in the ‘Restatement (Third) the general common law measurement of damages for right of publicity is the ‘the pecuniary loss to the other caused by the appropriation or for the actor’s own pecuniary gain resulting from the appropriation, whichever is greater’.
31 See Robertson v Rochester Folding Box Co 171 NY 544–6, 64 NE 443–4; Alisa M Weisman, above n 14, 739.
32 Ibid.
33 Murray v The Gast Lithographic and Engraving Co, 8 Misc 36 (NY Common Please 1894), quoting with approval Chapman v Western Union Tel Co; see also Robert E Mensel, above n 65, 32.
dealing with what is tangible and does not undertake to redress psychological injuries.34

This is in contrast to Warren and Brandeis’s view that ‘thoughts, emotions and sensations demanded legal recognition’.35 Where the misuse of a person’s image only results in embarrassment or humiliation, it is unlikely that a right of publicity will apply. As a result, even though the right of publicity applies to non-celebrities, it ‘acts as a “right without a remedy” for the non-famous’.36

7.3 Exceptions to the Right of Publicity

There are a number of exceptions to the US right of publicity. The following section examines the exceptions to the right of publicity in the context of personal images that are shared online.

7.3.1 Public Interest and Newsworthiness

One of the situations when the right of publicity may not protect personal images that are shared online is when the use of an image is in the public interest. The common law in the United States provides that ‘no cause of action will lie for the publication of matters in the public interest, which rests on the right of the public to know and the freedom of the press to tell it.’37 This might occur when the images are used for news reporting or journalistic purposes. Even though a person’s image is misused, if the use is for journalistic purposes, the misuse will not actionable under the right of publicity.38 This is because:

34 Murray v The Gast Lithographic and Engraving Co, 8 Misc 36 (NY Common Please 1894) quoting with approval Chapman v Western Union Tel Co; see also Robert E Mensel, above n 65, 32.
35 Samuel D Warren and Louis D Brandeis, above n 2.
36 KJ Greene, above n 9, 536–8, quoting Doe v County of Ctr Pa 242 F 3d 437, 456 (3rd Circ 2001); see also Alison C Storella, above n 31, 2072.

Koehler argues that the ‘right of publicity and the concept of newsworthiness require a balancing test that weighs the newsworthiness of the speech in question against the right of publicity of the person implicated as the subject matter of the speech.’\footnote{Jesse Koehler, above n 19, 975. The author further states at 974-5 that ‘because California’s right of publicity prevents a commercial speaker from inappropriately using an individual’s name or likeness and thus places a strain on what a speaker can say, the right of publicity can conflict with the First Amendment’s free speech and freedom of the press clauses’.} While it appears that newspapers have a complete defence against the right of publicity when using personal images,\footnote{W Mack Webner and Leigh Ann Lindquist, above n 39, 192; \textit{New Kids on the Block v News America Publishing} 971 F 2d 302 (9th Circuit 1992) 309, where the court said that ‘the papers have a complete defence to both claims [common law misappropriation and commercial misappropriation] if they used the New Kids name “in connection with any news, public affairs or sports broadcast or account” which was true in all material respects’.} there are some limitations on using personal images for news-reporting purposes. The first limitation is that even if an image is used for journalistic purposes, it cannot be used for commercial or advertising purposes without the subject’s consent.\footnote{WAC, above n 38, 1315; see also \textit{Bimms v Vitagraph Co Of America}, 210 NY 51 103, NE 1108 (1913); \textit{Kunz v Allen} 102 Kan 883, 172 Pac 352 (1918); W Mack Webner and Leigh Ann Lindquist, above n 39, 188.} The second is that people who are not celebrities are usually unable to satisfy the elements discussed above because non-celebrity images are usually not commercial. As a result, when images of ordinary people are shared on social networks, the right of publicity will not prevent any misuse of the image. However, it may possible for the right of publicity to protect a person’s image where that image is used in connection with advertising or marketing.

It seems that when the press uses a personal image, the person whose image is used will be challenged to have a successful claim for infringement of a right of publicity.\footnote{W Mack Webner and Leigh Ann Lindquist, above n 39, 193.} This is because newsworthiness ‘is interpreted sufficiently loosely and broadly so that almost any
activity associated with a press activity will be held to be under that umbrella’. Consequently, it is unlikely that a right of publicity will protect personal images when journalists and news reporters use personal images that are shared on social networks. As result, even if a person’s image is shared on a social network and the image is taken from the network to report news, there is no law to prevent the use of that image. This leaves a gap in the protection available under the right of publicity.

One issue that is unclear - which arises because of the way the internet is changing what we consider to be ‘news’: is whether an online posting made by a non-journalist could be newsworthy. Users of social media may consider anything that a friend posts online to be ‘newsworthy’. Judge Koh noted that because users were local ‘celebrities’ in their personal social network, their posting were considered to be newsworthy. If this approach was followed it would mean that anything that a user posts on a social network may be considered to be newsworthy to the people they are connected to.

7.3.2 Freedom of Expression

Another important exception to the right of publicity is when personal images are artistic works which are protectable under freedom of expression. In the United States, freedom of expression is protected under the First Amendment. Without doubt, the balance between protecting a person’s image and freedom of expression is a fragile endeavour. As Bass states, ‘there is an inherent tension between the right of publicity and the right of freedom of expression’. However, it seems as though a right of privacy is cast aside whenever it is considered alongside

44 Ibid.
45 This occurs, for example, when people are accused and journalists show the person’s image while telling the news. For example, when a lewd image of Todd Carney was captured in a nightclub restroom by another patron and later uploaded on Twitter, journalistic used the image: Harry Tucker and Debra Killalea, ‘What on Earth was Todd Carney Thinking When Shocking Lewd Photo was Taken’, Daily Telegraph (29 June 2014) <http://www.dailytelegraph.com.au/sport/nrl/teams/sharks/what-on-earth-was-todd-carney-thinking-when-shocking-lewd-photo-was-taken/news-story/3f6d0fa012593a98edaf4066be8b38aa>. See Jenni Ryal, ‘How a Darth Vader Selfie Showed the Ugly Side of Social Media’, Mashable (11 May 2015) <http://mashable.com/2015/05/11/darth-vader-selfie/#jc888fmbC8kqC>.
46 Fraley v Facebook 830 F Supp 2d 785 (ND Cal 2011), 805, Judge Koh (citing Downing v. Abercrombie & Fitch, 265 F.3d 994, 1002 (9th Cir. 2001) said that users were identified as ‘subjects of public interest among the same audience’; see Jesse Koehler, above n 19, 964.
freedom of expression. When people’s images are captured in a photograph, there may be competing interests. For example, John takes a photograph of Jane sitting on a park bench. John, as the creator of the photograph, owns the copyright in the photograph; this means that John controls the photograph and the use of the photograph. Jane, however, is the subject of the image and has no control over the use of the image that has been captured by John. In this situation, if John uploads the image of Jane onto a social network page, Jane will not be able to prevent the misuse of her image. This is because John has the freedom of expression to take photographs, and even if those photographs capture third parties, a right of publicity does not prevent a person from being photographed. In America, freedom of expression has become paramount to any privacy right, especially when the photograph is artistic or newsworthy. 48

A useful example of the way which the right of freedom of expression has been given precedent over privacy concerns can be seen in the decision Foster v Svenson,49 when a photographer (Svenson) had taken photographs of his neighbours in their home while in his own home using a high-powered lens.50 Svenson captured several different photographs of his neighbours (the Fosters) and their children sleeping, playing and undressing. The neighbours were not aware that Svenson was taking photographs until the photographs were displayed in an art gallery. Nor had the plaintiffs consented to the photographs being taken. At the first instance, the Fosters were unsuccessful in their claim because the photographer’s right to

48 See Alison C Storella, above n 17, 2050–1; Burrow-Giles Lithographic Co v Sarony 111 US 53 (1884); Bleistein v Donaldson Lithographing Co 188 US 239 (1903).

49 Foster v Svenson 2013 NY Slip Op 31782 NY Supreme Court 2013; Foster v Svenson 7 NYS 3d 96 (NY App Div 2015).

50 Foster v Svenson 7 NYS 3d 96 (NY App Div 2015) 128 AD 3d, 152. Renwick J stated: ‘New technologies can track thought, movement, and intimacies, and expose them to the general public, often in an instant. This public apprehension over new technologies invading one’s privacy became a reality for the plaintiffs and their neighbors when a photographer, using a high powered camera lens inside his own apartment, took photographs through the window into the interior of apartments in a neighboring building. The people who were being photographed had no idea this was happening. This case highlights the limitations of New York’s statutory privacy tort as a means of redressing harm that may be caused by this type of technological home invasion and exposure of private life. We are constrained to find that the invasion of privacy of one’s home that took place here is not actionable as a statutory tort of invasion of privacy pursuant to sections 50 and 51 of the Civil Rights Law, because defendant’s use of the images in question constituted art work and, thus is not deemed ‘use for advertising or trade purposes, ‘within the meaning of the statute.’
freedom of expression was thought to be more important than the privacy interests of the Fosters. As Rakower J said:

While it makes Plaintiffs cringe to think their private lives and images of their small children can find their way into the public forum of an art exhibition, there is no redress under the current laws of the State of New York. Simply, an individual’s right to privacy under the New York Civil Rights Law sections 50 and 51 yield to an artist’s protections under the First Amendment under the circumstances presented here.

On appeal the plaintiffs argued that a right of publicity ought to protect the use of their images because the images were exhibited in an art exhibition and some of the artworks had been sold. However, on appeal the court held that the plaintiffs:

do not sufficiently allege that defendant used the photographs in question for the purpose of advertising or for the purpose of trade within the meaning of the privacy statute. Defendant’s use of the photos falls within the ambit of constitutionally protected conduct in the form of a work of art. While a plaintiff may be able to raise questions as to whether a particular item should be considered a work of art, no such question is presented here. Indeed, plaintiffs concede on appeal that defendant, a renowned fine arts photographer, assembled the photographs into an exhibit that was shown in a public forum, an art gallery. Since the images themselves constitute the work of art, and artwork is protected by the First Amendment, any advertising undertaken in connection with the promotion of the artwork was permitted. Thus, under any reasonable view of the allegations, it cannot be inferred that plaintiffs’ images were used ‘for the purpose of advertising’ or ‘for the purpose of trade’ within the meaning of the privacy statute.

The court noted that there were gaps in the way that the right of publicity protected personal images in the United States. In particular, Renwick J noted that in order for a right of publicity to apply

51 Ibid
52 Ibid
53 Ibid (Rakower).
54 Ibid 160 (Renwick J).
(with respect to a right of privacy), a claim would need to overcome the First Amendment. The demand to strike a balance between a person’s right to privacy and freedom of expression has eroded the privacy rights for which Warren and Brandeis originally argued. As Renwick J said:

acknowledging that Civil Rights Law §§ 50 and 51 reflect a careful balance of a person's right to privacy against the public's right to a free flow of ideas, plaintiffs argue that defendant’s work should not be entitled to First Amendment protection because of the manner or context in which it was formed or made. In essence, plaintiffs seem to be arguing that the manner in which the photographs were obtained constitutes the extreme and outrageous conduct contemplated by the tort of intentional infliction of emotional distress and serves to overcome the First Amendment protection contemplated by Civil Rights Law §§ 50 and 51.55

The court also noted that freedom of expression:

will not lose entitlement to the newsworthy and public concerns exemption of Civil Rights Law §§ 50 and 51 unless the means by which a person’s privacy was invaded was truly outrageous. Indeed, while one can argue that defendant’s actions were more offensive than those of the defendant in Howell, because the intrusion here was into plaintiffs’ home, clearly an even more private space, they certainly do not rise to the level of ‘atrocious, indecent and utterly despicable’.56

It is unclear what circumstances or situations would give rise to ‘atrocious, indecent and utterly despicable’ behaviour, because even when the conduct is offensive, the balance between expression and a right of publicity tips in favour of expression. This highlights the inadequate protection afforded by the right of publicity because taking photographs of people while in their homes will not constitute conduct that is so outrageous that it oversteps the protected boundaries of freedom of speech or expression.57 It seems that a right of publicity will have a limited

56 Foster v Svenson 7 NYS 3d 96 (NY App Div 2015) 128 AD3d, 163. Renwick J said: ‘Further, the depiction of children, by itself, does not create special circumstances which should make a privacy claim more readily available. We note that defendant’s conduct here, while clearly invasive, does not implicate the type of criminal conduct covered by Penal Law § 250.40 et seq., prohibiting unlawful surveillance.’
57 In Foster v Svenson 7 NYS 3d 96 (NY App Div 2015) 128 AD3d (Renwick J) stated: ‘In short, by publishing plaintiffs’ photos as a work of art without further action toward plaintiffs, defendant’s conduct, however disturbing it may be, cannot properly, under the current state of the law, be deemed so
application to personal images, regardless of whether they are captured in public or private places when those images are taken and used as artistic works as in the case of Foster v Svenson. This is because a photograph is protected as an artistic work and, despite the manner in which the photograph is taken, will supersede any claims of privacy under a right of publicity.

The New York Court of Appeal recognised that US law did not address situations where people are photographed in the privacy of their own homes because:

Undoubtedly, like plaintiffs, many people would be rightfully offended by the intrusive manner in which the photographs were taken in this case. However, such complaints are best addressed to the legislature – the body empowered to remedy such inequities … Needless to say, as illustrated by the troubling facts here, in these times of heightened threats to privacy posed by new and ever more invasive technologies, we call upon the legislature to revisit this important issue, as we are constrained to apply the law as it exists.

It is clear that the demand to strike a balance between a person’s right to privacy and freedom of expression has resulted in an erosion of the privacy rights that Warren and Brandeis originally argued for. As a result, it has undermined the effectiveness of the action. One question here, however, is whether the absence of an equivalent to a First Amendment right in Australia would mean that a publicity right in Australia would be more effective in protecting against online misuse of images?

7.4 Problems with a Right of Publicity?

It is clear that a right of publicity morphed from originally protecting a right of privacy, as envisaged in Warren and Brandeis’s right to privacy to a right to protect commercial use of a person’s image. Warren and Brandeis, who were concerned with the impact that pervasive technologies such as instantaneous photography had on people, had the foresight to predict that such technology would be intrusive to a person’s privacy; hence they saw the need to exercise a right of privacy that was not founded in the law of confidence.

“outrageous” that it went beyond decency and the protections of Civil Rights Law §§ 50 and 51. To be sure, by our holding here – finding no viable cause of action for violation of the statutory right to privacy under these facts – we do not, in any way, mean to give short shrift to plaintiffs’ concerns.

7 NYS 3d 96 (NY App Div 2015).

Foster v Svenson 7 NYS 3d 96 (NY App Div 2015) 128 AD3d (Renwick J).
As highlighted previously, there are situations where a right of publicity will protect personal images against unauthorised use. However, this is limited – for example, a right of publicity will only apply in circumstances where the image is used for commercial or advertising purposes, or in the case of celebrities where it causes economic damage. While a right of publicity provides protection for a person to ‘control the commercial use of his or her identity’, there are a number of problems that arise when images of non-celebrities are uploaded and shared on social networks. The first problem with a right of publicity is that it does not prevent a person from being photographed. The second is that a right of publicity collides with copyright over photographs that are artistic works. The third is that a right of publicity may not extend to deceased people. The fourth is that when personal images are shared online, social networks will regulate the use of those images through the network’s contract agreement. The following sub-section examines these problems.

7.4.1 No Law Against Being Photographed

The first problem with a US style right to publicity is that it does not prevent a person from being photographed. This is particularly the case when people are photographed in public streets. As a New York court stated, even ‘private social affairs and prevailing fashions involving individuals who make no bid for publicity are custom, regarded as public property,


61 When people share personal images online, third parties may misuse those images. A right to publicity would provide some protection against the misuse of the image. For example, in Angel Fraley et al v Facebook Inc CA No 511-01726, the court allowed a motion where users alleged that their names and likeness were misused by Facebook’s ‘Sponsored Stories’ feature. While the case settled, the action highlights that when ordinary people’s images are misused, a right to publicity/appropriation will not result in adequate compensation. In this case, the plaintiffs were awarded $10 for the misappropriation of their image. Even though Facebook receives advertising revenue from the sponsored stories, the use of ordinary people’s images makes it difficult to determine adequate compensation.
where the apparent use is to convey information of interests and not mere advertising’. As Horridge J said in *Sports and General Press Agency Ltd v ‘Our Dogs’ Publishing Company*,

In my judgment no one possesses a right of preventing another person photographing him any more than he has a right of preventing another person giving a description of him, provided the description is not libellous or otherwise wrongful. Those rights do not exist.

Where there is no commercial use of an image, a right of publicity will not protect a person who is photographed in public where the resulting photograph is published online.

7.4.3 *A Right of Publicity May Not Extend to Dead People*

Another situation where the United States’ right of publicity may not protect personal images is when a deceased person’s image is shared online. This was highlighted in *Catsouras v*

---

62 *Martin v New Metropolitan Fiction Inc* 139 Msc 290 292 248 NYS 359, 362  Supreme Court, Renseselaer Country 1931. WJ Wagner, ‘Photography and the Right to Privacy: The French and American Approaches’ (1980) 25 Catholic Lawyer 195, 208. The author suggests that ‘protection against the taking of photographs seemed to be practically impossible, and that anyone may take another’s picture on any occasion that presents itself. Protection would be given solely against the use made of the photographs. The use of another’s photograph is permitted, according to the cases as long as it is not connected with commerce, trade or business.’

63 [1916] 2 KB 880.

64 *Sports and General Press Agency Ltd v ‘Our Dogs’ Publishing Company* [1916] 2 KB 880 at 884.

65 See WAC, above n 42,1309; *Gill v Hearst Publishing Co*, 40 Cal 2 D 224, 253 P2d 441 (1953).

Department of California Highway Patrol\textsuperscript{67} where the appellate court held that while ‘family members have a common law privacy right in the death images of a decedent subject’ that this was equal to certain limitations.\textsuperscript{68} Even though the case settled before going to trial, the California appellate court noted that the ‘parties cite no California or Ninth Circuit Court of Appeals case addressing whether a complaint alleging a violation of a family member’s privacy right to photographs of a decedent is sufficient to state a cause of action’.\textsuperscript{69} As a result it has been suggested that:

while most of the case law involves the government and its access to autopsy and crime scene photographs, neither statutes nor common law define the proper remedies for families who wish to bring a relational right of privacy claim against a private individual. As technology continues to expand, so too are the legal issues.\textsuperscript{70}

Even if the right of publicity extended to deceased people, it would still face the same challenges that are present when applying a right of publicity to living people – that is, those images would have to be balanced with the existing exceptions of freedom of speech and newsworthiness that are contained in the First Amendment.\textsuperscript{71}

\subsection{7.4.4 Publicity Rights May be Lost When Entering into a Social Network Contract}

Another reason why the right of publicity may not protect personal images shared on social networks is because people may contractually license their rights away. As shown in Chapter 2, when people join a social network they give the social network site very wide licences to use their content. The wide licences allow the networks to use, reuse and sub-license people’s photographs. Once an author subscribes to a social network service, they license their images in all of their content over to the social network. In so doing they lose the ability to use the right of publicity to protect themselves against misuse online (at least by the social network site).

\begin{itemize}
\item \textsuperscript{67}104 Cal, Rptr 3d 352 (Cal Ct App 2010); Marsh \textit{v} County of San Diego, 680 F3d 1148, 1153 (9th Circ 2012), 1159. Kozinski J stated that ‘although in Catsouras the court found a state privacy right over death images, it found no clearly established federal right’.
\item \textsuperscript{68}Catsouras \textit{v} Department of California Highway Patrol, 104 Cal, Rptr 3d 359.
\item \textsuperscript{69}Ibid 389.
\item \textsuperscript{70}Catherine Leibowitz, ‘A Right to be Sparred Unhappiness’ (2013) 32 Cardozo Arts and Entertainment Law Journal 347, 349; Clay Calvert, above n 66, 504–5.
\item \textsuperscript{71}Clay Calvert, above n 66, 517.
\end{itemize}
7.5 Conclusion

There is no doubt that if introduced into Australia a US style right of publicity would provide some protection for personal images. There are a number of limitations with the action however that would limit its usefulness. These include the fact that the right of publicity has been construed narrowly. The second is that freedom of expression has become paramount to protecting privacy in the use of personal images. The third is that a right of publicity does not extend to deceased people. The fourth limitation is that a right of publicity may not protect personal images that are regulated by social network contracts.

Despite these limitations, if Australia did adopt a right of publicity, it would close some of the gaps in the legal protection for personal images shared online. To provide effective protection, an Australian right of publicity would need to be broader in scope than the US law. For example, there should be no requirement that the use of the image should be for commercial purposes; nor should it be targeted only at celebrities. An Australian version of a right of publicity should apply where people are photographed in public and private spaces. According to the law in the United States, a person who takes a photograph of another person should obtain consent if they want to use the image commercially. The same should apply in Australia, with the added condition that the person has consented to their image being shared online.
Chapter 8
The right to be forgotten in Australia

8.1 Introduction

Social networks facilitate communication and interaction online. When people communicate and interact online, their private lives often become public. Social networks such as Facebook, Instagram and Twitter have sparked new trends in the way people exchange and communicate information, particularly personal images; they actively encourage people to share their lives with their friends, family and social connections within the digital environment.¹ All too frequently, people’s images are captured in photographs and shared on social networks without the person knowing that their images have been taken and shared online. In the process of sharing images on social networks, people often relinquish control over the use of their images, which allows the images to be exploited by third parties and social networks.² The use of digital and communication

¹ Recent notable example include the infamous photograph of a naked Prince Harry partying in Las Vegas; see ‘Prince Harry Naked Photos During Vegas Rager’, TMZ (22 August 2012), http://www.tmz.com/2012/08/21/prince-harry-naked-photos-nude-vegas-hotel-party. The problems with this is captured in Katy Perry’s tweet against Australian Media where she said: ‘Australian PRESS: you should be ashamed of your paparazzi & tabloid culture. Your paparazzi have no respect, no integrity, no character. NO HUMANITY.’ Perry also wrote: ‘I was stalked by many grown men today as I tried to take a quiet walk to the beach. These men would not stop as I pleaded over & over to let me have my space. Many other people stopped to try to help but the paps continued to laugh at me & hold their barrels up and shoot.’ And further: ‘This is PERVERTED & disgusting behaviour that should NEVER be tolerated, especially by people who do NOT want this.’ See Katy Perry, Twitter (21 November 2014), https://twitter.com/katyperry/status/535985788983721984/photo/1.

technologies creates a need to protect personal images and the information captured in those images from misuse.³

This chapter examines whether the European Union (EU)’s ‘right to be forgotten’ provides a possible solution to the problem of personal images being misused on social networks in Australia. Specifically, it considers whether the EU’s right to be forgotten is a model that could be adopted in Australia as a mechanism to protect against the misuse of people’s images within social networks.

The right to be forgotten has its origins in a growing concern about the impact of digital technologies in general on personal privacy. As Vivian Reding observed, ‘if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system’.⁴ The early 1990s saw the increasing use of digital technologies which created a need to protect people from potential abuse.⁵ As communication technologies sparked new trends in the way people exchanged and communicated personal information, the EU recognised that new data-protection laws were necessary to protect individual privacy and private life.⁶ To this end, European regulators developed the Data Directive⁷ in 1995 to protect an individual’s personal data and the processing of such data. European data-protection laws were enacted at a time when technology was less advanced and the exchange of personal information was significantly

---


⁵ See Bert-Jaap Kloops, above n 3, 230; Vivian Reding, above n 3.


lower than it is at present. Notably, in 1995 the use of social networks was not as prevalent as it is today.

One of the challenges that arises with most new forms of technology is that the technology often evolves faster than the law. The position with social networks is no different. As Giurgiu argues ‘the main problem relies in the fact that the rapidly, changing societal model has not allowed for legal norms to catch up’. Concerned about the threat to individual privacy created by the widespread use of data storage and data mining, European regulators recognised that the rights to privacy and data protection in the Data Directive have become outdated.

The problems with the law under the 1995 Data Directive were highlighted in the landmark 2014 Court of Justice decision of Google Spain v Gonzalez. The case arose when Mr. Gonzalez lodged a complaint against La Vanguardia Ediciones SL (a daily Spanish newspaper with a wide circulation), Google Spain and Google Inc. The basis of the complaint was that whenever an internet user searched for Mr. Gonzalez’s name using the Google search engine, the results would link to two pages from the La Vanguardia newspaper, which mentioned Mr. Gonzalez’s name in connection with proceedings for social security debts. Mr. Gonzalez requested two things. The first was that the newspaper remove or alter the pages so that ‘the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data’. The second request that Mr. Gonzalez made was that Google Spain and Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results. This was because the proceedings that were mentioned in the newspaper links had been resolved for a number of years and any references to that information were no longer relevant.

---

8 A Giurgiu, above n 2, 362-4.
9 A. Giurgiu above n 2, 362-5; Bert-Jaap Kloops, above n 3; Jef Ausloos, above n 2, 148.
10 [2014] EUECJ C-131/12.
12 Ibid.
13 Ibid 15.
14 Ibid.
15 Ibid.
The court ordered Google Spain to remove González’s personal data\textsuperscript{16} from the internet.\textsuperscript{17} The court held that data controllers should remove data where the data was ‘inadequate, irrelevant or no longer relevant, or excessive in relation to [the] purposes [for which they were originally collected or processed] and in the light of the time that has elapsed’.\textsuperscript{18} The Court of Justice issued a ruling that enabled people to request the removal of their data published by operators of search engines. The Google Spain v Gonzalez\textsuperscript{19} decision not only highlighted some of the inadequacies with the 1995 Data Directive, it also provided a possible solution. After some debate, to strengthen individual rights, in 2015 the European Parliament passed the General Data Protection Regulation\textsuperscript{20}, which amended the Data Directive. One of the key aspects of the revised law is the right to be forgotten.\textsuperscript{21} The General Data Protection, which was approved by the European Parliament on 17 December 2015,\textsuperscript{22} will repeal the Data Directive when it takes effect in 2018. In April 2016, both the European Council and the European Parliament adopted the General Data Protection Regulation.\textsuperscript{23} This means

\begin{itemize}
  \item \textsuperscript{16} European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ [1995] L281/31, Art 2(a), which defines data broadly as “‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.’
  \item \textsuperscript{17} The ruling is based on the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data, OJ [1995] L281/31.
  \item \textsuperscript{18} Google Spain v Gonzalez Case [2014] EUECJ C-131/12.
  \item \textsuperscript{19} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ [2016] L119/1, Art 4 (1). Hereinafter referred to as ‘General Data Protection Regulation’.
  \item \textsuperscript{20} The proposed amendments to the Data Directive included the rights of users to request that their personal data ‘no longer processed and deleted when they are no longer needed for a legitimate purposes’. General Data Protection Regulation, Art 17.
  \item \textsuperscript{22} The General Data Protection Regulation was approved by the European Parliament on 15 December 2015, however it was approved on 8 April by the Council and European Parliament approved the
that until the General Data Protection Regulation takes effect in 2018, the Data Directive is still effective. When it takes effect, there will be significant changes for social network sites that collect, process and store personal data.

The 2016 General Data Protection Regulation provides that where a data controller has made data public, they must take ‘all reasonable steps, including technical measures in relation to data for the publication of which the controller is responsible, to inform third parties which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data’.24 The General Data Protection Regulation provides that a data subject shall have ‘the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data especially in relation to personal data which are made available by the subject data while he or she was a child’.25 Article 17 also gives data subjects the right to be forgotten and to erase data relating to them.26 Specifically, Article 17 provides that users have the right to have information deleted in four situations. This is where:

Regulation on 14 April 2016. On 4 May 2016, the official texts were published in the EU Official Journal and will take formal adoption from 28 May 2018; see European Commission, Justice, Data Protection, Reform, Reform of EU Data protection rules <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>

24 General Data Protection Regulation, Art 17(2).
25 Ibid.
When applying the right to be forgotten to personal images shared online, there are a number of criteria that must be satisfied. Broadly, these are that:

1. the requirements for protection are met;
2. the use of the images falls within the scope of the right; and
3. the use of the images falls outside of the exceptions to the right to be forgotten.

The following section examines these elements in more detail.

### 8.2 Requirements for Protection

There are a number of criteria that must be satisfied in order for the right to be forgotten to apply. The first is that the images must fall within the meaning of ‘data’ as provided in the General Data Protection Regulation. The second is that the person must be a ‘data subject’. The third factor that needs to be satisfied for the right to apply is that the images must be controlled by a third party who is a ‘data controller’. The following sub-sections examine each in turn.

#### 8.2.1 Data

In Europe, the term ‘data’ is defined broadly to include any information that relates to a ‘data subject’. Any information that relates to a person or identifies a person in an online context may be considered to be ‘personal data’ within the meaning of the General Data Protection Regulation. This includes any data that can be used to identify an individual, such as their name, address, or email address.

---

27 *General Data Protection Regulation* Art 17; A Giurgiu, above n 2, 366; Dominic McGoldbrick, above n 26, 763; Alessandro Manterlero, above n 2, 233.

28 ‘Data’ is defined broadly in the *Data Protection Directive 95/46/ EC* The *Data Protection Directive* Art 2(a): “‘personal data’ shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”
environment will be considered ‘personal data’.\(^{29}\) Photographs depicting people’s images are a way of identifying individuals and thus satisfy the definition of data in the *Data Directive*.\(^{30}\)

People who join social networks and engage in the digital world exchange and share various types of information. This information forms the data that is processed, collected and stored in websites’ information systems. As social networks allow people to share images with multiple users simultaneously, this creates a number of issues for the control of the images when third parties reshare personal images. Sharing another person’s image on a social network by posting photographs of them online may be considered processing and collecting data under European law. Given that people not only share and exchange their own images but also third-party images on social networks, the images that are shared form the ‘data’ of the subject whose image is being used/shared.

### 8.2.2 Data Subject

The second criterion that needs to be satisfied for the right to apply is that the person must be a ‘data subject’. European data protection laws apply to data subjects who live in Europe. People who live in countries that are part of the European Union are entitled to rely on a right to be forgotten when their data is processed, collected or transferred to countries outside of the European Union.\(^{31}\)

According to Article 4(1) of the *General Data Regulation*, a data subject is a ‘natural person’,\(^ {32}\) construed broadly as a person who can be ‘identified directly or indirectly, in particular reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.\(^{33}\) People who are users of social networks and social media will fall within the definition of a ‘data subject’, and therefore any photographs that contain a person’s image would also fall within the definition of ‘personal data’, as discussed above.

---


\(^{31}\) In *Schrems v Data Protection Commissioner* Case C- 362/14, Schrems objected to the transfer of his personal data from Facebook Ireland to servers in the United States.


\(^{33}\) Ibid.
8.2.3 **Data Controller**

The third factor that needs to be satisfied for the right to apply is that the images must be controlled by a third party who is a ‘data controller’. A ‘data controller’ is defined as ‘a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law’.  

*Google Spain v Gonzalez* confirms that search engines are data controllers and as such are liable under the General Data Proposal Regulation. Given that social networks determine the purpose and means of processing personal data it is also clear social networks will fall within the definition of data controllers. For example, Facebook is a data controller because the network processes, stores, transfers and collects people’s personal data.

Given the scope of Web 2.0 and the participative culture that it created, individuals who share other people’s images may also be treated as data controllers. This is because an individual may collect and process another person’s data when they take a photograph or upload an image of another person online. Consequently, it is arguable that people who take photographs of third parties and upload and exchange the images on social networks would facilitate the ‘processing’ of personal data and as such arguably fall within the definition of ‘data controller’.

### 8.3 Use is Within the scope of the Right to be Forgotten

The right to be forgotten provides that the ‘fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data’ should be
The right to be forgotten strengthens the rights of data subjects when their data is used or misused. It does this by giving them the right to control the use of their image when the image is shared by third parties. The right to be forgotten allows people to request the removal of their image from data controllers that includes social networks sites and search engines.

The right to be forgotten operates in a number of different situations. The first is where the data is no longer relevant or if it is outdated (as in Google Spain v Gonzalez). The second is when a person withdraws the consent on which the processing of the data is based. Under the General Data Protection Regulation, the withdrawal must be unambiguous. When people sign up to a social network, they agree to the social network’s terms of use. By agreeing to the terms, they are providing their consent to the network to use collect, process and store their images. By entering into a social network contract, people give their consent to the network to capture their photographs legitimately. However, people often do not understand what the consent entails. Once a person gives their consent, their photographs (and personal image) and the ways in which their images may be used are beyond their control. This is because the network contracts allow personal images to be passed to third-party affiliates to be used for advertising and marketing purposes.

Under the General Data Protection Regulation, users may withdraw their consent allowing social networks to process, store and collect their data. This has ramifications for when a person terminates their social network account. As shown earlier, when a person terminates their social network contract, the network is still able to use a person’s images that have been shared on the network. In this case, when a social network continues to use people’s images after the contract ends, the network may be in breach of the General Data Protection Regulation.

---


40 General Data Protection Regulation Art 7, provides that a person can withdraw their consent.

41 Paul A Bernal, above n 2; see generally Jef Ausloos, above n 2, 146; Muge Fazlioglu, above n 2, 4-5, Alessandro Mantelelo, above n 2, 230.

42 Particularly significant are Facebook’s Terms of Use. In relation to the right to be forgotten, any requests from its users to erase the data would have to be erased from all of their data-storage systems, not just the Facebook platform. This contravenes Facebook’s new terms of use, which also state that the network can access archived copies of users’ shared data despite the user deleting or deactivate their account.
Regulation. When this occurs, a person would be able to use the right to be forgotten to request that the network remove their images from the network.

The third situation where the right to be forgotten might apply is when a person objects to the processing of their data. This might occur, for example, when a person takes a photograph of a third party who does not want their image to be shared online. The General Data Protection Regulation defines ‘processing’ broadly as:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

When a person takes their own photograph or a photograph of a third party, they are potentially ‘processing’ data in so far as they are collecting and recording the image. Similarly, the uploading of an image on a social network page may fall within ‘use, disclosure, dissemination or otherwise making available’.

A fourth situation where the right to be forgotten may apply is where a data subject’s information is transferred for processing to a country outside of Europe which does not protect data to the standard required by European law. Specifically, the right to be forgotten allows data subjects to object if their data has been transferred to third countries where those countries do not safeguard or protect the fundamental rights and freedoms that are guaranteed within the European Union. This is a result of Schrems v Data Protection Commissioner, where the Court of Justice held that the existing safe harbour provisions which provided that a data

---

43 An objection to the processing of a data subject’s data may be aimed at a data controller such as a search engine, Google, or a social network site like Facebook.

44 Emphasis added. General Data Protection Regulation, Art 4(2).

45 General Data Protection Regulation, Art 4(2).

46 Schrems v Data Protection Commissioner Case C-362/14, EU:C:2015:650, 78. The Court of Justice stated that ‘as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country “ensures” an adequate level of protection by reason of its domestic law or its international commitments’. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed ‘for the protection of the private lives and basic freedoms and rights of individuals’.

47 Ibid 90-91, citing judgment in Digital Rights Ireland and Others C 293/12 and C 594/12, paras 54–5.
subject’s data may be transferred to a third country were invalid.48 The Court of Justice held that a data subject may object to the transfer or processing of their data to a third country if it can be shown that the third country does not protect personal data in accordance with European law.49 As the Court of Justice said:

the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security.50

The Court of Justice also noted that when transferring a data subject’s data to a third country, the data subject would need to have ‘administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased’.51 Consequently, the right to be forgotten allows data subjects to object if their data have been transferred to third countries where those countries do not safeguard or protect the fundamental rights and freedoms that are guaranteed within the European Union.52

### 8.4 Exceptions to the Right to be Forgotten

There are a number of exceptions to the right to be forgotten in the General Data Proposal Regulation. One of the most important exceptions is in Article 80 of the General Data Regulation which provides an exception for journalists and artists for the processing of personal

---

48 Schrems v Data Protection Commissioner Case C-362/14, EU:C:2015:650. In a press release outlining the decision, the Court of Justice noted that the Irish High Court had to examine Schrem’s claims with ‘all due complaint with all due diligence and, at the conclusion of its investigation, is to decide whether, pursuant to the directive, transfer of the data of Facebook’s European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data;’ see Court of Justice of the European Union, Press Release No 1117/15 (6 October 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

49 Schrems v Data Protection Commissioner Case C-362/14, EU:C:2015:650.

50 Ibid 90.

51 Ibid, emphasis added.

52 Ibid 91, citing judgment in Digital Rights Ireland and Others C 293/12 and C 594/12, paras 54–5.
This requires that a data subject’s request to remove data must be balanced against freedom of speech or expression as well as the public’s interest in having access to the information. The balancing of freedom of expression and the right to be forgotten is critical when people share and exchange personal images on social networks. The **General Data Protection Regulation** recognises that when people upload and share images within a social network, there are competing interests between users who upload and share images, the people who access the image, and the subjects of those images. When deciding how the balance between these interests is to be drawn, a variety of factors are taken into account. These include ‘the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.’ In the case of public figures, the courts seem willing to give more weight to the public’s right to know than their ability to keep matters private. This is because ‘the interference with [a famous person’s] fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.’

One of the important consequences of the right to be forgotten is that it enables people to regain control over their data. It appears that if people did regain control, this would be detrimental to a person’s freedom of expression or speech. While these are valid concerns, they often disregard the key issue redressed by the right to be forgotten, which is that there are vast numbers of personal images collected and stored on the internet by large internet firms such as Google, Facebook and Microsoft that rely on people sharing their images online.

---

53 **General Data Protection Regulation**, Art 80. Compare with the exception of freedom of expression was previously contained in Article 9 in Data Directive 95/46/EC. Article 9 is an exemption that relates to the ‘processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression’ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data, OJ [1995] L281/31, Art 9. See generally Anne Flanagan, ‘Defining “Journalism” in the Age of Evolving Social Media: A Questionable EU Legal Test’ (2012) 21(1) *International Journal of Law and Information Technology* 1. See e.g. Giovanni Sartor, ‘The Right to be Forgotten: Balancing Interests in the Flux of Time,’ (2016) 24 *International Journal of Law and Information Technology* 72, 74-78; Muge Fazlioglu, above n 2, 5-6; Alessandro Manterlero, above n 2, 230-232.

54 *Google Spain v Gonzalez* [2014] EUECJ C-131/12 at 81.

55 Ibid at 97.

56 Paul A Bernal, above n 2.
Another exception that potentially restricts the operation of the right to be forgotten is the ‘personal or household purposes’ exception. This is found in Article 2 of the General Data Protection Regulation, which provides that where the processing of personal data is by a ‘natural person in the course of a purely personal or household activity’, it will fall outside the scope of the Regulation. The personal and household exception covers most of the activities that people engage in online, uploading and sharing a personal image on a personal profile page. The household exemption was incorporated in the 1995 European Data Directive 95/46/EC, at a time where the internet had not begun and the information that people had was limited to written records or held on a computer that did not have internet. Given that the exception effectively excludes individuals from the right to be forgotten, it has very important consequences for how useful the right to be forgotten may be in protecting against online misuse of images.

**Misuse of personal data by companies**

Companies such as Google, Instagram, Facebook, Microsoft, Twitter collect, process and store vast amounts of personal data. These companies retain a significant amount of their users’ data which increasingly intrudes on people’s personal lives. As Mantereolo argues, ‘in

---

57 General Data Protection Regulation, Art 2.
60 Google Spain v Gonzalez C -131/12 per Advocate General Jääskinen who stated at [27] ‘In 1995, generalised access to the internet was a new phenomenon. Today, after almost two decades, the amount of digitalised content available online has exploded. It can be easily accessed, consulted and disseminated through social media, as well as downloaded to various devices, such as tablet computers, smartphones and laptop computers. However, it is clear that the development of the internet into a comprehensive global stock of information which is universally accessible and searchable was not foreseen by the Community legislator’ ; see generally Claire Bessant, ‘The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online’, [2015] 6(2) European Journal of Law and Technology < http://ejlt.org/article/view/390/570>.
a world where it is assumed that no value is attributed to privacy and oblivion, the ones to gain from this abandonment of old rights are the owners of these platforms or services which have an exclusive and comprehensive view of the entire mass of data. Social networks ‘represent an antimony because they do not share information taken from the data and even though they give little value to privacy and affirm the end of oblivion (describing life as a timeline); they extract a high value from this data.’ As Manterelo suggests, the data collected and stored by social networks represents ‘not only money but also power’ which facilitates the ongoing exploitation and the expropriation of users’ data. The right to be forgotten is an ‘attempt to reduce the amount of data collected’, which undermines the social network’s power. One of the consequences of the right to be forgotten is that it enables people to regain control over their data. The EU’s right to be forgotten aims to re-shift the power imbalance that social networks have held over their users’ images. As Bernal argues, this ‘kind of transfer of power, that kind of re-balancing, could have possibilities to redress the current imbalance over personal data – and to help re-establish at least some control that people have lost and feel that they have lost’.

While the right to be forgotten is not a mechanism that will actually prevent the misuse of personal images, it does provide a remedy for people who have had their personal images misused. This is because it enables people to request that when their images which have been misused that they are deleted from the network. In this sense the right to be forgotten would provide a practical solution for people who use social media, as well as non-members whose images are captured and uploaded online.

A number of arguments have been made against the right to be forgotten. In so far as the right allows an individual to have data about them deleted or removed, there is a concern that it will facilitate self-censorship. The fear here is that the right to be forgotten will allow

---

61 Alessandro Manterlero, above n 2, 234-5.
62 Ibid, 234.
63 Ibid, Manterelo states that ‘for this reason owners of big data have tried to make it more difficult to change privacy settings, have used technical devices to track users in a persistent way and have thus evoked the end of the privacy era.’
64 Ibid.
65 Ibid.
66 Paul A Bernal above n 2.
67 Bert-Jaap Koops, above n 3, 231; see generally PS Castellano, ‘The Right to be Forgotten Under European Law: A Constitutional Debate’ (2012) 16(1) Lex Electronica; Steven C Bennett, above n 26; Stijn Smet,
people to rewrite history; that is, that it will allow people to manage public information in order to ensure that only certain perspectives of them are in the public domain. While there is a chance that the right to be forgotten may be used in this way, this would require the courts to adopt a very broad reading of the type of situations where the right to be forgotten might be applied. On most readings, such cases of ‘censorship’ would only be allowed in limited and presumably justified situations such as when the data is outdated, irrelevant, or when a person withdraws their consent to have the data published.

Another concern with the right to be forgotten is that it will restrict freedom of speech and/or expression. It is clear that the right to be forgotten will remove information from the public domain. In introducing the right to be forgotten the intention of the European legislators was not to restrict freedom of the press or free speech; rather it was to protect an equally important right: personal privacy. Given that the General Data Protection Regulation includes an exception for free speech, it seems that many of the complaints about free speech are about the balancing of the rights and where the line is to be drawn. Any risk to free speech or freedom of the press has been incorporated into the General Data Protection Regulation, and any requests must be balanced against freedom of expression and the public interests.


68 See generally, Steven C Bennett, above 26; Stijn Smet, above n 26; Rolph H Weber, above n 26; see generally Omer Tene and Jules Polonetsky, above n 67.

69 Some scholars argue that the right to be forgotten needs to be framed in a different language, such as ‘the right to delete’; see generally Paul A Bernal, above n 2; Steven C Bennett, above n 26; Stijn Smet, above n 26; Rolph H Weber, above n 26; Omer Tene and Jules Polonetsky, above n 67.

70 see Bert-Jaap Koops, above n 3, 238, 238-40.

71 This is because there are a number of exceptions to the right to be forgotten as stated in General Data Protection Regulation, Art 17 (3) that paragraphs 1 and 2 will not apply to the extent of the processing is necessary:

(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in
There are a number of other problems with the right to be forgotten; one of which is that many aspects of the new regulation are uncertain. For example, when personal images are misused online, it is unclear whether the social network or the individual would be responsible to remove the image. This is important because the data subject may not be the owner of the image and would need the copyright owner or social network site to remove the photographs on their behalf. As a result, it may be unclear whether the data subject has a claim on the copyright owner to remove their image from their personal profile page. It is also uncertain whether the data subject has a claim on the social network provider to remove their image from the network. This is because the distribution of responsibilities is ‘unclear, since both the SNS provider and the user/uploader are being designated as data controllers in the standard interpretation of the Directive’.

Another problem with the right to be forgotten relates to the scope of the personal or household purpose exception. The problem here is that it is unclear ‘whether an individual posting personal data openly for a worldwide, unrestricted audience can still be considered to be processing the data for personal or household purposes.’ This is because, arguably, a person who disseminates an image on a social network may fall within a personal or household purpose.

Another issue that is unclear is the way in which the right to be forgotten will apply in relation to photographs (as distinct to written information). While it is clear that photographs will fall within the definition of ‘data’, what is less clear is when an image will trigger the right to be removed. For example, it is not clear what will need to change for a photograph to be declared ‘irrelevant’, ‘inadequate’, or ‘excessive’? Most of the examples given where the paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

72 see Bert-Jaap Koops, above n 3, 238, 238-40.
73 Ibid.
76 Google Spain v Gonzalez C-132/12, per Advocate General: N. Jääskinen, 93 said ‘It follows from
right to be forgotten apply in relation to textual data – newspapers stories and the like - not photographs. While this is an issue that needs clarification, it would seem that while photographs will trigger the right to be forgotten in certain situations, this will be harder to establish than with textual data. Although the right to be forgotten may not be exercised in relation to trivial matters such as changes in fashion or a bad haircut, it may apply where a photograph presents factual information that later becomes irrelevant or where the image contains sensitive data. 77 For example, concerning about a person’s their political views or revealing something their health. 78

There a number of practical issues that arise with the implementation of the right to be forgotten. One issue is that the removal of images may be difficult to implement. 79 Even though
a network may remove an image, it may still be possible to view the image online. This is because it may take some time to remove the image from the cache memory, or the images may be stored on a person’s hard drive or in the cloud.

8.5 Does Australia Need the Right to be Forgotten?

If adopted in Australia a right to be forgotten would help to restore the imbalance between people whose images are captured and those who control the data. An Australian right to be forgotten would also enable people to regain control over their images on social networks. If introduced it ‘could give individuals the possibility of more control over their data and hence more autonomy. It could directly reduce the amount of data that is held – hence that is vulnerable – as individuals exercise their right to delete. In Australia, a right to be forgotten would also address broader privacy concerns with respect to social networks. It would help to respond to the fact that social networks increasingly chip away at personal privacy. Particularly concerning is the way that people’s personal images are prone to misuse by those who collect information, as the data can be aggregated and combined with other forms of data, which can then be used for profiling.

It is arguable the right to be forgotten might also force social networks to justify why they are holding information. As Bernal said:

It could force those holding data to justify why they’re holding it – in such a way that the data subjects understand, for if data subjects cannot understand why the data is wanted, they might simply delete it. If there is a benefit and that benefit

---

Reinvention: An International Journal of Undergraduate Research
<http://www2.warwick.ac.uk/fac/cross_fac/iatl/reinvention/issues/volume7issue1/>

80 Cecile de Terwangne, above n 79, 117.
81 Ibid
83 See Paul A Bernal, above n 2.
84 Ibid.
85 Ibid
is made clear, why would an individual wish to delete that data? Most importantly of all, the fact that data could be deleted at any time could encourage the development of business models that do not rely on the holding of so much personal data.\textsuperscript{86}

In so far that the right to be forgotten ‘poses a paradigm shift in privacy’, where the ‘individuals have power that can and should restrict the actions of those who might oppress, abuse or take advantage of those individuals’,\textsuperscript{87} it will help individuals to regain control over how their personal images are used. For too long, privacy interests have been overshadowed by or come second to freedom of expression and speech. A right to be forgotten would be useful in Australia because it would potentially close some of the gaps in the existing legal protection for personal images in this country. A right to be forgotten would enable people to control use of their image, particularly when it is shared by other people on social networks.\textsuperscript{88}

A right to be forgotten could be adopted in Australia by amending the Australian \textit{Privacy Act} and the Australian Privacy Principles (APPs) to include ‘data subject’ protection rights similar to the EU’s \textit{General Data Protection Regulation}. Incorporating data subject rights in the Australia’s \textit{Privacy Act} would provide more relief for people when their image is misused. As noted earlier, the \textit{General Data Protection Regulation} allows a person to object to the transfer of their data to another country when the standard of data protection is not to the European standard. The Australian \textit{Privacy Act} has a similar provision under the Australian Privacy Principles (APPs), that relate to cross-border

\begin{center}
\begin{tabular}{l}
\textsuperscript{86} Ibid. \\
\textsuperscript{87} Ibid. \\
\textsuperscript{88} Virginia Da Cunha is an Argentinian singer, dancer, model and actress who had posted various pictures of herself in short shorts, swimsuits, tank tops and at least one sexually provocative pose on Twitter and Facebook. She sued Yahoo Argentina for linking and showing results of her name and image to websites offering sexual content, pornography, escorts and other related activities. \textit{Da Cunha v Yahoo de Argentina SRL: Juzgado de Primera Instancia (1a Inst, Court of First Instance, 29 July 2009); ‘Da Cunha, Virginia c. Yahoo de Argentina s/ Daños y Perjuicos’ (Resulta, I) para 3 http://www.diariojudicial.com/documentos/adjuntos/DIArchadjuunto17173.pdf (hereinafter Opinion of Judge Simari). Da Cunha was successful at first instance; however, she lost on appeal in 2014. See also Edward L Carter, ‘Argentina’s Right to be Forgotten (2013) 27(1) \textit{Emory International Law Review} 23. \\
\end{tabular}
\end{center}
disclosure of personal information. However, it is uncertain whether the Australian Privacy Principle 8 would provide adequate protection to prevent an Australian national’s data from being disclosed to a third-party country. This is because Australian Privacy Principle 8 is silent on whether the disclosure of the information to a third party would constitute a ‘transfer’. Australian Privacy Principle 8 provides that, prior to any disclosure of personal information to an overseas recipient, there must be reasonable steps taken to ensure that the overseas recipient does not breach the Australian Privacy Principles. However, what is reasonable is not defined in the legislation, which makes it difficult to determine whether a person in Australia would have the same rights as European citizens. Where data is processed and stored overseas, it may also be difficult to prove that the data is processed, collected or stored in Australia, or by an Australian corporation. Consequently, similar provisions should be adopted in Australia.

While the European right to be forgotten would provide Australian citizens with greater control over their images, to improve protection a number of changes should be considered to the European law. It would be important, for example, to clarify who has the responsibility to remove images (particularly where are multiple parties involved). It would also be important to clarify the situations where an image may be required to be removed or deleted.

It would also be helpful to clarify when consent could be withdrawn. To minimise the adverse effects of the exception it might also be useful to consider limiting its use to reasonable withdrawal. Consideration should also be given to amending the personal and household

---


90 Office of Australian Information Commissioner, APP Guidelines, Chapter 8: APP 8, Cross Border Disclosure of Personal Information, Taking Reasonable Steps to Ensure an Overseas Recipient Does Not Breach the APPs, 8.2, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information, which states that ‘before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs’ (s 16C).

91 Consent is provided in Article 7 (3) General Data Protection Regulation. See also, Recital 32 General
exemption.\textsuperscript{92} This is because if a personal and household purpose was included in Australian law it would leave many images unprotected and vulnerable to misuse. This would have to be done in a manner that carefully balanced the right of individuals to protect their personal images with the ability for individuals to express themselves by uploading images (which was the motivation behind the exceptions). In this sense this is not to suggest that exception should be abolished so much that it should be modified to take account of the realities of new technologies.\textsuperscript{93}

\textit{Data Protection Regulation}, provides ‘Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.’

\textsuperscript{92} Oliver Butler, “The Expanding Scope of the Data Protection Directive: The Exception for a Purely Personal or Household Activity” (September 15, 2015) \textit{University of Cambridge Faculty of Law Research Paper No. 54/2015} < SSRN: https://ssrn.com/abstract=2660916 > the author refers to the problem of using spatial logic in the interpretation of the exception of purely personal or household activity which applies to the Data Protection Directive 95/46/EC. In particular, at 4, the author refers to the \textit{Rynes v Urad pro Ochranu Osobnich Udaju C-212/13 [2014] ECR 0} where he quotes the Advocate General ‘In my view, ‘personal’ activities under the second indent of Article 3(2) of Directive 95/46 are activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others. These activities may, however, take place outside the home. ‘Household’ activities are linked to family life and normally take place at a person’s home or in other places shared with family members, such as second homes, hotel rooms or private cars. All such activities have a link with the protection of private life as provided for under Article 7 of the Charter.’

\textsuperscript{93} The Article 29 \textit{Data Protection Working Party} urged ‘the legislature to use the process of introducing new data protection law as an opportunity to reduce as far as possible the legal uncertainty that currently surrounds various aspects of individuals’ personal or household use of the internet.’ See Article 29 Working Party, Annex 2 Proposals for Amendments regarding exemption for personal or household activities < http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>
It is clear that the EU General Data Protection Regulation provides better protection for people whose images are shared and exchanged on social networks. This chapter argued that the European Union’s right to be forgotten is a useful mechanism that enables people to regain control over the use of their images within a social network context. Currently the law in Australia values freedom of expression over privacy. While this may have made sense in a pre-internet world, technological changes that have radically changed the way that images are used and controlled have challenged the now-outdated arrangements. The right to be forgotten would help to reset the scales between privacy and freedom of expression. It is time that Australian law provided people with the right to be forgotten as a way of preventing the misuse of their images. In so doing it would give them the right to control the use of their personal images online.
Chapter 9
Conclusion

‘It is apparent that the word ‘privacy’ has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts ... Like the emotive word ‘freedom’, ‘privacy’ means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.’

This thesis has examined the way Australian law protects personal images that are uploaded and shared on social networks. Part I (Chapters 1–5) examined the different interests that arise in two situations: when a creator takes and uploads their image and when a third party takes and uploads an image of someone else on a social network. The thesis has shown that while Australian law provides some protection in these two situations, this protection is limited and fragmented.

One of the consequences of the current law in Australia is that people whose images are uploaded and shared online are unable to control the use of their images. This has serious ramifications for many people. This thesis has argued that the limitations of the current legal protection in Australia allow the misuse of personal images on social networks to continue. In particular, it has highlighted that people in Australia do not have a right not to be photographed, and thus are unable to prevent the misuse of their image.

Drawing upon the developments in Europe and the United States, Part II of the thesis (Chapters 6–9) identified three potential areas that could improve Australian law to protect against the misuse of personal images shared online. One potential reform would be for the federal government to enact and introduce a statutory tort for serious invasions of privacy. Despite the number of potential reforms put forward in the ALRC’s 2014 report to adopt a statutory cause of action for serious invasions of privacy, the federal government has yet to respond.

Another way by which Australian law could be improved is through the introduction of image rights or a right of publicity. If a right of publicity was incorporated into tort law, people

---

would have a right to the use of their image, which may prevent third parties from using personal images of others. If Australia did introduce image rights into its common law, this would potentially solve some of the problems of sharing personal images of third parties online. However, establishing image rights in Australia would be the first step in providing a solution.

A third means of helping to close the gaps in Australian law would be to adopt and incorporate a ‘right to be forgotten’. As Chapter 9 highlighted, Australia already has the initial framework for such a right in the Commonwealth Privacy Act. If the Privacy Act were amended to include a right to be forgotten, it would provide greater protection for personal images than currently exists. The right to be forgotten would allow a person a mechanism to remove images that are misused online. In particular, while the right to be forgotten does not prevent a person’s image from being captured or shared online, it would provide a person whose image is uploaded or shared, and subsequently misused, with the ability to control the use of that image by requesting that the image be removed from a social network. Perhaps the most viable solution to the current legal framework is to incorporate and adopt image rights and a right to be forgotten.

The criminalisation of sharing and distributing sexual images online potentially addresses the misuse of certain types of personal images because it creates an image right for a specific type of image. One recent development in Australia that may provide some protection for the misuse of personal images is the proposed new ‘revenge porn’ laws which respond to the growing problem of so called revenge porn. Because of the proliferation of sharing sexual

---

2 The Australian Labor Party has introduced a proposed Bill against revenge porn; however, there has been no movement to pass the Bill. New South Wales is the third state in Australia to introduce revenge porn legislation. This is in line with the United Kingdom, which has made revenge porn illegal, see UK Parliament, House of Lords, Hansard, 21 July 2014, Column 968 Amendment 37 where Lord Marks of Henley-on-Thames stated that the term ‘revenge pornography’ refers to the publication, usually but not always, on the internet, of intimate images of former lovers without their consent …Obtaining such images has become more common and much easier with the prevalence, popularity and sophistication of smartphones; with their ability to take or record high quality images, still and video, instantly and simply with accompanying sound in the case of video … The widespread publication of such images causes, and is generally intended to cause distress, humiliation and embarrassment for the victim’; see also Criminal Justice and Courts Act 2015 (UK), s 33.

images online, some states in Australia have attempted to criminalise the misuse of sexual images. In effect these provide that a person would have a right for a specific type of use of their image – for example, when a person is photographed partially nude.

It is uncertain whether attempts to criminalise the use of sexual images online will resolve the problems that once when people share images on social networks. Moving forward, the potential criminalisation of capturing images of people that are of a sexual nature without their consent is a step in the right direction. This is because the proposed reforms potentially create an image right for a particular use of a person’s image. While criminalising the uploading and sharing of sexual images is an important development it creates a disparity of protection for personal images that fall outside the scope of protection. Even though some Australian states have initiated reforms to criminalise the uploading and sharing of sexual images on social networks, the law remains uncertain.

While it is beyond the scope of this thesis to go into the issue in much detail, it is important to note that there are many practical issues that will potentially impact upon the effectiveness of these potential reforms. As socio-legal studies teaches us, these factors are often integral to the effectiveness of legal policy. Of the many issues that arise two stand out. The first relates to problems of group photographs. The problem here is that as a photograph may contain images of a number there may be a series of different rights that need to be negotiated if one person wanted to protect the use of their image. As occurred with performer rights, a problem may arise where one member of the group does not agree with other group member’s wishes. In the absence of specific considerations, there are two options: one is that an individual is able to hold the group to ‘hostage’ or the wishes of the group override the interests of the individual. While there may be some

---

4 See South Australia’s prohibition of ‘invasive images’; Summary Offences (Filming Offences) Amendment Act 2013 (SA), which introduced s 26C (1) into the Summary Offences Act 1953 (SA). See also Crimes Amendment (Sexual Offences and Other Matters) Act 2014 (Vic) which introduced ss 4DA and 41DB Summary Offences Act 1966 (Vic). Currently, New South Wales has some criminal provisions for the publication of sexual images – for example, s 578C (2) Crimes Act 1900: see Tom Gotsis, ‘Revenge Pornography, Privacy and the Law’, NSW Parliamentary Research Service August 2015, e brief Issue 7/2015.

5 Group interests in a photograph would be similar to films with large casts. As James Grimmelman, notes in relation to ‘films with a large cast—the proverbial” cast of thousands.” The silent epic Ben-Hur advertised a cast of 125,000 people. In The Lord of the Rings trilogy, 20,000 extras tramped around Middle-Earth alongside Frodo Baggins (played by Elijah Wood). Treating every acting performance as an independent work would not only be a logistical and financial nightmare, it would turn cast of
solutions (such as redacting a person’s image), this is be an issue that needs to be taken into account when creating new legal arrangements.

A second more practical problem relates to the removal of images from the internet. The problem here is that when people share and exchange personal images on social networks, the images are stored on the networks information systems. As Ausloos says, even if ‘notice and take down procedures might take content out of the (public) sight,’ it does not result in the removal of the images from the data user’s servers.6 Similarly, it may be difficult for a person to remove their image when it is captured and uploaded online by a third party.7 Even if a person chooses to remove their images from their own profile page, the image may still be available if the image has been shared and resharred. These problems are exacerbated by the global nature of the internet, which may place images in jurisdictions with little or no protection: there is little use in demanding an image be removed in Australia if users in Australia can simply obtain the image from another country.

These practical problems highlight the difficulties of controlling the spread of images after they have been published on-line. Clearly it would be much better to prevent the uploading of images before it happens than attempt to remove images once they have been uploaded and shared. (Although this will necessarily occur where the removal of the image is demanded because of a change in circumstances, as with the right to be forgotten). Ideally, the solution would be to change the way people deal with and think about private images to prevent problems arising in the first place rather than dealing with the problems after the event. A range of measures have been suggested to prevent (potentially harmful) information being shared in the first place including ‘‘awareness raising, transparency, clearer privacy notices, data


7 Jef Ausloos, above n 6, 147 who states ‘but, in an ever-increasing social internet, where many features depend on disclosing data, ex post measures are needed as well. Enabling a more effective control by the individual, the introduction of a (well-defined) right to be forgotten’; see also Bert Jaap Koops, ‘Forgetting Footprints, Shunning Shadows. A Critical Analysis of the “Right to Be Forgotten” In Big Data Practice’ (2011) 8(3) ScriptEd 229, 237 -239.
miminisation, stricter control on the purpose limitation principle, anonymization, transparency, encryption. While we wait for these solutions, the potential harm to the fundamental human rights of dignity, autonomy and private life caused by the misuse of personal images on-line demands that Australian law be modified to provide more effective protection. This is also important to protect the economic and property rights that (some) people have in their image. While such legal changes will not provide a complete solution, they will help to counter some of the problems that have been created by that have arisen around social media in recent years.

---

8 Jef Ausloos, above n 6, 147.
Bibliography

Cases

10th Cantanae v Shoshana (1987) 79 ALR 299
A v B Plc [2003] QB 195
Abernethy v Hutchinson (1824) 1 H & Tw 28; 47 ER 1313
Angel Fraley et al. v Facebook, Inc., CA No. 511-01726
Argyll v Argyll [1965] 1 All ER 611
Argyll v Argyll [1967] Ch 302
Attorney General v Guardian Newspapers (No. 2) [1990] AC 109
Australian Broadcasting Corporation (ABC) v Lenah Game Meats Pty Ltd [2001] HCA 63;
(2001) 208 CLR 199
Australian Consolidated Press Ltd v Ettingshausen (Unreported, New South Wales Court of
Appeal)
Australian Football League v The Age Company Ltd (2006) 15 VR 419
Bathurst City Council v Saban (1985) 2 NSWLR 704
Bernstein of Leigh (Baron) v Skyviews & General Ltd [1978] 1 QB 479
Bernstein v Murray [1981] RPC 303
Boardman v Phipps [1967] 2 AC 46
Bradley v Wingnut Films Ltd (1992) 1 ERNZ 202
British Leyland v Armstrong [1986] RPC 279
Buck v Information Commissioner (2007) WL 426611; [2008] WTLR 1

C v Holland (2012) 3 NZLR 672
Campbell v MGN Ltd [2003] QB 633
Campbell v MGN Ltd [2004] 2 AC 457
Chang v Virgin Mobile USA, LLC, 2009 WL 111570 (N.D.Tex. January 16, 2009)
Church of Scientology v Kaufman [1973] RPC 627
CMI-Centers v Phytopharm [1999] FSR 235
Coco v AN Clark (Engineers) Ltd [1969] RPC 4
Collins (Engineers) Ltd v Roberts & Co Ltd [1965] RPC 429
Collins v Wilcock (1984) 1 WLR 1172
Creation Records Ltd v News Group Newspapers Ltd [1997] EMLR 444
Cruise v Southdown Press Pty Ltd (1993) 26 IPR 125
DeMaudsley v Palumbo [1996] FSR
Doe v Yahoo!7 Pty Ltd [2013] QDC 181
Douglas v Hello! [2001] QB 967 (Douglas (No 1)
Douglas v Hello! Ltd [2001] 2 WLR 992, 1025; [2001] 2 All ER 289, 320
Douglas v Hello! Ltd [2003] EMLR 31 (Ch); [2006] QB 125 (CA)
Douglas v Hello! Ltd (No 3) [2006] QB 125
Douglas v Hello! (No 3) [2005] EWCA Civ 595; [2005] 3 WLR 881
Douglas v Hello! [2008] 1 AC 1
Duke of Queensbury v Shebbeare (1758) 2 Eden 329; 28 ER 924
Dye v Commonwealth [2010] FCA 720
Edwards Hot Water Systems v SW Hart Pty Ltd (1985) 5 IPR 1
Foster v Mountford [1978] FSR 582
Foster v Svenson (2013) NY Slip Op 31782 NY Supreme Court 2013
Francome v Mirror Group Newspapers [1984] 1 WLR 892
Franklin v Giddins [1978] Qd R 72
Gee v Burger [2009] NSWSC 149
Giller v Procopets [2004] VSC 113
Giller v Procopets (2008) 79 IPR 489
Google Spain v Gonzalez Case C-131/12.
Green v Broadcasting Corporation of New Zealand [1989] RPC 469
Grollo v Palmer (1995) 184 CLR 348
Hanson-Young v Bauer Media Limited [2013] NSWSC 1306
Hanson-Young v Bauer Media Ltd (No 2) [2013] NSWSC 2029
Henderson v Radio Corp Pty Ltd [1960] SR (NSW) 576
Hogan v Koala Dundee Pty Ltd (1988) 20 FCR 314
Holden v Express Newspapers Ltd (QBD), 7 June 2001

Honey v Australian Airlines Ltd and House of Tabor Inc (1990) 18 IPR 185

Hosking v Runting (2005) 1 NZLR 1

Hunter and Others v Canary Wharf Ltd; Hunter and Others v London Docklands Corporation [1997] AC 655

Oldham v Lawson (No 1) [1976] VR 654

Inline Logistics v UCL Logistics [2002] RPC 611

Jacqueline A v The London Borough of Newham (2001) WL 1612596

Jane Doe v ABC & Ors [2007] VCC 281

John v Associated Newspapers Ltd [2006] EMLR 27

John Fairfax Publications Pty Ltd v Rivkin (2003) 201 ALR 77

John Zinc v Lloyds Bank [1975] RPC 385

Kalaba v Commonwealth [2004] FCA 763; FCAFC 326

Kaye v Robertson (1990) 19 IPR

Kaye v Robertson [1991] FSR 62

Khorasandijan v Bush [1993] QB 727

Les Editions Vice-Versa Inc v Aubry [1998] 1 SCR 591

Lincoln Hunt (Australia) Pty Ltd v Willesee (1986) 4 NSWLR 457

Lord Ashburton v Pape [1913] 2 Ch 469

Louis v Smellie (1895) 73 LT 226

Macklin v Richardson (1770) Ambl 695; 27 ER 451,

Maggbury Pty Ltd v Hafele Australia Pty Ltd (2001) 210 CLT 181 53 IPR

Malone v Metropolitan Police Commissioner (1979) 2 WLR 700; [1979] Ch 344

Maynes v Casey [2011] NSWCA 156 (14 June 2011)

McKennitt v Ash [2007] EMLR 113

McKennitt v Ash [2005] EWHC 3003 (QB)

Millar v Taylor (1769) 4 Burr 2303l 98 ER 201

Mills v News Group Newspapers [2001] EMLR 957

Moreno v Hanford Sentinel Inc, 09 CDOS 4208

Morrison v Moat (1851) 68 ER 492

Mosley v News Group Newspapers Ltd [2008] EWHC 1777 (QB)
Mossimani by his Tutor Karout v Australian Radio Network Pty Ltd (ACN 065986 987) [2016] NSWDC

Murray v Express Newspapers PLC [2007] EWHC 1908

Murray v Express Newspapers plc [2009] Ch 481

Newton-John v Scholl-Plough (Aust) (1986) 11 FCR 233

Nichrothern Electrical Co Ltd v Percy [1956] RPC 272 (on appeal) [1957] RPC 207

OBG Ltd v Allan [2008] 1 AC 1 (HL)

Ocular Sciences [1997] RPC 289

PA Thomas v Mould [1968] QB 913

Pacific Dunlop Ltd v Hogan (1989) 23 FCR 553

Peck v United Kingdom (2003) 36 EHRR 41


Phillip v Pennel [1907] 2 Ch 577

Pollard v Photographic Co (1889) 40 Ch D 345

Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation [2011] AATA 907

Prince Albert v Strange (1849) 47 ER 302

R v Central Independent Television [1994] Fam 192

R v Khan [1997]AC 558

R v Sotheren [2001] NSWSC 204 (16 March 2001)

Raciti v Hughes (1995) 7 BPR 14

Re X [1975] Fam 47

Robin Jig v Tool Co Ltd v Taylor [1979] FSR 130

Saad v Chubb Security Australia Pty Ltd [2012] NSWSC 1183 [183],

Saltman Engineering Co Ltd v Campbell Engineering Co Ltd (1948) 65 RPC 203 (CA)

Pollard v Photographic Co (1889) 40 Ch D 345;

Sands & McGougal Pty Ltd v Robinson (1917) 23 CLR 49

Schrems v Data Protection Commissioner Case C-362/14

Seager v Copydex (No 1) [1967] 2 All ER 415
Sean Lane, et al. v. Facebook, Inc et al. No 10-16380 (9th Circuit 2012)

Seven Network (Australia) Operations Ltd v Australian Broadcasting Corporation [2007] NSWSC

Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance (MEAA) [2004] FCA 637

Shelly Films v Rex Features [1994] EMLR 134

Shepherd v Walsh [2000] QSC 177

Shepherd v Walsh [2001] QSC 358

Shering Chemicals Ltd v Falkman [1981] 2 WLR 848

Shoshana Pty Ltd v 10th Cantanae Pty Ltd (1987) 11 IPR 249

Smith Kline & French v Department of Community Health [1990] FSR 617

Steddal v Houghton (1901) 18 TLD 126

Stephens v Avery [1988] 1 Ch 449

The Duke of Queensberry v Shebbeare 2 Eden, 329


Trkulja v Google (No 5) [2012] VSC 533

Theakston v MGN Ltd [2002] EMLR 22

Theakston v MGN Ltd [2002] EWHC 137 (QB)

University of London Press v University Tutorial Press Limited [1916] 2 Ch 601

Valeo Vision Societ Anonyme v Flexible Lamps [1995] RPC 205

Victoria Park Racing and Recreations Grounds Co Pty v Taylor [1937] HCA 45

von Hannover v Germany App. No 59320/00 24 June 2004

Wainwright v Home Office [2003] UKHL 53; [2003] All ER 279

Wheatley v Bell [1984] FSR 16

Wickham v Association of Pool Builders 1988 12 IPR 567

Wilson v Ferguson [2015] WACA 15

WL v Randwick City Council [2007] NSW ADT 12

Yovatt v Winyard (1820) 1 Jac & W 394; 37 ER 425

Legislation

Civil Law (Wrongs) Act 2002 (ACT)
Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

Copyright Act 1968 (Cth)

Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Defamation Act 2005 (NSW) 2005
Defamation Act 2005 (Qld) 2005
Defamation Act 2005 (SA) 2005
Defamation Act 2005 (Tas)
Defamation Act 2005 (Vic)
Defamation Act 2005 (WA)
Defamation Act 2006 (NT)


Health Quality and Complaints Commission Act 2006 (Qld)
Health Records Act 2001 (Vic)
Health Records and Information Privacy Act 2002 (NSW)
Human Rights Act 1998 UK
Information Act 2002 (NT)
Information Privacy Act 2009 (Qld)
Information Privacy Act 2014 (ACT)
Personal Information and Protection Act 2004 (Tas)
Premier and Cabinet Circular No 12 (SA)
Privacy Act 1988 (Cth)
Privacy and Data Protection Act 2014 (Vic).

Privacy and Personal Information Protection Act 1998 (NSW)
Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM 2012


Secondary sources


Anyanwu, C, ‘Challenges to Privacy Law in the Age of Social Media’ (2013) 40(3) *Australian Journal of Communication* 121.


Bostic, Kevin, ‘No, Facebook Messenger Will Not Eat Your Privacy … Any More Than Facebook Already Has, at Least’, *Inquisitr*, 10 August 2014,


Caddick, Nicholas and Harbottle, Gwilyn (eds), Copinger and Skone James on Copyright, 14th ed. (Sweet and Maxwell, 1999).


Carbone, C.E, ‘To be or Not to be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age’ (2015) 22(3) Virginia Journal of Social Policy and the Law 525.


Colombi Ciacchi, Gert, Brüggemeier, Patrick, O'Callaghan, Aurelia, Personality Rights in European Tort Law (Cambridge University Press, 2010).


Doyle, Carolyn and Bagaric, Mirko, Privacy in Australia (Federation Press, 2005).


Felcher, Peter L and Rubin, Edward L, ‘Privacy, Publicity and the Portrayal of Real People by the Media’ (1979) 88(8) Yale Law Journal 1577.


Fiorella, Sam, ‘The Insidiousness of Facebook Messenger’s Android Mobile App Permissions (Updated)’, The Huffington Post (8 November 2014), http://www.huffingtonpost.com/technology.


Fuchs, Christian ‘An Alternative View of Privacy on Facebook’ (2011) 2(1) Information 140.


Giurgiu, Andra, ‘Challenges of Regulating a Right to be Forgotten with Particular Reference to Facebook’ (2013) 7(2) Masaryk University Journal of Law and Technology 361.


Global Voices Advocacy Defending Free Speech Online, ‘Spain on a Downward Spiral? New Law May Destroy the Digital Commons’ (July 2014),


Graves, Zachary, ‘The Dangerous Proliferation of the “Right to be Forgotten”, Huffington Post Technology (18 June 2014).


Grimmelmann, James, ‘The Internet is a Semicommons’ (2009–10) 78 Fordham Law Review 2799.


Harder, Sirko, ‘Gain-Based Relief for Invasion of Privacy’ (2011) 1 DICTUM Victoria Law School Journal 63.


Haythornthwaite, Caroline, ‘Social Networks and Internet Connectivity Effects’ (2005) 8(2) Information, Communication, & Society 125.


Hicks, Aubrie, ‘The Right to Publicity After Death: Post Mortem Personality Rights in
Seattle University of Law Review 275.

Some Will Predictably Inhibit “Fair Use”’, FindLaw (12 November 2007),

Hill, Kashmir, ‘Either Mark Zuckerberg Got a Whole Lot Less Private or Facebook’s CEO
Doesn’t Understand The Company’s New Privacy Settings’, Forbes (12 October
2009), http://forbes.com/sites/kashmirhill/2009/12/10/either-mark-zuckerberg-got-a-
whole-lot-less-private-or-facebook's-ceo-doesn't-understand-the-companys-new-
private-settings.

Hinkler, Amy A, ‘Privacy in the Age of Social Media Mergers and Acquisitions’ (2013),
https://works.bepress.com/amy_hinkler/1/download.

Hoadley, Christopher M, Xu, Heng, Lee, Joey J and Rosson, Mary Beth, ‘Privacy as
Information Access and Illusory Control: The Case of the Facebook News Feed
Privacy Outcry’ (2010) 9(1) Electronic Commerce Research and Applications,


Hogan, Bernie ‘A Comparison of On and Offline Networks Through the Facebook API’

Hornung, G, ‘A General Data Protection Regulation for Europe? Light and Shade in the

of Law & Technology 443.

Hoven, Michael, ‘Balancing Privacy and Speech in the Right to be Forgotten’,


Jones, H and Soltren, JH, ‘Facebook: Threats to Privacy’, unpublished paper (2005),


Judge, Elizabeth F and Gervais, Daniel, ‘Of Silos and Constellations: Comparing Notions of
Originality in Copyright Law’ (2009) 27 Cardozo Arts and Entertainment 375.

Jung, Andrew M, ‘Twittering Away the Right of Publicity: Personality Rights and Celebrity
Impersonation on Social Networking Sites’ (2011) 86 Chicago-Kent Law Review 381.

Kalinda, Basho, ‘Licensing of Our Personal Information: Is It a Solution to Internet Privacy?’

Kalven, H Jr, ‘Privacy in Tort Law: Were Warren and Brandeis Wrong?’ (1966) 31 Law and
Contemporary Problems 326.

Kane, B, ‘Balancing Anonymity, Popularity, and Micro-Celebrity: The Crossroads of Social
Networking and Privacy’ (2010) 20(2) Albany Law Journal of Science and
Technology 327.

Review 1193-1294

Review 1193.

Kaplan, A and Haenlein, M, ‘Users of The World, Unite! The Challenges and Opportunities

Kasper, Debbie V. S. ‘The Evolution (Or Devolution) of Privacy’ (2005) 1, Sociological
Forum 20, 69.


Kirkpatrick, Marshall, ‘Facebook’s Zuckerberg Says the Age of Privacy is Over’,


Krishnamurthy, Balachander and Wills, Craig E, ‘Characterizing Privacy in Online Social Networks’, In Proceedings of the First Workshop on Online Social Networks (ACM, 2008).

Krishnamurthy, Balachander and Wills, Craig E, ‘On the Leakage of Personally Identifiable information via online social networks’, in Proceedings of the 2nd ACM workshop on Online Social Networks (ACM, 2009).


Kuczerawy, Aleksandra, ‘Facebook and Its EU Users: Applicability of the EU Data Protection Law to US Based SNS’, in M Bezzi et al. (eds), Privacy and Identity (International Federation for Information Processing, 2010).


Lee, E, ‘Warming Up to User-Generated Content’ (2005) 2(1) University of Illinois Law Review 102/

Lee, N, Facebook Nation: Total Information Awareness (Springer, 2013).


Locke, John, John Locke, Two Treatises, Book II.

Lopez-Portas, B, ‘The Right to be Forgotten in the EU: The Importance of its Juridicial Regulation to Guarantee Personal Rights in Public Places’, in WCCL – Workshop 8:
The Citizen and the State in the Digital Age,
https://www.jus.uio.no/english/research/news-and-

Ludwig, FJ, ‘Peace of Mind in 48 Pieces v Uniform Right of Privacy’ (1948) 32 Minnesota
Law Review 734.

10 Law Text Culture 135.

Lum, Aimee Jodoi, ‘Don’t Smile, Your Image Has Just Been Recorded on a Camera-Phone:
The Need for Privacy in the Public Sphere’ (2005) 27 University of Hawai’i Law
Review 377.

Luo, W, Xie, Q and Hengartner, U, ‘Face Cloak: An Architecture for User Privacy on Social
Networking Sites’, in Proceedings IEEE CSE’09, 12th IEEE International Conference
on Computational Science and Engineering (2009).

Lussier, Jake T, Raeder, Troy and Chawla, Nitesh V, ‘Digging Up the Dirt on User Generated
Content Consumption’, in International Conference on Management of Data COMAD
2010 (2010).


Madow, Michael , ‘Private Ownership of the Public Image: Popular Culture and Publicity

Magtelli, Cara, ‘Facebook is Not Your Friend: Protecting a Private Employee’s Expectation
of Privacy on Social Networking Content in the Twenty-First Century Workplace’

Manterelo, Alessandro, ‘The EU Proposal for A General Data Protection Regulation and the


McCarthy, J Thomas, The Rights of Publicity and Privacy (Clark Boardman Callahan, 1995).


Moffatt, Alex, ‘The Copyright Bill’ (1898) 10 The Judicial Review 161.


Morgan, O, ‘Copyright, the Public Interest and Content Restrictions’ (2003) 8 Media and Arts Law Review 213.


Nordhaus, Jamie E, ‘Celebrities’ Rights to Privacy: How Far should the Paparazzi be Allowed to Go?’ (1999) 18(2) The Review of Litigation 286.

Witzleb, Norman, ‘Justifying Gain Based Remedies for Invasions of Privacy’ (2009)


O’Hara, K, Shadbolt, N and Hall, W, A Pragmatic Approach to the Right to be Forgotten, (Global Commission on Internet Governance, 2016),


Opsahl, Kurt, ‘Facebook’s Eroding Privacy Policy: A Timeline’ (2010),


Orlowski, Andrew, ‘UK Gov Passes Instagram Act: All Your Pics Belong to Everyone Now’,

*The Register* (29 April 2013),

http://www.theregister.co.uk/2013/04/29/err_act_landgrab.

Ovadia, S, ‘An Early Introduction to the Google+ Social Networking Project’ (2011)

30 *Behavioural and Social Sciences Librarian* 259.


Perez, Juan Carlos, ‘Facebook’s Beacon More Intrusive Than Previously Thought’, *IDG News* (30 November 2007).


Pletcher, Christa, ‘Are Publicity Rights Gone in a Flash? Flickr, Creative Commons, and the Commercial Use of Personal Photographs’ (2009) 8(1) Florida State University Business Review 129.


Posner, Eric, ‘We All Have the Right to be Forgotten’, Slate (May 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html.


Redmond, Sean and Holmes, Su, Stardom and Celebrity: A Reader (Sage, 2007).


Sanvenero, Richard, ‘Social Media and Our Misconceptions of the Realities’ (2013) 22(2) *Information and Communications Technology Law* 89-108


Sarvas, Risto and Frohlich, David M, ‘The Future of Domestic Photograph in From Snapshots to Social Media - The Changing Picture of Domestic Photography


Scherker, Amanda, ‘Didn’t Read Facebook’s Fine Print? Here’s Exactly What It Says’, *The Huffington Post* (21 January 2014),


Stewart, Daxton R, ‘Can I Use This Photo I Found on Facebook? Applying Copyright Law and Fair Use Analysis to Photographs on Social Networking Sites Republished for News Reporting Purposes’ (2012) 10 *Journal on Telecommunications and High Technology Law* 93.


Townsend Gard, Elizabeth and Whetstone, Bri, ‘Copyright and Social Media: A Preliminary Case Study of Pinterest’ (2013) 31 Mississippi College Law Review 249.


Tushnet, Rebecca, ‘All of This Happened Before and All of This Will Happen Again: Innovation in Copyright Licensing’ (2014) 29 Berkeley Technology Law Journal 1447.


Wacks, Raymond, Privacy and Media Freedom (Oxford Scholarship Online, 2013),


Wagner, Mike and Yun, Li-Reilly, ‘The Right to be Forgotten’ (2014) 72(6) The Advocate 823.


Young, Alyson L and Quan-Haase, Anabel, ‘Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook’, in Proceedings of the Fourth International Conference on Communities and Technologies (ACM, 2009).


Zimmer, Michael, “‘But the Data is Already Public’: On the Ethics of Research in Facebook’ (2010)

12 *Ethics Information Technology* 313.