The Law Handbook

YOUR PRACTICAL GUIDE TO THE LAW IN NEW SOUTH WALES

15th EDITION

THOMSON REUTERS

REDFERN LEGAL CENTRE PUBLISHING

Published in Sydney
by Thomson Reuters (Professional) Australia Limited
ABN 64 058 914 668

19 Harris Street, Pyrmont NSW 2009
First edition published by Redfern Legal Centre as *The Legal Resources Book (NSW)* in 1978.
First published as *The Law Handbook* in 1983
Second edition 1986
Third edition 1988
Fourth edition 1991
Fifth edition 1995
Sixth edition 1997
Seventh edition 1999
Eighth edition 2002
Ninth edition 2004
Tenth edition 2007
Eleventh edition 2009
Twelfth edition 2012
Thirteenth edition 2014
Fourteenth edition 2016
Fifteenth edition 2019

Note to readers: While every effort has been made to ensure the information in this book is as up to date and as accurate as possible, the law is complex and constantly changing and readers are advised to seek expert advice when faced with specific problems. *The Law Handbook* is intended as a guide to the law and should not be used as a substitute for legal advice.

ISBN: 9780455243689

This edition is up to date as of 1 October 2019.

The Law Handbook is part of a family of legal resource books published in other states:
Vic: *The Law Handbook* by Fitzroy Legal Service, ph: (03) 9419 3744
SA: *Law Handbook* by the Legal Services Commission of South Australia, ph: (08) 8111 5555
Qld: *The Queensland Law Handbook* by Caxton Legal Centre, ph: (07) 3214 6333
Tas: *Tasmanian Law Handbook* by Hobart Community Legal Service, ph: (03) 6223 2500
NT: *The Northern Territory Law Handbook* by Northern Territory Legal Aid Commission, Australasian Legal Information Institute and Darwin Community Legal Services, ph: (08) 8982 1111

Editor: Newgen Digitalworks
Product Developer: Karen Knowles

Printed by: Ligare Pty Ltd, Riverwood, NSW

This book has been printed on paper certified by the Programme for the Endorsement of Forest Certification (PEFC). PEFC is committed to sustainable forest management through third party forest certification of responsibly managed forests.

30

Internet Law

Niloufer Selvadurai – Deputy Dean of Law – Operations and Planning, Macquarie Law School, Macquarie University

Introduction

[30.10] The internet is a network of computers linked via a shared "language" or "protocol", known as TCP/IP. Neither it is administered by a central body, nor does it have any fixed location or point of administration. The "content" of the internet is created by public and private users and distributed "online" via optical, fibre and other networking technologies.

For most users, connection is made through a company that offers internet access. Individuals or organisations involved in enabling access to the internet fall under the following categories:

1. the content provider, who creates the material that is uploaded onto a website;
2. the internet content host (ICH), who provides the website and controls what is uploaded; and
3. the internet service provider (ISP), who supplies internet access so that the material can be transmitted to individual computers and then viewed and downloaded by members of the public.

Legal issues arising from use of the internet have tended to result from three specific areas: first, the publication of particular types of information "online"; second, the reproduction and distribution of content such as text, sound and images; and finally, the online sale of goods and services.

It is important to recognise that the internet is not subject to its own governing legislation (ie, an "Internet Act"), notwithstanding the considerable number of legal issues arising through its use. The internet is often described as the "wild west" of the law, insofar as it is largely unencumbered by the type of case-specific laws and regulations that are operative on other forms of media. Indeed, the approach to regulation of the internet to date has largely been to reconcile any such issues within pre-existing laws and regulations.

Relevant legislation

[30.20] Commonwealth

Competition and Consumer Act 2010;
Copyright Act 1968;
Crimes Act 1914;
Criminal Code Act 1995;
Designs Act 2003;
Electronic Transactions Act 1999;
Interactive Gambling Act 2001;
Patents Act 1990;
Privacy Act 1988;
Racial Discrimination Act 1975;
Spam Act 2003;
Telecommunications Act 1997;
Telecommunications (Interception and Access) Act 1979;
Trade Marks Act 1995.

[30.30] New South Wales

Anti-Discrimination Act 1977;
Defamation Act 2005;
Electronic Transactions Act 2000;
Fair Trading Act 1987.

Defamation on the internet

[30.40] In *Dow Jones v Gutnick* (2002) 210 CLR 575, the High Court confirmed that:

- The laws governing defamation on the internet are the same as those that govern defamation in other types of publications.
- *Publication* (one of the elements of defamation) occurs when material is downloaded, read and comprehended by a reader.

Unintentional meanings

The nature of the internet allows users flexibility in:

- how they view information;
- how they contribute to a site through bulletin boards or chat rooms.

This may have consequences for defamation in that unintentional *imputations* (the meaning conveyed by the material) may arise from words or images on a website that are linked to words or images on a different site.

Independently the words or images may be innocent. When linked, they may acquire a defamatory meaning.

It could be argued that you may be found liable for linking to defamatory material on another website, although there do not appear to be any cases where this has been successfully put forward.

[30.50] Posting defamatory material

In addition to liability for defamatory material on your own website, you can also be found liable for posting defamatory material on other sites, including blog services and popular community sites like Facebook, YouTube and Wikipedia. This is the case even if you are not the author or creator of the defamatory material (eg, if you posted a friend's home video to YouTube). Even if you think that you are just expressing a personal opinion on a public issue, you may still be liable if you do not have a legitimate basis for your comments and your comments damage the reputation of an individual. In *Dods v McDonald* [2016] VSC 201, the defendant was found liable for posting defamatory material on a website about the actions of the plaintiff police officer. A defence of fair comment was rejected on the basis the defendant's comments were "a baseless challenge to the moral foundation of the plaintiff's personal integrity and public standing".

Responsibility of internet service providers and internet content hosts

The *Defamation Act 2005* (NSW) provides a defence of "innocent dissemination" for subordinate distributors, which means that a defamation action can potentially be defended by both an internet service provider and an internet content host, provided that:

- They were not the first or primary distributor of the material.
- They were not its author or originator.
- They did not have capacity to exercise editorial control over the content before publication.
- They did not know, or could not reasonably have known, that the matter was defamatory.
- Their lack of knowledge was not due to any negligence on their part.

Notification of a defamatory posting

It is important to give notice, or respond to a notice, about potentially defamatory material promptly.

If you are notified that you have posted defamatory material on a website, you should immediately seek legal advice as to whether you may be liable for defamation.

If you consider that the material is defamatory and you do not have a defence (considered in the following pages), you should remove the material immediately.

Offers to make amends

If someone alleges that you have defamed them, you can make an "offer to make amends". You must do so within 28 days of receiving a written notice of the complaint. The offer to make amends must also be in writing and must include:

- an offer to publish a reasonable correction;
- an offer to pay expenses reasonably incurred by the complainant to the time of the offer.

If your offer is accepted, the matter ends there. If your offer is rejected and you are taken to court, the court may reduce any damages payable, provided your offer was reasonable.

Publishing an apology

An apology cannot be used against you as an admission of liability. Also, if the defamation claim is successful, an apology may help to reduce the damages.

For information on defamation generally, see Chapter 31, Media Law.

Online shopping – protection of consumers

[30.60] Consumer protection on the internet

When a person buys goods or services over the internet from an Australian trader, Australian consumer protection laws, such as the *Competition and Consumer Act 2010* (Cth), apply (a "trader" is defined as a business or individual engaging in trade or commerce).

There are no laws in Australia that specifically deal with online shopping. Legally the same requirements exist whether the purchase is conducted over the internet or offline (such as shopping at a retail outlet).

The laws protecting the rights of Australian consumers are discussed in Chapter 10, Consumers.

When shopping online, important consumer protection laws to consider are those dealing with:

- unconscionable conduct;
- misleading or deceptive conduct;
- implied warranties and conditions.

Unconscionable conduct

Generally, unconscionable conduct occurs whenever a consumer is at a special disadvantage in dealing with the trader because of illness, ignorance, inexperience, impaired faculties, financial need or other circumstances affecting their ability to protect their own interests and the trader takes advantage of the situation.

Misleading or deceptive conduct

Traders in Australia must not engage in conduct that is misleading or deceptive, or is likely to mislead or deceive. Prohibited conduct may be constituted by an overt statement about existing facts, a prediction about the future, or even silence.

For the conduct to be illegal, it must convey or contain a misrepresentation, not merely be confusing. Whether the trader intended the conduct to carry any particular meaning is irrelevant.

The following must not be misleading or deceptive, or likely to mislead or deceive:

- material on a website;
- the conduct of an online trader, including:
  - advertising;
  - writing;
  - conducting business; and
  - putting information on the internet about the business, products or service.

Implied conditions and warranties

When consumers purchase goods and services from traders, various non-excludable conditions and warranties are implied by the law.

In other words, certain terms become part of the contract even though not specifically included or referred to. Any attempt to exclude, restrict or modify rights or liabilities (responsibilities) under these implied conditions and warranties will be void (ie, not effective).

Goods purchased online

Under implied warranties, goods bought from a trader online must:

- comply with the description of them relied on by the consumer;
- be of merchantable quality, unless:
  - the relevant defect was drawn to the consumer's attention before the contract was made; or
  - the consumer examined the goods before sale and should have found the defect;
- be fit for their purpose if that purpose was made known to the trader.

Implied warranties and auctions

In NSW, implied warranties can be excluded when goods have been bought at an auction.

Services purchased online

Under implied warranties, if a service is bought online from a trader:

- The service must be provided with due care and skill.
- Any materials supplied in connection with the service must be reasonably fit for the purpose for which they are supplied.
- If the customer makes known the purpose for which the service is required, the service (and any materials) must be reasonably fit for that purpose in most cases.

Other consumer protection laws

Other consumer protection laws may apply to the purchase of goods and/or services over the internet, depending on the circumstances.

[30.65] Internet scams

Unfortunately, the internet is subject to fraud just like the offline world. Given the nature of the internet, which allows for anonymous and cross-border transactions, it may be difficult to bring those who commit online frauds to justice. When shopping online, you should be more aware of scams than when shopping offline.

For information about how to recognise, avoid and report internet scams, visit the Australian Competition and Consumer Commission's website www.scamwatch.gov.au.

[30.70] Purchasing goods and services from overseas suppliers

Application of consumer protection laws

When you buy something over the internet from an overseas trader, it is not always certain whether Australian consumer protection laws apply or whether an Australian court has jurisdiction.

Is it worth it?

Even if Australian consumer protection laws apply and an Australian court has jurisdiction, it may be too difficult or too expensive to enforce a judgment against a trader with no assets in Australia.

Does the trader carry on business in Australia?

The *Competition and Consumer Act* applies to overseas traders carrying on business in Australia.

If an internet overseas trader is found to have been carrying on business in Australia, Australian consumer protection laws apply, even if the contract states otherwise ("this contract is governed by the laws of California").

If Australian laws cannot apply (because the trader is found not to have been carrying on business in Australia), the consumer protection laws of the trader's country (if there are any) will apply. This may result in you having fewer rights online than if the purchase had been made in Australia.

Going through customs

When overseas traders supply physical goods, the Australian Customs Service checks them to decide whether they should be cleared for entry. Imported goods that are prohibited or restricted are seized. Others may require a permit.

Customs duty

Imported goods may also be subject to customs duty. Relevant factors in determining the rate of duty payable by the importer (ie, the consumer) include:

- the classification of the item by the Australian customs tariff;
- the country of origin.

The goods and services tax

The Australian Customs Service also levies GST on imports. Low value thresholds apply, and the method of ordering (electronic, phone or mail) does not affect whether GST is payable.

When purchasing from overseas?

- Find out from the Australian Customs Service whether you can legally import the goods you wish to buy and whether they are subject to GST (or equivalent) or any other taxes.
- Goods bought from overseas can have significant delivery expenses, so always check the delivery charges carefully.
- Overseas traders may not list the purchase price of the goods or services in Australian dollars – do the conversion.
- Check the overseas trader's website for any terms and conditions that state which country's laws apply and which country's courts would be relevant to bringing an action should a dispute arise.

It is common practice for an overseas trader to designate the law and courts as being those of the country where the business is located. However, as noted earlier, these clauses are not always determinative where a trader is found to have been conducting a business in Australia.

How to protect yourself when shopping online?

[30.80] Before you buy something online, you should obtain certain information in order to protect yourself.

Who is the trader?

Establish who is selling the goods or services, including details of the trader's business: physical address, business registration details (such as business name and/or ACN/ABN number) and contact details.

The Australian Securities and Investment Commission (ASIC) has a free service on its website (www.asic.gov.au) allowing users to search for registered business names. ACN/ABN numbers of Australian organisations are located at www.asic.gov.au/online-services/search-asics-registers.

What are the details of the transaction?

Knowing the full details of the transaction before entering into an agreement with the trader will help you to know what to expect if you buy the goods or services. Details you should obtain include:

- a clear description of what is being purchased;
- the full cost in Australian dollars, including costs such as delivery, insurance and credit card charges;
- any return, exchange, refund and warranty policies;
- when and how delivery will take place;
- the terms of any insurance (eg, does it include damage to the goods while being delivered?);
- complaints-handling and dispute-resolution policies;
- the terms and conditions of the agreement. Read them carefully – you are agreeing to be bound by them.

Always print out any terms and conditions that you agree to – traders may change them later. Keep copies of your correspondence (including emails) with the trader, and print out any forms that you fill in and any offers on web pages that you accept – they are relevant to your transaction.

Privacy concerns

Always check for a privacy policy on the trader's website. The policy should explain why the trader collects your personal information and how that information will be used. The trader might want to use your personal information for marketing purposes or even to sell it to third parties. The privacy policy should tell you if this is so.

If there is no privacy policy on the trader's website you should be concerned, because the trader is not informing you of what will happen to any personal information that you submit.

Security concerns

People often use credit cards for online shopping. This involves submitting credit card details over the internet. The nature of the internet means that transmitted information may be intercepted by a third party.

In order to minimise the risk you should make sure that the trader is using a secure system for transferring information during a transaction. The most common method used in online shopping is the *secure sockets layer* (SSL) technology. SSL technology encrypts data to protect the information being sent, including your credit card details.

How to check?

An unbroken key or padlock at the bottom of your web browser will indicate whether there is a secure connection, and so whether the information you send will be encrypted. To obtain information about the security used by the website, you can double-click on the unbroken key or padlock.

[30.90] Internet auctions

Internet auction sites (such as eBay) provide a mechanism for individuals to enter into transactions with each other. These are often referred to as consumer-to-consumer transactions (c2c transactions in internet parlance).

The application of consumer protection laws

Laws such as the *Competition and Consumer Act* apply to transactions in trade or commerce.

Transactions not in trade or commerce

Consumer-to-consumer transactions conducted through internet auctions will generally be regarded as private sales between individuals and consumer protection laws will not apply.

This does not mean that consumers have no rights in this situation, but they have fewer rights than if consumer protection laws applied.

Transactions that are in trade or commerce

If a person buys something through an internet auction from an individual or business that

is defined as being "in trade or commerce", consumer protection laws will apply.

However, there may be less protection than if the purchase had not been made at auction (where bidding is involved), because the implied warranties spelt out in legislation may not apply when goods are purchased at auction.

The applicable laws vary between states. For example, in Victoria, goods bought at auction are generally required to be of merchantable quality.

The organisation running the auction

The organisation providing the forum or venue to conduct an internet auction (the auction site operator) will probably be subject to consumer protection laws because they are engaging in trade or commerce (eg, by charging a fee or commission for use of the auction website).

Options when things go wrong

Contact the trader

Contact the trader (or in internet auction purchases, the seller) to try to resolve the matter, by phone, fax, post or email. Explain the problem and explain what you want (eg, a refund or return).

Keep records of all your communications with the trader. It is recommended that you write a letter so that there is a record of your complaint, which can be used if further action is taken.

For help in writing such a letter, see "Writing a complaint letter" at www.moneysmart.gov.au/tools-and-resources/how-to-complain.

Contact your payment card provider

If you purchased the goods or services with a payment card (such as credit card, debit card or stored value card), there may be protections available to you. For example, some credit cards have a charge-back facility (see Making payments at [30.90]).

Contact an industry body or professional association

Many traders are members of an industry body or association that follows a code of conduct. If the trader at issue belongs to such an organisation, it may be able to assist in resolving your dispute.

Details of Australian industry bodies and professional associations are in *The Australian Consumer Handbook* at www.accc.gov.au/consumers/online-shopping/shopping-online.

If the trader is overseas, the relevant foreign consumer protection agency might be able to tell you whether the trader belongs to an appropriate industry or organisation.

Seek help from a consumer protection agency

If the problem is not resolved, you may wish to contact the Consumer Affairs/Fair Trading agency for the state or territory where the trader is located.

If you are in a different state or territory from the trader you can also contact the Australian Competition and Consumer Commission (ACCC). The ACCC may also be able to help you if the trader is overseas.

When dealing with overseas traders, you can also visit www.econsumer.gov, a joint project of consumer protection agencies from around the world that provides information for international consumers and facilitates cross-border complaints.

Take legal action

If your dispute has not been resolved, you may wish to take your matter to the relevant court or tribunal. However, legal action can be costly and may only be worth pursuing if the dispute concerns a significant sum of money. Legal action against an overseas trader is considerably more expensive than against a local trader, and claims can be extremely difficult to prosecute.

Whether you should proceed with legal action depends on the circumstances of your case. You should obtain advice from a lawyer.

Participating in online auctions

Before making a bid

- Read the auction site's terms and conditions so as to understand the service being provided by the auction site and what to expect.
- Use any tutorial offered by the auction site to familiarise yourself with the services being offered.
- Look at how frauds and complaints are handled by the site. Some auction sites offer protection to successful bidders in the form of free insurance (there may be a fee for making a claim) up to a specified amount when things go wrong; for example, if the item purchased is not delivered. Read the insurance terms and conditions carefully.

The fine print may contain details of when your claim will not be successful (eg, if you pay by an instant money wire transfer service such as Western Union).

- Verify the seller's identity and contact details.
- Make arrangements with the seller about what to do if there is a problem.
- If you have any queries, contact the seller. If the seller's answers are unsatisfactory, do not bid.
- Check feedback comments or ratings about the seller on the website. Comments from previous purchasers will help you decide whether to go ahead.
- Find out the terms of sale, including:
  - who pays for shipping and handling;
  - whether there is insurance, what it covers, who pays for it and what it costs;
  - whether there is a return policy;
  - what payment mechanisms can be used.

Making payments

A good method when shopping online is to pay when the product has been delivered (cash on delivery).

If the seller does not agree to such an arrangement, an online payment service such as PayPal should be used because such services often offer protection in the form of free insurance (there may be a fee for making a claim) up to a specified amount when things go wrong; for example, if the item purchased is not delivered. Read the insurance terms and conditions carefully as they will generally contain details of when your claim will not be successful (eg, if you do not complete the purchase at the auction site but instead do so by email).

If you purchase an item at an online auction by credit card, you may be able to use a "charge-back" facility that many financial institutions attach to their credit cards (reversing the card charge if the seller fails to deliver the product). However, your credit card details may be misused if you provide them to a disreputable online auction seller.

Both sending a bank cheque or money order and making a direct deposit before receiving goods expose you to higher risks of fraud. If the seller will not send the product unless you make such a payment, you must be willing to take the risk.

Escrow agents

An alternative is to use an *escrow agent* (such as www.escrow.com). The agent's role is to hold the payment for the buyer until the product is received. Escrow agents are used to protect both parties from fraud and usually charge the buyer a percentage of the cost of the product for the service.

If you elect to use an escrow agent, you should familiarise yourself with the terms of the service offered and check to see whether the agent is reputable.

Insurance

Consider using insurance offered by the auction site or another organisation to protect yourself if something goes wrong.

Keep records

Always keep records, such as:

- the product description (including a photograph);
- the seller's identification;
- every bid made;
- all emails between you and the seller;
- every receipt or record provided.

Problems with internet auctions

The options discussed may be helpful with internet auction purchases, but there are particular issues with this type of transaction, as described.

Industry bodies and professional associations generally cover businesses, so may not be helpful in resolving disputes against individual sellers. Consumer protection agencies may be helpful if the seller sold something to you in trade or commerce, so it is worth contacting them.

Given the costs and time taken to resolve a dispute – along with the risks in an unsuccessful outcome – legal action is recommended only as a last resort.

The following options should also be explored.

Post-feedback about the seller on the auction website

Many auction websites have feedback services allowing you to post a comment and/or ranking about the trader from whom you made your purchase.

While this warns subsequent users about the seller, it will not provide you with any refund or exchange.

Make a claim to the auction site

Some internet auction websites offer free insurance up to a specified amount.

Check the terms and conditions of the auction site operator's insurance policy to see if you can

make a claim. You will probably need to make a claim or charge-back application with your online payment service provider (such as PayPal) or credit card company (see Making payments at [30.90]) before you can make a claim with the auction site operator.

Make a complaint against the auction website

Although you did not purchase something from the auction site operator, they might have contravened your rights as a consumer. For example, this can happen if the site operator made misrepresentations about the auction site's safety regarding fraud. The abovementioned options (such as seeking help from a consumer protection agency or taking legal action) can then also be explored in relation to the site operator.

Copyright on the internet

[30.110] When downloading material from the internet, it is important to consider who owns the copyright in the downloaded material, and whether you need to obtain the owner's consent for any actions you plan to take with the information. Copyright laws apply to material on the internet and reusing or distributing downloaded material without the consent of the copyright owner can leave a person open to a charge of copyright infringement. In certain cases, it will be necessary to pay a fee for the use of the copyright material. Educational and research institutions have limited rights to use copyright material without charge but in each case it is prudent to check with the relevant body.

Internet content regulation

[30.120] Parents and guardians are often concerned about children encountering inappropriate material on the internet.

This section outlines the ways in which internet material is regulated in Australia, what parents and guardians can do and where to find more information.

[30.125] The internet content regulation scheme

In Australia, there is a scheme for regulating content on the internet. The scheme is created by the *Broadcasting Services Act 1992* (Cth) and administered by the federal government.

The scheme aims to address community concerns about content, particularly where children might access inappropriate material. At the same time, it is guided by industry practicalities and the principle that what is restricted offline should also be restricted online.

Internet content is regulated by a public complaints procedure, laws and industry codes of practice, such as the *Internet Industry Codes of Practice – Internet and Mobile Content*.

The scheme also provides information and tools to the community so that, for instance, parents can better protect their children through managing their access to the internet.

[30.130] Making a complaint

When can a complaint be made?

The complaints process is an important part of the content regulation scheme. Anyone can complain about what they feel is objectionable content on the internet, but the specific procedure and solutions vary, depending on the nature and source of the material.

Complaints are usually made to the Australian Communications and Media Authority (ACMA).

Classification of content

Internet content is generally classified using the same categories used for classifying films and computer games (see Chapter 31, Media Law).

Refused classification

RC (refused classification) content cannot be legally hosted on an internet site in Australia, just as an RC film cannot legally be brought into the country.

Material will be refused classification where it is considered to deal with sensitive topics like sex, drug misuse, crime or violence in a way that offends the standards of reasonable members of the community, or offensively depicts a person who is or who looks as though they are under 16.

X-rated material

X-rated material (depictions of actual sexual activity) is also prohibited on the internet, as are X-rated films (except in the ACT and the Northern Territory). Content that contains depictions of actual sexual activity between consenting adults and is considered unsuitable for a minor to see but does not fall into the RC category is classified X.

R-rated material

R-rated content is material which is not RC or X but is unsuitable for a minor to see. For this material, there should be a *restricted access system* to prevent access to the content by people under 18. A *restricted access system* for R-rated material means that a person seeking access to R18+ content must apply for it in writing, orally or electronically. The access control system must issue a warning to the user seeking to view the content that it is an R18+ content and also requires an age verification and/or other safeguards. A complaint can be made where there is no *restricted access system* in relation to *R-rated material*.

Exemptions

Some films can be exempt from classification, for instance, where they might be screened in a particular film festival or were made for scientific purposes.

Other types of content may only be unlawful if children can easily gain access to it.

When a complaint is received?

ACMA must investigate any complaint it receives relating to prohibited content on the internet. As part of an investigation, ACMA may request the Classification Board to classify the content according to its guidelines for the Classification of Films and Computer Games (see Chapter 31, Media Law).

If the material is on an Australian site

If the internet content is hosted in Australia and is prohibited or likely to be prohibited, ACMA will direct the internet content host to remove the content from their service by issuing a *takedown notice*. An internet content host can be fined if it does not comply with the takedown notice despite being aware of the content.

Prohibited content is anything that is or would be classified RC or X by the Classification Board.

In serious cases (eg, child pornography), state or territory police can also become involved. Depending on the state or territory, the content provider, internet content host and internet service provider may all be prosecuted and face fines or a jail term where it can be established that such parties knew that the content was illegal.

R-rated content hosted without a restricted access system is prohibited and can result in a takedown notice being issued to the internet content host by ACMA. A restricted access system must have a registration process that permits only people over 18 to access the adult (R) content.

If the material is hosted outside Australia

The Australian co-regulatory scheme does not apply to overseas internet content hosts, though it does apply to Australian internet service providers.

When an internet service provider is issued with an *access prevention notice* by ACMA, it must comply with internet industry codes of practice or an industry standard, or take reasonable steps to block the prohibited overseas-hosted material.

The codes of practice require an internet service provider to have an approved *filter* on its system for this purpose. ACMA will forward the content details to the filter makers or suppliers so that they can update the software.

The authority also regularly notifies internet service providers about prohibited or potentially prohibited content.

In serious cases, the Australian Federal Police or the relevant overseas law enforcement agencies may become involved.

Discrimination and vilification

Some internet material does not fall under the RC, X or R classifications and procedures but is still illegal.

Material that denigrates a particular group of people may be prohibited. The Australian Human

Rights Commission assesses this type of content. For example, there has been a successful complaint about website material that was deemed to incite racial hatred.

For information on how to complain, see www.humanrights.gov.au/complaints_information.

In Victoria, the *Racial and Religious Tolerance Act 2001* (Vic) specifically covers electronic communications, including email. Complaints should be made to the Victorian Equal Opportunity and Human Rights Commission (see www.humanrightscommission.vic.gov.au).

In NSW, the *Anti-Discrimination Act 1977* (NSW) makes it illegal to communicate material that vilifies someone on the basis of their race or ethno-religious background, homosexuality, transgender status or because they are living with HIV/AIDS.

Complaints should be made to the NSW Anti-Discrimination Board (see Chapter 17, Discrimination).

How to make a complaint?

Complaints must be in writing and must include the following:

- name and contact details;
- the internet address of the content and any other details required to access it (such as a password);
- a description of the internet content;
- a description of why the content is objectionable.

An online complaint form can be filled in at www.acma.gov.au. Alternatively, you may email your complaint to online@acma.gov.au, or post or fax it to The Content Assessment Hotline Manager, Australian Communications and Media Authority, GPO Box Q500, Queen Victoria Building, NSW 1230 (fax 9334 7799).

[30.140] Codes of practice

The complaints system is only one part of the shared effort to regulate internet material. The Internet Industry Association has also developed codes of practice. While these are largely voluntary and self-regulated, ACMA can direct particular internet service providers and internet content hosts to comply with their responsibilities under the codes, or risk fines.

ACMA can also implement mandatory industry standards where there is no code, or the code is inadequate.

Compliant internet service providers are registered with ACMA and are entitled to display a "family friendly" ladybird seal.

[30.150] Education and information

Education and information are other important aspects of the co-regulatory scheme. These are mainly provided by ACMA and community bodies such as NetAlert. The idea is that both the industry and the community have responsibilities to comply with the rules and to prevent access to inappropriate content by children.

ACMA and the Internet Industry Association regard parents and teachers as being in the best position to advise children and monitor their access using available resources.

ACMA hosts *smart net surfing for kids and their grownups*, which gives tips and suggestions (see www.esafety.gov.au).

Other information and advice sites are available at:

- www.classification.gov.au (Classification Board and Classification Review Board);
- www.commsalliance.com.au (Communications Alliance, formerly Internet Industry Association);
- www.childrenandmedia.org.au (Australian Council on Children and the Media).

For more information on children and cyber safety and bullying, see Chapter 7, Children and Young People.

[30.160] Filters and labels

Internet content that is created in real time (chat rooms, live audio and video streaming) is generally not covered by the classification procedures or the industry codes (Victoria is a partial exception, with email content that vilifies on racial or religious ground being illegal). However, there are other tools to help regulate this material and assist parents and guardians in managing their children's access.

Filters are programs that in some way block access to inappropriate material from websites, newsgroups, chat rooms and email. Filters can also restrict results from search engines.

Labelling tools can help filters by creating lists of sites. *Black lists* use the names of sites with offensive content to block access to them. *White lists* block everything except inoffensive sites. *Content-based filters* block access to sites based on key offensive words or on some photographic content that might be unsuitable for children.

The different types of filter can be used in combination, depending on what is required.

Filter programs can operate on a home computer or through an internet service provider (ISP). ISPs are obliged to provide information about filtering software and the filters it offers and must also provide a filter approved in the Internet Industry Association codes of practice.

Filters and labelling tools can also be purchased from computing shops and online. The Communications Alliance site gives more information: www.commsalliance.com.au.

[30.170] Safe zones

Safe zones are networks suitable for young children and are separated from the rest of the internet. They are available via subscription or through some internet service providers. Specific children's zones may also be hosted on commercial sites or supported by advertising.

It is important to remember that no tool is completely infallible. The consumer advice websites can help parents and guardians to choose the best strategy.

[30.180] Social media

Chat rooms are places where real-time conversations take place in text mode. They are usually public, although private chat rooms are offered on some sites.

Most children (and indeed many adults) use pseudonyms so that the person's true identity is not apparent. This means that sometimes a child may believe that they are chatting to another 12-year old, when in fact they are communicating with an adult. There have been instances where adults have attempted to exploit children by contacting them in chat rooms.

The current regulatory approach emphasises education and guided information for children. It is important that children know what personal details they can give out when they are online, for their general safety and for the security of the household.

[30.190] Internet gambling

Australia also regulates internet gambling, using a process similar to the internet content regulation scheme. Access to certain forms of interactive gambling by Australia-based customers is prohibited, and it is also an offence to provide particular forms of Australia-based interactive gambling to customers in specific countries.

Problems with email

Spam

Spam is a generic term used to describe unsolicited commercial electronic messaging, generally delivered by SMS or email (electronic junk mail). Under the *Spam Act 2003* (Cth), spam can only be sent with consent, although consent can be reasonably inferred from a business relationship. Subsequent commercial messages must include an "unsubscribe" facility.

More information on spam, including making complaints about it, can be obtained from ACMA.

Phishing

Phishing is a form of identity theft where fake emails and websites, designed to look like legitimate persons, businesses, financial institutions and government agencies, are used to deceive internet users into disclosing their bank and financial account information or other personal details.

Information about phishing is available at www.scamwatch.gov.au/types-of-scams.

Discrimination and harassment

Unlawful discrimination can occur through email. An organisation that deals with an employee or other person via email in a way that treats them less favourably than someone else on the basis of their sex, race, disability, sexuality, gender status, age, pregnancy, marital status or other grounds could be actionable under workplace relations and discrimination law.

Certain other email practices, including sending offensive material or giving another person unwanted attention, may constitute discrimination or harassment under discrimination and workplace relations law.

Electronic stalking

Repeated email contact, chat room messages or posting messages to bulletin boards with the intention of causing psychological harm or arousing in the recipient a reasonable fear for their safety (or that of others) may constitute the crime of stalking, punishable by fine or imprisonment.

Privacy online

[30.230] Privacy laws differ dramatically both within Australia and between Australia and the rest of the world. Australia, Canada, New Zealand and the European Union generally have much stricter data protection laws than the United States, Asia and South America. Not all Australian states have data protection legislation, although the *Privacy Act 1988* (Cth) and the *Australian Privacy Principles 2014* do regulate the way the federal government (and its agencies) and most Australian businesses handle personal information. Similarly, the *Privacy and Personal Information Protection Act 1998* (NSW) places obligations on the way NSW public sector agencies handle personal information.

[30.240] Providing personal information online

Where you provide information online to an Australian business or government department, the organisation collecting your information will likely be bound by privacy obligations under Australian law (although this is not guaranteed). Where providing information to a business located overseas (particularly if that business is located in the United States), it should not be assumed that the information is subject to any legislative protection.

Personal information sent via email or through other electronic means should be encrypted so as to ensure that it is not inappropriately accessed, copied or corrupted by a third party in transmission. The more sensitive the information provided, the greater the need for security of the system transferring that information. Information that can lead to theft or fraud, such as credit card information or bank account details, should be more highly protected than more generic forms of information.

[30.250] Online identity theft

Personal information

Snippets of personal information which together can be used for the purposes of identity theft (such as a full name, date of birth and unique identifiers such as a Medicare number, driver's licence number or TFN) should only be sent via a secure system if being sent online. Where appropriate protection cannot be guaranteed by the organisation collecting your information (and transacting is necessary), consider providing the information via an alternative medium such as facsimile transmission or post.

Social networks

The internet is increasingly being used for purposes other than business transactions: social and business networking sites, blogs and fan sites are increasingly common. Before engaging with these applications, it is important to read the organisation's privacy policy to ascertain how the personal information you provide will be stored, used and disclosed: many of these sites will want to on-sell your personal information for direct marketing purposes and/or use it to target advertising to you.

When providing information online, consider the amount of personal information you are providing and whether you may like to engage with the site anonymously or through a pseudonym. It should be remembered that once you post information, it will be extremely difficult (if possible at all) to permanently remove that information, particularly where social networking sites and blogs are concerned. For example, if you upload a photo, it could be stored in cached pages, copied by others and/or disseminated widely before you decide to remove it. Even where the site allows you to restrict access to your personal information through passwords or by requiring you to expressly accept those seeking access to your information, glitches in the site's software or low security measures (which result in hackers gaining access) can leave your personal information exposed. In addition, changes to the site's default system for providing access or its terms of use can result in your personal information being available to more people than you originally intended or expected. For these reasons, you should be cautious when posting personal information, particularly information that you do not want the general public to have access to.

Internet crime

[30.260] Hacking into a computer system to obtain personal or commercial information is a crime. The federal *Criminal Code* criminalises the unauthorised access of computer data and the modification of such data. It is also a criminal offence to impair the proper operation of electronic communications.

Misusing telecommunications networks for a wide variety of reasons, such as to make a threat, conduct a hoax, menace, harass, engage in child abuse or upload child pornography material, is also a criminal offence.

In addition, dishonestly dealing in personal financial information without the consent of the individual concerned is a crime under the *Criminal Code*.

The states and territories also create a range of criminal offences in relation to computer misuse.

Telecommunications interception and access

[30.270] It is an offence for a person to intercept or access private internet communications without the knowledge of the parties involved. The *Telecommunications (Interception and Access) Act 1979* (Cth) allows access to communications content for law enforcement and national security purposes but private individual who intercepts communications for private purposes can face significant penalties.

Contact points

[30.280] If you have a hearing or speech impairment and/or you use a TTY, you can ring any number through the National Relay Service by phoning **133 677** (TTY users, chargeable calls) or **1800 555 677** (TTY users, to call an 1800 number) or **1300 555 727** (Speak and Listen, chargeable calls) or **1800 555 727** (Speak and Listen, to call an 1800 number). For more information, see www.communications.gov.au.

Non-English speakers can contact the Translating and Interpreting Service (TIS National) on **131 450** to use an interpreter over the telephone to ring any number. For more information or to book an interpreter online, see www.tisnational.gov.au.

Changes are expected to the websites for many NSW government departments that were not available at the time of printing. See www.service.nsw.gov.au for further details.

Arts Law Centre
www.artslaw.com.au
ph: 1800 221 457

Australasian Legal Information Institute (AustLII)
www.austlii.edu.au

Australian Communications and Media Authority (ACMA)
www.acma.gov.au
ph: 1300 850 115

Australian Competition and Consumer Commission (ACCC)
www.accc.gov.au
ph: 1300 302 502

Australian Copyright Council
www.copyright.org.au
The Legal Advice Service is available online only.

Association for Data-Driven Marketing and Advertising (ADMA)
www.adma.com.au
ph: 9277 5400

Australian Information Commissioner, Office of
www.oaic.gov.au
ph: 1300 363 992

Communications and the Arts, Department of
www.communications.gov.au
ph: 1800 254 649 or 6271 1000

Communications Alliance (including Internet Industry Association of Australia)
www.commsalliance.com.au
ph: 9959 9111

Communications and Media Law Association (CAMLA)
www.camla.org.au
ph: 4294 8059

Information and Privacy Commission NSW
www.ipc.nsw.gov.au
ph: 1800 472 679

Media, Entertainment and Arts Alliance
www.meaa.org
ph: 1300 656 513

Ombudsman, Commonwealth
www.ombudsman.gov.au
ph: 1300 362 072

Scamwatch, run by the Australian Competition and Consumer Commission (ACCC)
www.scamwatch.gov.au

Stay Smart Online, hosted by the Australian Government
www.staysmartonline.gov.au
ph: 1300 292 371

Telecommunications Industry Ombudsman (TIO)
www.tio.com.au
ph: 1800 062 058