Privacy and Information Rights

Edited by Justin Healey

Volume | 341

The Spinney Press

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
# Contents

## CHAPTER 1  PRIVACY REGULATION AND RIGHTS

- What’s ‘privacy’? 1
- What is privacy? 5
- Don’t leave privacy to chance … 6
- Government moves on privacy law 8
- A right to privacy in Australia 8
- Is there a need for a statutory cause of action for serious invasion of privacy in Australia? 9
- When should privacy be legally protected? 12
- Legisllate the right to privacy 14
- The great privacy debate 16
- Little evidence Australia needs a new privacy law 17

## CHAPTER 2  COMMUNICATIONS PRIVACY

- Protect your identity and privacy 19
- How do I deal with … 20
- Are there any privacy risks associated with using social networking sites? 23
- Safe social networking 24
- Mobilise your phone privacy – top tips 26
- Photos and surveillance 28
- Being watched constantly is too high a price for safety 29
- Protecting privacy while responding to terrorism 30
- Digital fingerprints the next privacy invasion? 33
- Communications privacy complaints: in search of the right path 35

## CHAPTER 3  PRIVACY AND THE MEDIA

- Privacy in the age of no privacy 37
- What happens when you extend the idea of public interest to privacy? 39
- How the media will react to a right to privacy 40
- Phone hacking scandal proves we need more laws to protect privacy 41
- Privacy eye: media paranoia distorting facts on privacy tort 42
- How do we protect privacy in the digital age? 44
- Breaches of privacy by large corporations the real problem 45
- Privacy in the information age free for all 46
- Far from sinister, privacy laws might mean media does its job better 48

- Exploring issues – worksheets and activities 49
- Fast facts 57
- Glossary 58
- Web links 59
- Index 60
**Introduction**

*Privacy and Information Rights* is Volume 341 in the ‘Issues in Society’ series of educational resource books. The aim of this series is to offer current, diverse information about important issues in our world, from an Australian perspective.

**KEY ISSUES IN THIS TOPIC**

We live in a public age in which the free flow of personal information is increasingly exposed to serious invasions of privacy. Privacy protection is a growing concern in relation to how people use rapidly advancing technology to store and share their personal information with family, friends, organisations and governments. Many Australians’ daily interactions are conveyed by social networking websites and mobile phones, and can involve sharing personal and financial data online, often under the watchful eye of CCTV surveillance – but are our privacy laws and protections keeping pace with technological change?

Although people are able to complain about the misuse of their personal information to a national information commissioner, Australian laws do not clearly allow a person to take action against a person or entity that seriously violates their privacy. In light of the British media’s recent phone hacking scandal, should people’s right to privacy be at the expense of freedom of expression and the freedom of the media to seek out and disseminate information of public interest? Can a balance between these principles be struck? Is anything really private anymore?

This book consists of three chapters: Privacy regulation and rights; Communications privacy; Privacy and the media.

**SOURCES OF INFORMATION**

Titles in the ‘Issues in Society’ series are individual resource books which provide an overview on a specific subject comprised of facts and opinions.

The information in this resource book is not from any single author, publication or organisation. The unique value of the ‘Issues in Society’ series lies in its diversity of content and perspectives.

The content comes from a wide variety of sources and includes:

- Newspaper reports and opinion pieces
- Website fact sheets
- Magazine and journal articles
- Statistics and surveys
- Government reports
- Literature from special interest groups

**CRITICAL EVALUATION**

As the information reproduced in this book is from a number of different sources, readers should always be aware of the origin of the text and whether or not the source is likely to be expressing a particular bias or agenda.

It is hoped that, as you read about the many aspects of the issues explored in this book, you will critically evaluate the information presented. In some cases, it is important that you decide whether you are being presented with facts or opinions. Does the writer give a biased or an unbiased report? If an opinion is being expressed, do you agree with the writer?

**EXPLORING ISSUES**

The ‘Exploring issues’ section at the back of this book features a range of ready-to-use worksheets relating to the articles and issues raised in this book. The activities and exercises in these worksheets are suitable for use by students at middle secondary school level and beyond.

**FURTHER RESEARCH**

This title offers a useful starting point for those who need convenient access to information about the issues involved. However, it is only a starting point. The ‘Web links’ section at the back of this book contains a list of useful websites which you can access for more reading on the topic.
WHAT’S ‘PRIVACY’?

The following explanation was prepared for an Australian Law Reform Commission workshop by Roger Clarke from the Australian Privacy Foundation

INTRODUCTION

Privacy is important, from a number of different perspectives. Philosophically, particularly in Europe, people are regarded as being very important for their own sake. The concepts of ‘human dignity’ and integrity play a significant role in some countries, as do the notions of individual autonomy and self-determination. In some (though perhaps not all) traditions and jurisdictions, these are the ideas that underpin the notion and significance of human rights.

Psychologically, people need private space. This applies in public as well as behind closed doors and drawn curtains. We need to be able to glance around, judge whether the people in the vicinity are a threat, and then perform actions that are potentially embarrassing, such as breaking wind, and jumping for joy.

Sociologically, people need to be free to behave, and to associate with others, subject to broad social mores, but without the continual threat of being observed. Otherwise we reduce ourselves to the appalling, inhuman, constrained context that was imposed on people in countries behind the Iron Curtain and the Bamboo Curtain.

Economically, people need to be free to innovate. International competition is fierce, and countries with high labour costs need to be clever if they want to sustain their standard of living. And cleverness has to be continually reinvented. But the chilling effect that surveillance brings with it stifles innovation. All innovators are, by definition, ‘deviant’ from the norms of the time, and they are both at risk, and perceive themselves to be at risk, if they lack private space in which to experiment.

Politically, people need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and undermines democracy.

In Australia, the pragmatic or utilitarian approach tends to dominate the philosophical. Of the four bases on which it can be argued that privacy is needed, the most dominant in discussions tends to be the psychological perspective. It is a serious mistake, however, to limit the justification in that way. Privacy invasions are seriously harmful to the societies, economies and polities in which humans have flourished. Balances must be sought, and privacy protections must be devised, with that in mind. In turn, it is essential that a sufficiently broad conception of privacy be used.

PRIVACY AS A HUMAN RIGHT

Privacy’s importance is reflected in the fact that the fundamental documents that define human rights all include reference to privacy or related ideas. For a list of such documents, see APF (2006), and see Bygrave (1998).

For example, the Universal Declaration of Human Rights (UDHR 1948, Article 12) states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”, and Article 17 of the International Covenant on Civil and Political Rights (ICCPR 1966, Article 17) is expressed in very similar terms.

In the European Convention on Human Rights (1950), Article 8 is entitled ‘Right to respect for private and family life’, and states that “Everyone has the right to respect for his private and family life, his home and his correspondence. 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 wellbeing 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”. Unlike the previous two, this Article enumerates categories of factors that can result in compromise to the right, and it has generated case law.

The Charter of Fundamental Rights of the European Union (2000) deals with privacy in Articles 7 and 8, and there are many specific European Directives. Many national Constitutions and Bills of Rights also encompass privacy.

But these documents evidence a considerable degree of inconsistency. The instruments generally do not define the term ‘privacy’, and its scope interleaves with a range of other freedoms and rights. These Notes endeavour to tease out the range of possible meanings, and propose the interpretation most appropriate to contemporary needs.
SOCIAL NEEDS

It would be a mistake to commence a search for the meaning of the term in the law. The law reflects social and economic needs, and hence they are the appropriate starting point. Reference then needs to be made to the emergence of the legal concept of privacy from the late 19th century onwards. The discussion needs to take into account the fact that a considerable amount of change that has occurred, and continues. On that basis can a useful contemporary interpretation of the term be proposed.

A framework is provided by Maslow’s Hierarchy of Needs (Maslow 1943). This postulates that people’s more basic needs have to be largely satisfied before higher-order needs come into play. Moreover, if a lower-order need is threatened, the significance of higher-order needs is suspended until the lower-order needs are once again satisfied.

The usual classification scheme is presented as a pyramid:

➤➤ Self-actualisation
➤➤ Status (or Self-esteem)
➤➤ Love or Belonging
➤➤ Safety
➤➤ Physiological or Biological Needs.

Physiological needs are matters of survival (such as air, water, food, warmth and rest). Safety encompasses basic considerations such as physical security, family security and health, but also broader concerns such as security of personal assets and employment.

THE COMPREHENSIVE INTERPRETATION OF PRIVACY

Interpreted most broadly, privacy is about the integrity of the individual. It therefore encompasses all aspects of the individual’s social needs. Applying Maslowian thinking the following categories can be valuably distinguished.

Privacy of the Person, sometimes referred to as ‘bodily privacy’, is concerned with the integrity of the individual’s body, and is related to the Physiological and Safety levels of the Maslowian hierarchy. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include compulsory immunisation, imposed treatments such as lobotomy and sterilisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.

Privacy of Personal Behaviour, including what is sometimes referred to as ‘media privacy’, is related to both the Belonging and Self-esteem levels of Maslow’s hierarchy, and perhaps to Self-actualisation as well. Many issues that come to attention relate to sensitive matters, such as sexual preferences and habits, political activities and religious practices. But the notion of ‘private space’ is vital to all aspects of behaviour, is relevant in ‘private places’ such as the home and toilet cubicle, and is also relevant in ‘public places’, where casual observation by the few people in the vicinity is very different from systematic observation and the recording of images and sounds.

Privacy of Personal Communications, including what is sometimes referred to as ‘interception privacy’, is also related to both the Belonging and Self-esteem levels of Maslow’s hierarchy, and perhaps to Self-actualisation as well. Individuals desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. Issues include mail ‘covers’, use of directional microphones and ‘bugs’ with or without recording apparatus, telephonic interception and recording, and third-party access to email messages.

Privacy of Personal Data, sometimes referred to as ‘data privacy’ and ‘information privacy’, is again related to the upper layers of Maslow’s hierarchy. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. The last five decades have seen the application of information technologies to a vast array of abuses of data privacy (e.g. Clarke 1988, 2003).

TERMINOLOGICAL AMBIGUITIES

The term privacy is sometimes used in the broad sense outlined in the previous section. But it is often used to refer to some quite specific need or expectation that is in the public eye at the time, such as freedom from the attention of paparazzi, protections against voyeurism in such old forms as ‘peeping toms’ and such new forms as mobile cameras in change rooms, or the conduct of interviews in closed rooms rather than semi-open cubicles. One of the most common narrow usages of privacy is to refer solely to what is described in the previous section as ‘privacy of personal data’, or sometimes the combination of that with ‘privacy of personal communications’.

A serious debasement of the term ‘privacy’ has occurred in the case of US and Australian statutes that have equated it with the highly restrictive idea of ‘data protection’. That notion derives from the ‘fair information practices’ movement that has been used by corporations and governments since the late 1960s to avoid meaningful regulation. The origins of that movement are commonly associated with Westin (1967, 1971) and Westin & Baker (1974). The paucity of the concept is addressed in Clarke (2000).

EMERGENCE OF THE LEGAL CONCEPT

This section presents a brisk survey, from a layman’s perspective, and is intended as a complement to comprehensive studies by legal academics, not as a substitute for them.

It is conventional to observe that privacy was not a significant feature of tribal or even village life. It became a
more significant human value during the period following the *rinascimento*, as attitudes in Western Europe began to place greater value on individualism, and as human rights discussions expanded in such contexts as the abolition of slavery and improvements to the conditions of workers in ‘dark satanic mills’.

The concept maps poorly to social philosophies in regions not dominated by the Western European tradition. This applies in particular to East Asia, where confucianist notions are commonly used to interpret subjugation of the individual to the State or collective as a higher value than individualism.

At the end of the 19th century, United States judges argued that “the right to be let alone ... secures the exercise of extensive civil privileges” (Warren & Brandeis 1890). The expression ‘the right to be let alone’ is consistent with the broadest interpretation discussed earlier in these Notes. On the other hand, the authors were preoccupied with incursions by the media into the lives of the influential, and an argument can be made that the term’s compass is narrower than it sounds.

A significant early contribution was Packard (1964). Important sources of learned discussions about the need for privacy can be found in a series of UK studies (Younger 1972, Sieghart 1976, Lindop 1978). These envisaged the emergence or creation of broad tort notions of privacy, but they appear to have had only limited influence on action in the legislatures and the courts. Although those ideas are not convincingly alive, they are perhaps less dead than dormant. The possibility exists that a tort is emergent in the UK, at least in the context of media privacy for celebrities and notorieties, and even in Australia.


In Australia, the earliest publication of significance appears to have been Cowen (1969). A vital contribution was that of Morison (1973), which expressly avoided expression of privacy as a ‘right’, and focussed on it as an ‘interest’ that people have, that is in need of protection, but that needs to be carefully balanced against other interests, variously of the individual themselves, of other individuals, of groups, of society, and of organisations. Others of significance include Benn (1978), Hughes (1991), Bygrave (2002) and Lindsay (2005).

**DEBASEMENT OF THE LEGAL CONCEPT**

Since the late 1960s, however, the dominance of the ‘fair information practices’ movement has resulted in very narrow usage of the term. In almost all jurisdictions, statutory activity has been restricted to ‘privacy of personal data’ and ‘privacy of personal communications’. Some statutes have been appropriately described as ‘data protection laws’, while others have been inappropriately entitled ‘privacy laws’.

The reasons for this diminution in the scope applied to the idea arose because one aspect of privacy achieved dominance over the others. Contrary to conventional assumptions, the primary driver was not information technology.

Since the late 19th century, there has been a marked increase in the scale of organisations. This has led to increased (and still increasing) social distance between individuals and the social and economic institutions that they deal with. As that distance grows, so does distrust, and dependence on abstract data rather than direct relationships. The term coined by Jim Rule to refer to this was ‘information intensity’ (Rule 1974, Rule et al. 1980). It needs to be remembered that Orwell’s 1984 was written in 1948, some years before a computer was first used for administrative purposes; and the foundation novel of the surveillance dystopia genre, Zamyatin’s *We*, was written in 1922, and long predates the construction of the first computer (Clarke 1993).

Subsequently, however, computers emerged, networking technologies were married with them, and they were harnessed to the task of assisting governments and corporations to monitor people (Clarke 1988). Concerns about ‘information intensity’ exploded, and for several decades discussions about privacy protection have been largely focussed on (limited) protections for data, instead of the protection of people’s interests.

The first such statute was enacted in Hesse in 1970, and the first national legislation in Sweden in 1973. Through what Michael Kirby dubbed ‘the decade of privacy’ of the 1970s, many European nations acted. Nervousness among corporations about inconsistencies and trans-border provisions harming trade in personal data resulted in the codification of ‘fair information principles’ (OECD 1980). This has provided the framework for all subsequent laws.

Australia was slow to comply with its undertaking to implement the OECD Guidelines. A study by the Australian Law Reform Commission took over 5 years (ALRC 1983), and by the time it was published the political momentum had
been entirely lost. Data protection legislation regulating the Commonwealth public sector was passed in 1988, but only in the aftermath of the Australia Card debacle, and as a trade-off for enhancements to the Tax File Number scheme. The States and Territories moved even more slowly, although half of the States and both Territories now have ‘fair information practices’ legislation for their public sectors. Highly confusing and extremely weak private sector legislation was passed by the Commonwealth in 2000. For a list of relevant Australian laws, see APF (2005a) and APF (2005b).

Europe has evidenced two contrary tendencies in data protection. On the one hand, the EU Directive is strongly driven from the human rights perspective, and has resulted in more effective protections for data (and hence to some extent better protections for people) than anywhere else in the world. On the other, some of the most extremist social control schemes have been implemented in European countries, such as Denmark and Finland, and the EU Directive accommodates them, because any privacy-abusive arrangement is feasible, provided that it has legal authority.

The US has stood out from Europe. Burkert (1999) characterised the difference as being that the US has an ‘economic-technological approach’, whereas Europe is ‘social values oriented’ (or, in the terms used in the Introduction, the US is pragmatic whereas Europe places greater weight on the philosophical).

The US has to date avoided passing comprehensive laws regulating the private sector, even of the weak ‘data protection’ kind. The vacuum has resulted in frequent, knee-jerk legislation on specific issues (most famously, for video rental records). Despite the long delay caused by the extraordinary dominance of the social control agenda since 11 September 2001, it appears likely that some kind of legislation may emerge shortly (Clarke 1999, Economist 2005, Clinton 2006).

Reflecting its desire to facilitate business at the expense of individuals, the US Administration has recently utilised APEC, with its dominance of East Asian nations and its willing proxy Australia, as a means of establishing an even weaker document than the OECD Guidelines, in the form of the APEC Privacy Framework (2004).

CONCLUSIONS

The world’s ‘data protection’ and ‘privacy’ laws have been very largely motivated by the facilitation of the business of government and private enterprise. Most were not conceived as implementations of human rights needs, although many countries have contrived ways of reconciling the two in order to make it appear that they are fulfilling their obligations under ICCPR.

The social need is for the broader interpretations of privacy to again become dominant, and for the harm wrought to individuals by decades of dominance of the ‘fair information practices’ movement to be reversed.

The following is the working definition that I’ve used since the early 1990s (Clarke 1997). It owes much to Morison (1973):

Privacy is the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations.

REFERENCES


AUTHOR AFFILIATIONS
Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law and Policy Centre at the University of NSW, a Visiting Professor in the E-Commerce Programme at the University of Hong Kong, and a Visiting Professor in the Department of Computer Science at the Australian National University.

The word ‘privacy’ means different things to different people. Your idea of privacy is likely to be different from the ideas of your family and friends.

### Types of privacy

The type of privacy covered by the *Privacy Act* and the Office of the Australian Information Commissioner is the protection of people’s personal information (see below). See *Privacy Act snapshot* for further information. However, this is just one aspect of privacy. Other types of privacy can include territorial privacy and physical or bodily privacy and privacy of your communications.

This Office generally handles privacy issues which involve a person’s personal information. This can include privacy issues associated with information about your location, your health and body and your communications with others.

### What is personal information?

Personal information is information that identifies you or could identify you. There are some obvious examples of personal information, such as your name or address. Personal information can also include medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work – basically, any information where you are reasonably identifiable.

Information does not have to include your name to be personal information. For example, in some cases, your date of birth and postcode may be enough to identify you.

To be precise, the *Privacy Act* definition of personal information is:

‘... 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.’

### What privacy is not

The protection of your personal information privacy is different to other related concepts such as:

- Confidentiality
- Secrecy
- Freedom of information.

However, there can be some crossover. If you are in doubt, please visit [www.oaic.gov.au/about/contact.html](http://www.oaic.gov.au/about/contact.html)

© Commonwealth of Australia,
Source: [www.privacy.gov.au](http://www.privacy.gov.au)
This document is designed to help you protect your personal information. It provides a broad overview of some of your rights and the obligations of organisations and Australian and ACT Government agencies set out in the Privacy Act 1988 (Cth). The information contained in this document is not comprehensive. If you have any queries about anything in this document, or any privacy related issue, please visit our website at www.privacy.gov.au or call our Enquiries Line on 1300 363 992.

1. Read privacy policies
   Many organisations and each Australian and ACT Government agency have publicly available information on how they handle your personal information. This information sets out the privacy practices and obligations of the organisation or agency you are dealing with. The information may be in a written document or you may be told in person or over the phone. This information generally sets out the law that the organisation is bound by, any exemptions that may apply and details for obtaining further information about the way the organisation manages the personal information it holds. For information about personal information held by Australian and ACT Government agencies, please view the Personal Information Digest page available on our website at www.privacy.gov.au/government/digest.

2. Ask why the information is required, what they will do with it and who will it be disclosed to
   There may be times when your information is requested but does not need to be collected. For example, very few businesses need information about your medical history. So, if you think the information being asked for by an organisation or agency is not required, consider asking why the information has been requested. Knowing why will allow you to remain informed about how your personal information is being used, and if it will be disclosed, who it will be disclosed to.

3. Only give out as much personal information as you need to
   There are many cases when you may not need to provide your personal information. For example, you may not need to disclose your marital status to a retail outlet. If you don’t think you need to, consider whether you should hand the information over, ask more questions about why the information is required or seek advice from our Office about what else you can do.

4. Request access to your personal information
   You have a general right to be granted access to the personal information that organisations and agencies hold about you. There are some exceptions provided under the
Privacy Act to deny access, but you should be told what the exception is and why the organisation or agency is relying on it. Knowing what personal information an organisation or agency holds about you is a good way of checking that the information that they hold is accurate and up to date.

5. Make sure the information an organisation or agency holds about you is accurate and up to date

When your personal information changes, it’s a good idea to inform organisations and agencies that hold your personal information of these changes particularly when you have an ongoing relationship with them. Organisations and Australian and ACT Government agencies are required to take steps to amend their records to reflect the changes to your personal information. They must do this so that the records they retain are accurate, complete and up to date. A good idea is to make a written request for your record to be amended and request confirmation in writing that the amendment has taken place.

6. Take steps to protect online privacy

Protecting your privacy online will ensure that you are not leaving your personal information open to abuse. Good computer security includes installing reputable anti-spyware, anti-virus scanners and firewalls software and ensuring they are all up to date. Also, make sure you are visiting secure websites when handing over personal information including banking and credit card details. For further information, visit our website at www.privacy.gov.au/topics/technologies/security

You should be mindful of the many email scams that are around. The Australian Competition and Consumer Commission has useful information on how to protect yourself against scams. For further information, please visit their website at www.accc.gov.au. State and Territory Departments of Fair Trading may also maintain lists of current scams.

7. Take steps to ensure your hard copy records are properly destroyed

Don’t leave your personal information lying around. Make sure you properly destroy personal information you don’t want others to see when throwing it out. This may involve properly shredding documents or physically destroying expired banking and government issued cards. This is also a good way to protect yourself against potential identity theft. For further information, please see the following document, ID Theft Booklet – Protecting your identity, at www.ag.gov.au/crimepreventionandenforcement/pages/identitysecurity

8. You may wish to ‘opt out’ of further contact with an organisation when completing forms unless you know you want to be in further contact with them

Opting out of further contact will ensure you do not receive unwanted direct marketing, such as promotions and spam emails, from the organisation or any of its subsidiaries. For further information about spam emails, please see the document SpamMATTERS on the Australian Communications and Media Authority website at www.acma.gov.au

9. Know your privacy rights

The more you know about your rights, the easier it will be for you to safeguard your privacy. For more information about your privacy rights, and the obligations that organisations and agencies have to protect your privacy, visit our website at www.privacy.gov.au or call our Enquiries Line on 1300 363 992.

10. Exercise your privacy rights

If you believe that your personal information has been mishandled, you should first raise the matter with the organisation or agency in question and give them 30 days to adequately deal with your complaint. If you receive no response or are not satisfied with the response provided, you can then lodge a complaint with the Office of the Privacy Commissioner, which may be able to investigate the matter. For further information visit our website at www.privacy.gov.au or call our Enquiries Line on 1300 363 992.

© Commonwealth of Australia, Office of the Australian Information Commissioner | www.oaic.gov.au
Source: www.privacy.gov.au
**GOVERNMENT MOVES ON PRIVACY LAW**

_The Federal Government has moved to introduce a legal right to privacy in the wake of Britain’s ‘News of the World’ phone-hacking scandal. ABC News reports_

A discussion paper will be released to the public today to canvass the prospect of a law dealing with serious invasions of privacy.

Home Affairs Minister Brendan O’Connor says privacy is a growing concern in Australia, partly because of the events in Britain, as well as other breaches such as the theft of the Sony PlayStation users’ personal details.

“Right now there is no general right to privacy in Australia, and that means there’s no certainty for anyone wanting to sue for an invasion of their privacy,” Mr O’Connor said.

“The News of the World scandal and other recent mass breaches of privacy, both at home and abroad, have put the spotlight on whether there should be such a right.”

He says the Government will eventually decide if it should legislate on the issue. In 2008 the Australian Law Reform Commission made 295 recommendations, including that Australia bring in a privacy law.

“It’s a timely debate to be had, we did always look to attend to those recommendations,” Mr O’Connor said.

He says a media organisation should have to ensure that any breach of a person’s privacy was in the public interest.

“I don’t mean the public has an interest in it for titillation purposes, for example there’s certain gossip which might be disclosed,” he said.

“I’m talking about whether in fact it’s in the public interest for the freedom of expression to prevail over that other value, which is of course the right to privacy.”

But Australia’s Privacy Commissioner Timothy Pilgram says the laws need to be changed.

“They have been the subject of two years of consideration by the Law Reform Commission, so I think these issues aren’t new to us all as a community,” he said.

“We’re now looking at mechanisms to recognise the changing environment we’re in and to consider updating the laws to meet the challenges.”

Mr Pilgram says freedom of the press is an integral part of our society.

“It’s welcoming that the Government will be putting out an issues paper so we can get all interested parties to comment on it, including the media, to make sure that as we go down this path we make sure we don’t erode the freedom of the press,” he said.

“At the end of the day it’s integral to our free democratic society to have a very vibrant media.”

Opposition communications spokesman Malcolm Turnbull says with new media there are privacy issues that aren’t new to us all as a community, “We’re now looking at mechanisms to recognise the changing environment we’re in and to consider updating the laws to meet the challenges.”

Mr Pilgram says freedom of the press is an integral part of our society.

“It’s welcoming that the Government will be putting out an issues paper so we can get all interested parties to comment on it, including the media, to make sure that as we go down this path we make sure we don’t erode the freedom of the press,” he said.

“At the end of the day it’s integral to our free democratic society to have a very vibrant media.”

Opposition communications spokesman Malcolm Turnbull says with new media there are privacy issues that need to be addressed, such as cyberbullying and stalking.

But he says any discussion about legislation should not just echo the _News of the World_ inquiries.

“If we’re going to look at privacy we should look right across all media and have an honest debate about how much privacy,” he said.

“What do we believe we are entitled to and to what extent should that limit the right of the media to free speech.”

The UK hacking scandal has forced the resignations of senior executives at News Corporation and two of Britain’s top policemen, as well as fuelling opposition attacks on prime minister David Cameron’s judgment.

It has torn through News Corp chief Rupert Murdoch’s empire, causing it to axe the 168-year-old tabloid _News of the World_ and leading to the resignation of two of his top aides, Rebekah Brooks and Les Hinton. Mr Murdoch appeared before a parliamentary committee on Tuesday night, where he expressed his “humble” regrets but did not take personal responsibility for the crisis.
Is there a need for a statutory cause of action for serious invasion of privacy in Australia?

This section from an issues paper produced by the Australian Government invites comment on whether a statutory cause of action for serious breach of privacy should be introduced in Australia. It discusses the considerations the law reform commissions thought relevant to the question of whether such a reform was desirable. It then turns to whether evolution of the common law or new legislation provides the most appropriate vehicle for development of the law in this area.

The ALRC was the first Australian law reform commission to consider whether or not there was a need for a cause of action for serious invasion of privacy. It considered this question in light of the recommended broader reforms to privacy law and practice. Following an extensive community consultation exercise, the ALRC recommended that the Government legislate for a right to sue, stating that there was ‘strong support for the enactment of a statutory cause of action for a serious invasion of privacy’ in Australia. The NSWLR and VLRC came to the same conclusions (though the latter recommended two causes of action – for misuse of information and interference in seclusion).

This paper now turns to discuss some of the arguments in favour of and against a statutory cause of action.

Existing protections: comprehensiveness and adequacy

Some stakeholders have argued that existing laws and industry codes of conduct adequately protect privacy in Australia. However, the ‘gap-filling’ role of a statutory cause of action for the most serious privacy invasions has also been widely acknowledged.

The Commonwealth Privacy Act has as its focus information privacy and data protection, rather than privacy protection more broadly. That Act, and some State and Territory privacy legislation, also make only certain types of remedies available, or those remedies are available only against particular entities or types of entities, or only after particular procedural steps have been followed (e.g. after notification to the entity or to the Information Commissioner).

The tort of trespass, and statutory actions for defamation, have their own rules, requirements and exclusions. These limit the scope and application of these bodies of law where particular privacy invasions have occurred. To take one example referred to by the ALRC, the equitable action for breach of confidence is:

Presently confined to cases involving the use of information of a private nature, whether in word or pictorial form. So, however strong and understandable may be the feeling of harassment of a person who is hounded by photographers when carrying out activities of a private nature, and however unacceptable the behaviour of the pack, there will be no cause of action until an intrusive photograph is published.

The VLRC pointed to a different kind of gap in its report:

There is a clear gap in the current regulatory regime. Although the criminal law deals with the most offensive
invasions of privacy, there is no parallel civil cause of action for people harmed by that behaviour ... The Victorian Privacy Commissioner informed the [VLRC] that people contact her office with complaints about interferences with spatial privacy or misuse of private information for which there is no redress under Victorian and Commonwealth law. 83

The Commonwealth Office of the Privacy Commissioner, in its 2007 submission to the ALRC consultation process, stated that:

A dedicated privacy based cause of action could serve to complement the already existing legislative based protections afforded to individuals and address some gaps that exist both in the common law and legislation.84

Other legal remedies or mechanisms may provide more appropriate method to protect privacy or influence behaviour than a civil mechanism such as the proposed cause of action. For example, criminal laws (and sanctions such as imprisonment), or data protection laws (and sanctions such as monetary fines), may be more appropriate to deter particular types of conduct than a civil cause of action.

Prevention
Proponents of a statutory cause of action argue that a new civil cause of action may be useful in preventing privacy breaches in first place, with Professor John Burrows stating that the possibility of civil action: ‘can create a climate of restraint which ensures that serious breaches do not happen in the first place’.85

If real and severe consequences flow from seriously breaching a person’s privacy, individuals and organisations may be more inclined to think twice before acting in a manner that would cause a breach in the first place.

Such a statutory cause of action may also help to establish social norms as to what is acceptable and unacceptable behaviour, particularly in relation to the use of new technologies.

Human rights
Australia is a party to the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR accords everyone the right to protection against arbitrary or unlawful interference with their privacy, family, home or correspondence. What is arbitrary will be determined by the circumstances of each particular case. In order for an interference with the right to privacy not to be ‘arbitrary’, the interference must be consistent with the ICCPR and reasonable in the particular circumstances. Reasonableness, in this context, incorporates notions of proportionality, appropriateness and necessity.

A statutory cause of action of action to protect against serious invasions of privacy, if established, would provide an additional remedy for breaches of privacy and would be a practical additional mechanism for the protection and promotion of privacy in Australia as set out in Article 17 of the ICCPR.86

The Office of the Commonwealth Privacy Commissioner has indicated that a statutory cause of action would ‘clearly establish that privacy is an important human right that warrants specific recognition and protection within the Australian community’.87

Uncertainty
One argument against the introduction of a statutory cause of action for serious invasions of privacy includes the difficulty of defining privacy with sufficient precision to create a legal wrong.88 The ALRC sought to remedy part of this problem by suggesting the inclusion of a list of types of invasion that would fall within the cause of action.89 To the extent that such imprecision is unavoidable, it could cause confusion as to the state of the law and deter conduct or activities that were entirely legal.

Uncertainty is also an issue that arises in the context of the development of common law causes of action for invasion of privacy. Courts can only make decisions in response to the specific factual circumstances before them in a particular case.

Economic effects and interference in commercial activity
Arguments against a statutory cause of action also opine that it will have an impact on the commercial activities of Australian business.

Marketers and door-to-door salespersons made submissions to the ALRC that a cause of action would chill marketing campaigns, telemarketing and door-to-door sales. They also argue that certain economic or commercial activities, such as recovering debts and enforcing security rights, may also necessitate use of private information and ‘direct interaction with home and family’90, and the introduction of a statutory cause of action would hamper those activities.

Other concerns have been raised in
relation to the economic impact that enactment of a cause of action would have on those who may be subject to it. For example, an entity may reduce levels of certain types of economic activity in light of the potential for an award of damages against such an entity if such activity continues. If cases were to be commenced against such entities, the cost of litigation may also tend to divert resources from other economic activities or investment.

Law enforcement and national security

The public interest in effective law enforcement and the maintenance of national security is an important factor to consider in developing a cause of action. It is essential that certain agencies can continue to appropriately exercise legitimate law enforcement, national security and related functions. Police, corrective services officers, intelligence agencies and similar entities have functions, powers and duties conferred on them by legislation for the purposes of enforcing the law and maintaining national security (including through international cooperation).

Account must be taken of these functions, duties and responsibilities in crafting any cause of action. This paper returns to this matter in the discussion of defences and exceptions at Page 42.

Freedom of expression, artistic freedom, and freedom of the press

An action for invasion of privacy is seen by some as posing a threat to free expression, artistic freedom, and freedom of the press.

The NSWLRC summarised the position as follows:

A particular argument in support of this position is that, unlike the situation that tends to apply in human rights instruments where protection is afforded both to privacy and to freedom of expression, the provision of a statutory base for the protection of privacy alone would unfairly tilt the balance in favour of the interest in privacy at the expense of the interest in freedom of expression, which would not itself be protected by statute. The result would be that the individual interest in privacy would acquire a strength that would impede the free flow of information to the public on matters of public concern.91

The ALRC refers to a variety of submissions on this point92 and discusses the international instruments and Australian law protecting freedom of expression in various forms.93

Freedom of expression is also a right recognised under the ICCPR and would need to be taken into account in developing the cause of action.94 Under the ICCPR, freedom of expression can be limited by law where necessary for the respect of the rights (such as privacy rights) or reputations of others, amongst other reasons.95

Concerns that a cause of action would impede artistic expression, particularly artistic expression based on representations of what is occurring ‘in public’, were described in the ALRC’s report.96 Street artists and photographers, for example, may have concern that a cause of action which was cast in wide terms, or which did not include sufficient defences, may impose upon them unfair liabilities or expose them to costly legal action, each of which might tend to deter them from creating the art which they would otherwise produce.

The interaction between any proposed cause of action and laws protecting journalists from being required to disclose their sources – new rules of evidence often called ‘journalist shield laws’97 – is also an important matter that arises for consideration. While a privacy cause of action would not seek to alter the journalist shield protection, it may create additional causes of action to which this rule of evidence may have application.

The ALRC, NSWLRC and VLRC concluded that while there are significant benefits accruing to individuals and the Australian community at large from the introduction of such a cause of action, an important part of any such reform would be the balancing of the various public interests that the law should protect. This includes the interests in freedom of expression, in freedom of the press and in the free flow of information.98

ENDNOTES

76. A cause of action may be understood as a legal right to sue another party to obtain particular ‘remedies’, such as damages or court declarations, in respect of an enforceable claim against that other party.

77. See ALRC Report at 2564 passim.

78. Which included, for example, some 250 meetings and the receipt of 585 submissions: see further NSWLRC Report at 7-8.

79. ALRC Report at 2557.

80. See NSWLRC Report at 8-10. See further NSWLRC Report at 7-22 and VLRC Report at 143-146.

81. See VLRC Report at 147.


83. VLRC Report at 147.

84. Office of the Privacy Commissioner, Submission PR 499 [to the ALRC privacy review], 20 December 2007; cited in ALRC Report at 2557.


86. In relation to remedies, a topic to which this paper returns at page 45 below, Article 17 of the ICCPR may be read in conjunction with Article 23(1) of the ICCPR, which provides that: Each State Party to the present Covenant undertakes: a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; c) To ensure that the competent authorities shall enforce such remedies when granted.

87. Office of the Privacy Commissioner, Submission PR 499 [to the ALRC privacy review], 20 December 2007; cited in ALRC Report at 2557.

88. NSWLRC Report at 9-10 (citations omitted).

89. See below at page 41.

90. ALRC Report at 2561.

91. ALRC Report at 9-10 (citations omitted).

92. ALRC Report at 2558-2560.

93. ALRC Report at 2573-2575.

94. The ALRC briefly considered Article 19 of the ICCPR at page 2573 of its report.

95. See further Article 19 of the ICCPR.

96. See ALRC Report at 2559.

97. See, e.g., Evidence Amendment (Journalists’ Privilege) Act 2010 (Cth) and Part 3.10, Division 1A of the Evidence Act 1995 (Cth).

98. The various public interests are considered further below at pages 34-37.

Extract from Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy, © Commonwealth of Australia, September 2011, Department of the Prime Minister and Cabinet

Source: Licensed from the Commonwealth of Australia under a Creative Commons Attribution 3.0 Australia Licence. The Commonwealth of Australia does not necessarily endorse the content of this publication.

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
When should privacy be legally protected?

Megan Richardson favours incrementally-developing common law over a statutory cause of action, when it comes to privacy protection.

There’s been a lot of talk in recent weeks about the need for a statutory privacy tort. This comes in the wake of the Murdoch press’s phone hacking scandal. Even before then there were the reports of the challenges that social media sites such as Facebook and Twitter and their millions of users offer to the privacy of users, their ‘friends’ and others discussed. The apparent trends towards untrammelled publicity suggest that not only sporting figures and other celebrities may find themselves constantly on show to their voracious audience, despite their efforts to prevent this happening. Now we are seeing a multitude of ordinary and sometimes quite vulnerable people also suffering inconvenience and distress and even deeper harms from the prying eyes and gossipy comments of others. Indeed given that ordinary people and celebrities are often not that different it is easy for these two groups to overlap – I would say Lara Bingle is a good example here. So perhaps it is not surprising that the public pressure for more effective legal privacy protection might be increasing.

To demonstrate its sincerity in tackling the possible problem of privacy the government has recently published an Issues Paper asking the Australian people for advice on the need for a new statutory tort. In fact, this represents just one more stage in a constant public consultation program on the benefits (or not) of a statutory cause of action in privacy. In 2008 the Australian Law Reform Commission made recommendations for a statutory privacy tort, after a substantial review including a nationwide program of consultation. Following that report there were further reports from the New South Wales Law Reform Commission (in which I was involved as a member of an expert advisory panel) and the Victorian Law Reform Commission, both also coming at the end of a program of public consultation. And both also recommended statutory causes of action for invasions of privacy (although in each case these were slightly differently framed). So it seems that there is considerable public support for a statutory privacy tort. But would this bring all the benefits proclaimed?

My question here is not about the possible benefits of a new statutory action. It is true that our existing law already provides a significant degree of protection to privacy, through the actions such as breach of confidence, defamation, passing off, harassment, and intentional infliction of emotional distress. Breach of confidence especially functions as a privacy doctrine, being based on an idea of trust and confidence that information that is not a matter of ‘public knowledge’ will be treated according to the wishes of the party it concerns. (It would have been the obvious action for the Australian Defence Force Academy cadet who recently discovered that images of her engaging in sex had been secretly streamed to her partner’s friends). But a statutory action for invasion of privacy would provide greater transparency than an action which is not framed around privacy – in the same way that the statutory tort of misleading or deceptive conduct is more transparent than the traditional common law misrepresentation and passing off actions. It could also usefully provide more avenues for enforcement than the courts, utilising the federal and state information and privacy commissions. And it would hopefully be more easily updated than the slow-moving incrementally-adapting common law to accommodate new situations and circumstances.

And the benefits would not only have to be on the side of privacy claimants. A statutory public interest defence, as recommended for instance by the Victorian Law Reform Commission, would provides a vehicle for interests in privacy and publicity to be balanced on a case by case basis – providing a clear basis for protecting free speech while not conceding automatic and absolute priority when it comes to speech which involves or results from an invasion of other’s privacy. There are many cases where a balance between privacy and free speech may seem relatively straightforward. The leaked shower photo of Lara Bingle is a good example. Here the free speech argument for publication is weak to non-existent compared to Bingle’s claim for privacy. Or, to take another real-life example (from the 2006 case of Australian Broadcasting Corporation v O’Neill which went to the High Court as a defamation case), the public interest in revelation on the ABC of a convicted child killer’s confession to an undercover journalist (and former police officer) that he had killed other children seems very strong even in the face of his claim for protection of privacy. For the revelation not only raises questions of public safety but also of the operation of the justice system.

Of course not every case would be so straightforward. For instance, there is the controversial English case of the blogger ‘NightJack’ who became famous for his insider’s account on the life of a serving police officer and then found that The Times proposed to publish his true identity having discovered this via a journalist, using ‘mainly’ internet sources (the other sources were less clear). The blogger sought an injunction on the basis that the information as to his identity was ‘private and confidential’, that he gone to lengths to secure his identity, and that those who knew he was NightJack also knew this was private and confidential – adding, moreover, that there was no clear public interest that justified publication in The Times. The judge refused an injunction on the grounds that, first, blogging is a ‘public activity’ and, second, the public interest supported public exposure of the blogger’s violation of the police code of practice. It may be wondered...
whether blogging should be deemed to be such a ‘public activity’. But I am sympathetic to the argument that on balance the public interest supported the publication. In any event, the blogger (Richard Horton) seemed to accept the finding. He wrote a follow-up article of his own in The Times where he talked about his motivations and at the same time expressed loyalty to the police force (which had for its part had limited its penalty to a warning). Needless to say, he showed less sympathy for idea of the inherently public nature of blogging. Why would he?

But the question whether a statutory privacy tort would bring all the benefits that have been claimed by its supporters still has to be asked. The question comes down to how the tort would be framed as a matter of statutory language. One question currently being considered is whether a privacy claimant should have to show that the violation of privacy would be ‘highly offensive to a reasonable person of ordinary sensibilities’, as recommended by the Australian Law Reform Commission. The Victorian Law Reform Commission made a similar recommendation. But it was not the recommendation of the New South Wales Law Reform Commission. And there are several (including myself) who have argued that a high offensiveness standard would be an onerous and unfair standard for a privacy claimant. It would effectively carve out a sphere of absolute protection for speech and other conduct which invades a person’s privacy according to that person’s own lights, not on the basis of any public interest in knowing the information but simply on the basis that a ‘reasonable person of ordinary sensibilities’ would not be highly offended. What justifies the ordinary/reasonable person’s involvement in filtering individual privacy claims in this way?

Certainly, this standard is not historically part of our law. For instance, our action for breach of confidence is traditionally premised on allowing individuals to decide how seriously concerned they are about the public discussion of their affairs – that was noted by Mason J in the 1980 defence papers case Commonwealth v John Fairfax & Sons (pointing out that the government should be held to a higher standard). Although Gleeson CJ hinted that a high offensiveness standard might be a useful adjunct to the breach of confidence action when used to protect privacy in the 2001 case of Australian Broadcasting Corporation v Lenah Game Meats, operating as a ‘useful practical test’ in scenarios where information was not ‘necessarily private’, there was no suggestion there that it should be erected into a threshold that might deny protection to otherwise private information. Nor does it come from the United Kingdom’s statutory provision for privacy in the Human Rights Act 1998 (implementing the Article 8 right to private life in the European Convention on Human Rights). And the UK courts for their part have rather preferred as the starting point for assessing a privacy claim a ‘reasonable expectation of privacy’, treating this as a matter to be judged from the perspective of the claimant, not the audience which is seen to have its own vested interest in publication (given its role as consumer).

In fact, the highly offensive standard comes from the US privacy torts which are notoriously difficult to satisfy. In practice, not only does this threshold carve out a protected zone of privacy-intrusive free speech. It takes the majority’s will as the proper standard of what a privacy expectation should be. While this might make sense in a jurisdiction which has erected freedom of speech to an overriding constitutional imperative, in jurisdictions (such as ours) where freedom of speech is traditionally treated in a more balanced and fact-specific way it would be a curious development in our law. Why should we import this US standard into our law, especially when the American attitude to privacy is historically so different from our own?

Perhaps the language of ‘highly offensive’ to an ordinary/reasonable person could be read differently in an Australian context than an American one. I would hope so. In the US, courts refused to uphold a privacy claim brought by a chronically private former child protégé, now a recluse, who was exposed in an article in The New Yorker using information obtained by an undercover journalist masquerading as a friend of the claimant and which was “merciless in its dissection of intimate details of its subject’s personal life” (in the 1940 case of Sidis v F-R Publishing Corporation). They also gave no credence to the privacy claim of a Hasidic Jew of the Klausenberg sect whose religion prohibited the use of ‘graven images’ after he was secretly photographed by a street photographer hiding behind a scaffolding in Times Square New York with the photograph later exhibited and sold as an artwork (in the 2007 case of Nussenzweig v diCorcia). And they had no sympathy for the privacy claim of a Berkeley student Cynthia Moreno who having posted a critical comment about life in her former hometown on her ‘Cynthia’ MySpace page and taken them down six days later found her former headmaster had arranged its publication in the local newspaper with her full name attached (in the 2009 case of Moreno v Hanford Sentinel, Inc). A subsequent claim for intentional infliction of emotional distress also failed notwithstanding that after the forced publicity she suffered threats and her family was forced to close its business and leave town.

The American media lawyer David Anderson once wrote that the fact that Americans (in general) do not value privacy highly and rather want to know everything about their neighbours goes some way to explain what he called ‘the failure of American privacy law’ (in Markesinis (ed), Protecting Privacy, 1999). If there is an Australian culture of privacy I would say it is more sympathetic to individual claims of privacy as a counterweight to free speech, in keeping with 19th century Millian ideas of individual liberty and utilitarian balances which are traditionally embedded in our common law. Perhaps we are changing in our expectations of privacy, but for my part the American approach is not a good model for where we might want to go with privacy protection. If that is where a statutory cause of action would take us, I would rather stick with the incrementally-developing common law.

Megan Richardson is a professor at the Melbourne Law School.

The Federal Government should be applauded for giving serious consideration to the recommendation of the Australian Law Reform Commission three years ago that Parliament legislate for a right to sue for damages for serious invasion of privacy.

Media companies have sprung to oppose the recommendations. But their arguments are unconvincing.

The reasons why Parliament should legislate are more fundamental than the need to respond to the wrongdoing of a rogue media company.

The reasons why Parliament should legislate are more fundamental than the need to respond to the wrongdoing of a rogue media company, even if it does control about two-thirds of metropolitan newspaper circulation in this country.

Parliament should act because technological change is eroding privacy to such a degree and so rapidly that, without some legal protection, very little privacy will be left to us before long.

The technological and other innovations that have encroached on privacy in recent years include:

- The internet, with its capacity to broadcast personal information instantaneously around the world, its spyware to snoop on users and its social networking sites that turn users into open books
- Mobile phones, with their GPS systems that can track your movements
- Smartcard technology that records your movements (through public transport, toll roads and credit and debit card purchases), profiles your spending habits and your health details
- The spread of CCTV
- Anti-money laundering legislation that swept away banker-customer confidentiality and compels a range of people from bankers to solicitors to report ‘suspicious’ activities of clients to the government
- Mandatory reporting legislation that requires health care and other professionals to report suspicions of abuse of various kinds to the government
- Copying and scanning technology that enables nightclub bouncers and taxi drivers to make permanent records of the personal details of their customers.

These innovations no doubt have many positive applications. But they have fundamentally redefined privacy and it is futile to think we can enjoy the sort of privacy that prevailed before this technology.

There are good reasons why we should try to retain as much privacy as possible in the information age.

Privacy can be thought of as denoting that sphere of a person’s life that they control completely, to the exclusion of others. What we keep private is a matter of personal choice. The key thing is that choice.

A common feature of democratic societies is the recognition that all citizens are entitled to a private life and to a wide range of choice about what is kept private.

By contrast, the control exercised by totalitarian and authoritarian states is inconsistent with personal privacy. They deny any right to choose to keep things private and permit the state to reach into the deepest recesses of personal lives.

Most of the great human rights instruments marking out the freedoms of democratic societies include a right of privacy: the Universal Declaration of Rights, the International Covenant on Civil and Political Rights, the EU Directive on Data Protection.

But the Victorian Charter gives only limited legal recognition to this right. It merely requires courts to interpret other legislation in a manner consistent with the right and requires public officials to act in accordance with it.

There is a patchwork of laws in Australia that requires government agencies and certain other bodies to deal properly with personal information but none of them gives redress of the kind proposed by the Law Reform Commission, i.e. a general right to sue for damages for a serious and intentional invasion of privacy.

Strict regimes for the protection of databases have not managed to defeat human inquisitiveness, leading to a number of serious breaches of privacy in Australia and overseas, quite apart from the recent News Corporation scandal.

In the aftermath of one such breach in the United Kingdom, the motoring journalist Jeremy Clarkson derided the alarm expressed about the disclosure of personal bank account details. He published his own bank account details and was then embarrassed when a hacker accessed his account and transferred £500 to a charity!

Clarkson had the sense and good grace to admit he was wrong to be blasé about privacy.

A common feature of democratic societies is the recognition that all citizens are entitled to a private life and to a wide range of choice about what is kept private.

Let us hope the naysayers in Australia can learn the same lesson but less painfully. They should recognise the many and far-reaching intrusions into privacy wrought by recent technological and other innovations. They should acknowledge the need to provide some legal redress for serious breaches of privacy, even if it means less celebrity gossip in the press.

Such a right will no more prevent invasions of privacy than the law of negligence prevents car accidents. But it should serve to reduce them and to provide legal redress in cases of serious personal harm. Just as the law of negligence developed in response to changing technology and social conditions of the early 20th century, a similar legal development is needed now in the early 21st century.

There are serious restrictions on the equitable action for breach of confidence, which prevents it from developing to fill this gap. A legislative response is therefore the best solution. And so the ALRC’s recommendation deserves serious consideration and support. The self-interested complaints of media organisations should not drown out the important policy issues behind this proposed reform.

Michael Pearce SC is a lawyer and immediate past president of Liberty Victoria.

First published in The Age, 27 July 2011
The great privacy debate

Any debate about privacy should start and finish with the Government’s own hypocritical role on the issue, argues Mungo MacCallum

O K, let’s have a debate about privacy. But before we get around to the dastardly Murdoch press, let’s be honest about a couple of things. And the first is that we have very little privacy left anyway.

Many years ago, when the then-government proposed the idea of an Australia Card as a useful way of putting together various bits of information and as a foolproof means of identification, there was a public outcry: Big Brother wanted to snoop and spy on our most intimate secrets, creeping totalitarianism was invading our most precious moments.

Now, of course, virtually all of us have tax file numbers, Medicare cards, at least one credit card and a bank account; and a great many of us also receive some kind of pension, family benefit or other kind of welfare payment. And just in case anyone had been missed, we are all about to fill out a comprehensive census form. We have happily handed over far more personal details than were ever envisaged by the Australia Card, and the ones we have not volunteered can very easily be taken from us.

While the authorities have no compunction in invading your privacy in the name of national security, they use exactly the same excuse to protect their own.

There are now commercial surveillance cameras everywhere. Eavesdropping devices are readily available and openly used in many businesses. And if private enterprise has not already done the job, the Government has vastly beefed up its own already unwieldy security apparatus, using the so-called War on Terror as a pretext. Organisations such as ASIO and the Federal Police, whose main purpose is to spy on the citizenry, now control huge budgets for which they are largely unaccountable, and there are other, more sinister bodies which we seldom if ever hear about.

These, we are assured, have kept us safe from mayhem and massacre on our own shores: the proof is that there hasn’t been any. Yes, the elephant repellent must be working; let’s apply more of it. These days Big Brother is not only watching you and listening to you; there is research under way to enable him to touch, smell and taste you as well.

And while the authorities have no compunction in invading your privacy in the name of national security, they use exactly the same excuse to protect their own. The very words ‘national security’ have become a cover for anything that the Government might not want made public; they can be and are used to cover up a multitude of errors, misjudgements and embarrassments.

Other useful tags include ‘commercial in confidence’, and ‘operational matters’. And if all else fails there is always the frequently used fallback ‘inappropriate’. It is not in the public interest for the public to know.

Well, hang on a minute; surely that is a matter for the public to decide. When the WikiLeaks argument was at its height, Julia Gillard scolded Julian Assange for believing that the public had a right to know everything. Well, precisely; that is the default position in a free and open society.

Government should be transparent; where it is not, it is up to the Government to give very good reasons why. The people do not have to justify ‘a right to know’; that it assumed in any democracy worth the name. If material is to be concealed it is up to the Government to justify the exception and for the voters to judge whether the justification is adequate. Of course there are times when it will be; but the constant use of weasel words instead of logical explanation suggests that the principle is greatly abused.

Which finally brings us back to those other great catchalls, free speech, the freedom of the press, and the right to personal privacy. But before we go any further let’s be clear about one thing: no sane person, and that includes Rupert Murdoch, can condone the hacking of a murdered child’s phone and its subsequent manipulation to deceive the child’s parents and obstruct the police investigation. There are some lines which cannot be crossed in a civilised community and that is clearly one of them.

And the wilful invasion of the private space of private citizens is generally considered taboo. But with public figures and so-called celebrities, the lines become less distinct. Politicians and others who have real jobs in the real world may well feel they have some right to privacy and that what they do in their spare time should be off-limits unless it clearly impinges on their public duties.

But what about those who are simply famous for being famous, who live by and for the media spotlights? Can anything Paris Hilton does be said to be private? And many otherwise undistinguished people are drawn to follow the same path. Can those who go the full monty on Facebook and Twitter really complain about lack of privacy?

With the new media rampant, there may well be a case for re-opening the argument. But any debate about privacy should start and finish with the Government’s own hugely hypocritical role on the issue.

Mungo MacCallum is a political journalist and commentator.
In May 2008 the Australian Law Reform Commission issued a report recommending the introduction of a specific legal provision that would allow people to take action for serious invasions of privacy. The report has lain dormant ever since.

Against this backdrop, federal Privacy Minister Brendan O’Connor’s announcement of a consultative period as a forerunner to a new legal provision for invasion of privacy is curious.

Hysteria over the *News of the World* phone hacking scandal has masked the deafening public silence in response to the commission’s recommendation for such a provision, a right of action many view as a privilege that will be available only to the wealthy and famous. Also, there is little evidence that such a provision is needed and, if it were enacted, would have any work to do.

The *News of the World* saga presents the best and most topical example of this. Were Australian journalists to engage in the type of conduct that is the subject of the British police investigations – and there is not a skerrick of evidence to suggest they have, underscoring doubts over the need for privacy reform – they would almost certainly be guilty of offences under the *Telecommunications (Interception and Access)* Act and the *Commonwealth Criminal Code*. The former makes it illegal to access stored communications such as voicemail and email without consent; the latter makes it illegal to pretend to be someone else for the purpose of committing an offence.

As well as criminal liability, the offender is liable under the legislation to be sued for damages by the aggrieved person in relation to any unauthorised accessing of voicemail or email. No tort of privacy required.

Based on these trends, one doubts that an Australian court would have much trouble affording protection to plaintiffs involved in sexual escapades, such as Mosley and Giggs. While the Mosley and Giggs cases raise serious questions about the efficacy of existing remedies for invasion of privacy (in particular, the potential futility of injunctions in a social media world), they do not provide any support for the introduction of an Australian privacy tort.

In many ways, the Australian breach-of-confidence law is more strict than the UK law. Unlike in Britain, there is no overarching...
‘public interest’ consideration in the Australian law. Defendants are entitled to expose wrongful or criminal conduct but only to the relevant authorities. Unless conduct is of the most serious kind, perhaps wrongdoing in public office, it is highly unlikely a court would sanction media disclosure.

Australian law also does not recognise a person’s capacity to place segments of their life in the public domain. This was the basis of the British court’s decision to reject part of Naomi Campbell’s privacy claim. Campbell may well have had more success in Australia than in the privacy mecca of the UK, and we must not lose sight of this.

We all should be thankful we live in a country that enjoys a largely ethical and responsible media. Existing privacy and reputational protections have been instrumental in shaping this landscape. Indeed, many would argue existing laws are already too heavily weighted against free speech and press freedom. Our defamation laws are some of the most onerous for publishers in the Western world and we lack the broad constitutional protection for free speech that exists in the US and under the European Convention on Human Rights. Perhaps conscious of this, and of existing privacy protection, the High Court and Victorian Court of Appeal have been extremely hesitant to recognise a common law provision of privacy.

**Australian law also does not recognise a person’s capacity to place segments of their life in the public domain.**

In such circumstances, and the absence of any evidence the Australian media has engaged in systemic phone hacking or other forms of illegal or egregious conduct, the government should be very wary of imposing further restrictions on the press in the form of a legal provision that would let people take action for invasions of privacy. More fundamentally, the government needs to ask: what would such a law achieve?

_Sandip Mukerjea is a senior associate with law firm Minter Ellison, which is an external legal adviser to ‘The Age’_.

First published in _The Age_, 22 July 2011
Chapter 2
Communications privacy

Protect your identity and privacy

Advice from the Department of Broadband, Communications and the Digital Economy

Treat your personal information as you would treat your money – don’t leave it lying around for others to take.

Most people are very careful with personal documents such as a birth certificate or driver’s licence. You keep them in a safe place and wouldn’t give them to someone you didn’t know or trust.

You should do the same thing with your personal information online to prevent others from using this information to impersonate you.

With a stolen identity, a person may access your bank account, obtain credit cards or loans in your name or claim welfare benefits, and potentially ruin your credit rating.

Top tips
➤ Stop and think before you share any personal or financial information – about you, your friends or family. Don’t disclose identity information (drivers licence, Medicare No, birth date, address) through email or online unless you have initiated the contact and you know the other person involved
➤ If you use social networking sites, adjust your privacy settings to control the amount and type of information you want to share, so that people you don’t know very well can only see certain parts of your profile
➤ Don’t give your email address out without needing to. Think about why you are providing it, what the benefit is for you and whether it will mean you are sent emails you don’t want
➤ Before giving your email address online read the website privacy policy. This should tell you how they will use the email address you provide
➤ If you often use your email address online you may want to have a secondary email account. Use your primary email with friends and businesses you know and trust
➤ Set strong passwords, particularly for important online accounts and change them regularly – consider making a diary entry to remind yourself.

Steps to protect your identity online
➤ Use a strong password and do not share it with anyone. A random combination of numbers, letters and punctuation over eight characters long is recommended
➤ Check your billing and account records carefully to detect potential identity theft early
➤ Set up a separate email address for shopping and newsgroups. If you need to, you can then change this address without disrupting online business activities
➤ Only share your primary email address with people you know
➤ Be careful when signing up to mailing lists – spammers use the unsubscribe button to validate addresses
➤ Only make online purchases from companies that have a clear privacy policy
➤ Think before you fill out online forms. Ask yourself, how much information do I need to enter into this site?
➤ Keep a record of what information you’ve given to whom.

Be careful how much personal information you post or reveal online
➤ Users who share addresses, telephone numbers, birthdays, and other personal information put themselves at a greater risk for identity theft, stalking and harassment. This includes information you may post on your Facebook wall or someone else’s
➤ If you use social networking sites, adjust your privacy settings to control the amount and type of information you want to share, so that people you don’t know very well can only see certain parts of your profile
➤ Think about information spread across multiple sites as people can piece together information from separate websites. Identity thieves can piece together your identity from public information piece by piece like putting together a jigsaw.

What to do if your identity has been stolen
➤ Notify financial institutions
➤ Change passwords
➤ Notify relevant websites
➤ Request a credit report from credit bureaus
➤ Notify the authorities. A list of who to contact is included in the Protect Yourself Online – What everybody Needs to Know brochure published by the Attorney-General’s department.

Protect your identity and privacy fact sheet
Stay Smart Online
www.staysmartonline.gov.au
© Commonwealth of Australia 2011 – reproduced by permission

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au

Issues in Society | Volume 341
Privacy and Information Rights 19
The net has become an essential part of daily life and while it allows you to connect, create and communicate 24/7, there are some very real risks that you need to be aware of.

Unwanted contact, sexting and cyberbullying are just some of the situations that you may find yourself faced with.

Safeguard yourself and your friends by understanding the issues and knowing how to respond.

**CYBERBULLYING**

*What is it?*

Cyberbullying is using technology to deliberately and repeatedly bully someone else. It can happen to anyone, anytime, and can leave you feeling unsafe and alone.

Cyberbullying can include:

- Abusive texts and emails
- Posting unkind messages or images
- Imitating others online
- Excluding others online
- Inappropriate image tagging.

Remember; treat others as you would like to be treated when communicating online.

*How is it different to face-to-face bullying?*

While cyberbullying is similar to face-to-face bullying it also differs in the following ways:

- It can give the person doing the bullying a sense of being anonymous
- It can occur 24/7 and be difficult to escape
- It is invasive and you can be targeted while at home
- It can have a large audience – sent to groups or posted on a public forum
- It can be permanent.

**How do I deal with it?**

- Don’t retaliate or respond
- Block the person doing the bullying and change your privacy settings
- Report it – click the report abuse button
- Collect the evidence – keep mobile phone messages and print emails or social networking conversations
- Talk to someone you trust, like a family member or friend.

Talking to your teachers or parents can make a difference. Your school may have policies in place to deal with bullying and cyberbullying.

**What do you do if your friend is being bullied online?**

While it can be hard to know if your friends are being cyberbullied if you see or know about cyberbullying happening to a friend:

- Don’t forward messages or pictures. Though you may not have started it, you will become part of the cyberbullying cycle
- Stand up and speak out – tell a trusted adult
- Support your friend and report the bullying.

If you want to talk about a problem with cyberbullying, you can call Kids Helpline on 1800 55 1800, visit their website or contact the Cybersmart Online Helpline service.

**UNWANTED CONTACT**

*What is it?*

Unwanted contact is any type of online communication that you find unpleasant or confronting.

The contact can come from online friends you don’t know or someone you know in the offline world.

Unwanted contact can include:

- Being asked inappropriate or personal questions from someone you don’t know
- Being sent offensive, confronting or obscene content
- Being asked to send intimate pictures or do things online that make you feel uncomfortable.

**How do I deal with it?**

- Tell someone you trust, like your mum, dad or another adult
- Don’t respond and leave the site or chat session
- Block the contact or remove them from your friends list
➤ Change your profile settings so that your personal details are kept private
➤ Don’t open messages from people you don’t know
➤ Keep the evidence. This can be useful in tracking the person posting unsuitable material
➤ Contact your ISP and/or phone provider, or the website administrator. There are actions they can take to help.

Most importantly – report it. Talk to an adult that you trust or to the police if there is a threat to your safety.

Suspicous online behaviour towards a child should be reported to the Australian Federal Police.

Remember, if you want to talk about a problem with unwanted contact you can call Kids Helpline on 1800 55 1800, visit their website or contact the Cybersmart Online Helpline service.

SOCIAL NETWORKING AND ONLINE FRIENDS

Chatting to friends using IM, chat or social networking is a great way to stay in touch and make new friends. However, you should always keep in mind that there are some risks meeting people online – especially if you don’t know them in real life.

Tagged photos, blog posts and social networking interactions will all shape how you are perceived by others online and offline.

Know the basics of safe social networking
➤ Limit your friend list – don’t friend randoms
➤ Protect your privacy – don’t share your password and set your profile to private
➤ Your personal details are valuable – don’t share them without a good reason
➤ Protect your reputation – remove flirty photos and nicknames
➤ Be careful who you trust – a person can pretend to be someone they are not
➤ Think before you post.

Meeting online friends in the real world
If you want to arrange to meet an online friend, ask an adult to go with you.
Always meet in a public place, preferably during the day. Remember, if you want to talk about a problem, you can call Kids Helpline on 1800 55 1800, visit their website or contact the Cybersmart Online Helpline service.

DIGITAL REPUTATION

What is my digital reputation?
Your digital reputation is defined by your behaviour in the online environment and by the content that you post about yourself and others.
Tagged photos, blog posts and social networking interactions will all shape how you are perceived by others online and offline.
A poor digital reputation can affect your friendships and relationships as well as your future job prospects.
What happens online can permanently affect you in the real world – so protect your digital reputation.

How do I protect my digital reputation?
➤ Think before you post!
➤ Set your profile to private – and check every now and then to make sure the settings haven’t changed
➤ Keep an eye on photos tagged by your friends.

Remember, online information could be there forever. Your personal information may end up being seen by people you don’t know, including potential employers.

ONLINE SHOPPING

Online stores and auction sites are a convenient way to save money and shop after hours. You should make yourself aware of some of the differences between shopping online and offline.

Know the basics
➤ Use the websites of well-established, recognisable retailers
➤ Use sites that you know deliver and that fall under Australian consumer laws
➤ International websites may not be governed by Australian consumer laws
➤ Use a reputable auction site and make sure you are comfortable with how transactions work
➤ Know the cost – read the terms and conditions related to delivery charges and warranty conditions
➤ Understand the service – is it a one-off cost or an ongoing contract?
➤ Know what you’re getting and when – contact the seller directly to ask questions.
Protect yourself
➤ Read the site’s privacy policy
➤ Make sure that you can make a complaint or cancel an order
➤ Ask for help if you are unsure
➤ Look for the padlock symbol in the browser during the transaction process – this shows that the transaction is a secure one
➤ Know how to stop an ongoing service.

IDENTITY THEFT
What is identity theft?
Identity theft is when your personal information is used without your knowledge or permission.

With sufficient information, criminals can use your information to:
➤ Open bank accounts in your name
➤ Apply for credit cards or loans in your name
➤ Transfer money directly from your bank accounts
➤ Impersonate you online on social networking sites.

Identity theft can damage your chances of applying for loans and credit cards when you are older.

How do I avoid it?
➤ Monitor your content – if your profile has been hacked shut it down ASAP
➤ Use secure websites for online shopping and banking
➤ Don’t post personal information – small pieces of personal data can be used to build a much bigger picture
➤ Change passwords – password should be:
  - Eight or more characters in length, preferably a mix of symbols, letters and numbers
  - Changed regularly
➤ Never shared.
➤ Don’t get phished – don’t respond to calls or emails from banks asking for passwords or other details. If the email asks you to click on a link, chances are it’s a scam. If you receive a call from someone saying they’re from the bank, hang up and call back on their publicly listed number to see if it’s real.

How do I deal with it?
➤ Watch your bank account and respond immediately to any unexpected withdrawals or suspicious spending
➤ Report it – talk to an adult that you trust, and to your bank.

Remember, if you want to talk about a problem with identity theft, call Kids Helpline on 1800 55 1800, visit their website or contact the Cybersmart Online Helpline service.

LOCATION-BASED SERVICES
Smart phones have a built-in feature called geolocators that can pinpoint your exact location. This data is often published online through social networking sites, or used by location-based services such as maps, public transport apps, retail services and so on. It can also be embedded in images you take with your smart phone camera.

Sometimes, you might want to think twice before you check in and tell the world where you are.

Know the basics
➤ Geolocators can be switched off – go into your phone settings and switch off location services on your handset
➤ Checking in from your smart phone tells people where you are and what you’re doing
➤ Checking in also lets people know where you aren’t
➤ Be aware of how the information might be used by online friends that you don’t know in the real world.

Protect yourself
➤ Turn off the geolocator unless you absolutely need to use it
➤ Make sure that your location is only visible to friends you know in the real world
➤ Double check your privacy settings so that if you do share location information it’s really only going to the people you want it to
➤ Check that the service doesn’t also show your details to those nearby who you might not know
➤ If you have problems while using a service, report it to the service provider
➤ If you feel unsafe while you’re at a particular location contact the police
➤ If in doubt, don’t check in.

Remember, if you want to talk about a problem, call Kids Helpline on 1800 55 1800, visit their website or contact the Cybersmart Online Helpline service.

© Commonwealth of Australia 2012
Reproduced with permission of the Australian Communications and Media Authority’s Cybersmart program | www.cybersmart.gov.au

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
Yes. Like many activities on the web, there are some privacy risks. You can minimise the risks by taking steps to protect your personal information online.

Protecting information online
Here are some of the things you should think about when using social networking sites. They are not meant to scare you, just help you to be prepared.

Don’t be under any illusions – it’s not just your close friends listening in!
Sometimes it can feel like your MySpace page is like an online diary and the only people reading it are your close friends.

Not true! Think carefully about the information you post. Would you be comfortable with your teacher, uni lecturer, employer, parents or a police officer reading the information you post?

Are you sure you want that information to be public?
Be careful about what sort of information you post on social networking sites.

You have probably seen some of those media reports where people have applied for a job and found that their MySpace or Facebook page has let them down. Others have actually lost their jobs due to comments they have made about their employer on MySpace or Facebook.

Remember that comments you post on social networking sites are mostly public. So, think carefully about what information you publish about yourself.

If you have a message for a particular friend, consider sending it to their inbox rather than posting it publicly on their wall.

Remember that activities online affect your life offline
Imagine you are planning a party and post the details on your MySpace page including your address. On the day, strangers show up uninvited, gatecrash the party and vandalise your house.

This is an extreme example but it does happen!
A more common example is if you are part of a social group on MySpace or Facebook. If the group meets regularly or attends certain events, your membership of this group may allow people you don’t know to find you.

When you are online on MySpace or Facebook, it can feel a bit like these sites are a world away from your real, physical life at home.

Not true! These different worlds aren’t as far apart as you think. When you give out information about yourself online, you make it easier for people online to find you offline.

So, think carefully about who you want knowing where you live, what your phone number is, or which school you go to.

Protected your own privacy? ... what about your friends?
So you’ve been careful to protect your own privacy, but what about the privacy of other people? When you use a social networking site, the privacy of your friends and family is in your hands. Are they comfortable with (or do they even know about) the information you are revealing about them on your MySpace page?

A risk with social networking sites is that people lose control over their personal information – people who might not even use the site.

Think carefully about what you’re going to post about others. Try putting yourself in their shoes. Maybe it’d be a good idea to ask your friend before you post that information or photo.

Remember that others have a right (like you) to control how information about them is made public.

Watch out for identity theft
Identity theft occurs when someone steals information about you, often so that they can steal money from you.

For example, if someone gets enough personal information about you, they may be able to apply for a credit card or a loan in your name. After they’ve taken off with the money, the ‘real’ you is left with the bill and the bad credit rating.

Identity theft doesn’t always have to involve money.
Your MySpace or Facebook account details and password could be stolen by an identity thief who then logs onto your profile, vandalises your page and sends messages to your friends pretending to be you.

You make it easier for identity thieves when you make lots of information about yourself public.
SAFE SOCIAL NETWORKING

While most people who use social networking sites are well intentioned, you need to be careful about the information that you share and how you protect it. Advice from Stay Smart Online

People can inadvertently or intentionally use your information to embarrass you or damage your reputation, or to even steal your identity. Social networking sites such as MySpace, Facebook, Twitter and Linkedin are used to stay in touch with friends, make new friends or business connections and to share information and opinions about topics we’re interested in.

You need to think about how much information you provide and to whom.

TOP TIPS

➤ Always type your social networking website address into your browser
➤ Never use the same password that you use for your bank or email accounts. Have a different password for each social networking site so that if one password is stolen, not all of your accounts will be at risk
➤ Don’t automatically click on links in ‘friend request’ emails you receive. Genuine friend requests will appear on your home page on your social networking site
➤ Be careful about how much personal information you post online. Use privacy settings to control who has access to your information
➤ Be careful about the amount of information that you reveal to people you don’t know. It is easy to create a fake profile online and people are not always who they say they are
➤ Stop and think before you write a message or post pictures. Ask yourself if the information you are sharing is something you want your future employers, friends or family to see. Even items you delete can remain on the internet for years.

CHECK THE SITES’ PRIVACY POLICIES

Read the website Privacy Policy before you sign up. Legitimate social networking sites will have a privacy statement which tells you how they collect and use your information and when and how they might disclose this information either through the website or to third parties.

➤ Some sites may share information such as email addresses or user preferences with businesses, which could send you spam
➤ Locate the sites’ policies for handling referrals to make sure that you do not accidentally sign your friends up for spam
➤ Privacy policies can change. In some cases these sites may notify you of changes. In many cases by continuing to access or use the Services after those changes become effective, you agree to be bound by the revised Privacy Policy. If not you should regularly review privacy policies and review how much information you reveal in your profile
➤ If you use applications or sign up for games inside the website remember to read the individual privacy policy. Don’t assume that they will have the same policy as the parent website. Some online games are set up to utilise the ‘networking’ aspects of the site and specifically state that they can use your information and your friend’s information in whatever way they like.

The photos, comments, messages and wall posts that you share could be seen by anyone, and are not always removable if you change your mind.

BE CAREFUL HOW MUCH PERSONAL INFORMATION YOU POST OR SHARE ONLINE

Once information is online, it is not easy to remove it completely. Even if you remove information from your profile, saved or cached versions may still exist on other computers.

➤ Adjust your privacy settings to control the amount and type of information you want to share, so that people you don’t know very well can only see certain parts of your profile
➤ The photos, comments, messages and wall posts that you share could be seen by anyone, and are not always removable if you change your mind. This includes information in your profile, on blogs and other forums. People often forget that people other than their friends might see the information
➤ Often when you apply for a job, companies may check to see if you have an online profile. Be aware that the photos and information you share with your friends may not be what you want you prospective employer to see

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
➤ Do not post information that would make you or your family vulnerable (e.g. your date of birth, address, information about your daily routine or holiday plans). This information can be used by criminals to commit identity theft. Users who share addresses, telephone numbers, birthdays, and other personal information put themselves at a greater risk for identity theft, stalking and harassment. This includes information you may post on your wall or someone else’s.

**BE CAREFUL ABOUT SHARING YOUR OPINION ONLINE**

Be careful about what you say about others online. Posting something rude, offensive or derogatory about another person or business in a public forum can have consequences. Once you post a comment it can be difficult to remove all record of it. Comments you make may be used as legal evidence.

Once you post a comment it can be difficult to remove all record of it. Comments you make may be used as legal evidence.

**BE WARY OF STRANGERS**

People are not always who they say they are.

➤ It is a good idea to limit the number of people you accept as friends

➤ If you are ‘friends’ with people you do not know, be careful about the amount of information that you reveal and don’t agree to meet them in person

➤ Use your social networking site’s privacy settings to limit their access to your information.

**WATCH OUT FOR PHISHING EMAILS**

Emails pretending to be friend requests from social networking sites try to direct people to fake versions of these websites. These fake websites may contain malicious software that could steal your personal information and infect your computer.

To help protect yourself from phishing emails:

➤ Never click on links in emails, even if they look genuine, and

➤ Always type your social networking website address into your browser.

Any genuine friend requests will appear on your home page on your social networking site.

**OTHER STEPS TO PROTECT YOURSELF WHEN SOCIAL NETWORKING**

Protect your accounts with strong, unique passwords. Never use the same password that you use for your email account. This reduces the chances of a hacker or even your friends logging in to your account without your permission. Have a different password for each social networking site so that if one password is stolen, not all of your accounts will be at risk.

Never click suspicious links – even if they appear to be from your friends. Their accounts could have been infected with viruses or other malicious software. If you click the links that they post on your profile page or send in messages, your computer and account could become infected by malicious software too.

© Commonwealth of Australia 2010 – reproduced by permission
Stay Smart Online | www.staysmartonline.gov.au
We use mobile phones for many things: to make calls, send messages and emails, listen to music, store calendar appointments, take photos, pay for things, get directions and access the web. It is easy to forget how much personal information is stored on your phone and just how easy it is to leave your phone unattended or open to theft. Here are some steps to increase your phone privacy and security to give yourself peace of mind.

1. **Know where your phone is**
   It sounds obvious but you’d be surprised at how many phones are lost or stolen each year. Treat your phone like your wallet – know where it is at all times and don’t leave it unattended.

2. **Turn on your security features**
   All phones have security settings so familiarise yourself with them and turn them on. On most phones, you can find security settings under the general ‘settings’ part of your phone’s main menu.

3. **Set a password or pin**
   To protect your personal information, set your phone to ask for a password or PIN each time you use it. This is the best way of safeguarding your phone if lost or stolen. It can also help stop anyone else from tampering with it. Using a PIN on your SIM card will prevent thieves from stealing your phone credit or running up your phone bill.

4. **Report your lost or stolen phone**
   Every phone has a unique International Mobile Equipment Identity (IMEI) number. Most phones will display their IMEI if you key in *#06#. If your phone is lost or stolen, you can ask your network provider to block your IMEI to prevent others using your phone.

   **Not only does loss or theft mean your personal information is vulnerable, it may also mean that a thief might run up a large phone bill.**

5. **Turn off Bluetooth and GPS when you are not using them**
   Not only are Bluetooth and GPS a drain on your battery, they can also sometimes allow others to see the location of your phone. Bluetooth can also be used to transmit viruses and intercept data. Although Bluetooth and GPS are useful tools with great benefits, it is a good idea to turn them off when you don’t need them.

6. **Think before you click**
   Be careful when opening multi-media messages (MMS), attachments in emails, and clicking links in emails and text messages. Messages and attachments may contain viruses and links which can send you to dodgy websites containing malware that might infect your phone. Make sure you only click links and attachments if you are expecting them, or if they are from a trusted source.

7. **Check for software updates regularly**
   Install software updates to your phone as soon as they become available.
Office of the Privacy Commissioner
The Australian Privacy Commissioner is the national privacy regulator. The aim of the Office of the Privacy Commissioner is to promote awareness and protection of personal information. The Office performs key functions under the Australian Privacy Act 1988, such as providing information and advice about privacy, handling complaints, conducting audits, and undertaking promotional and educational activities. For further information about the Office, visit www.privacy.gov.au

Department of Broadband, Communications and the Digital Economy
The Department of Broadband, Communications and the Digital Economy maintains Stay Smart Online – www.staysmartonline.gov.au – a website that provides all Australians with information on the simple steps they can take to protect themselves online. The Department also has a program of cyber security awareness raising activities. Culminating each June in the annual National Cyber Security Awareness Week.

Australian Communications and Media Authority
The Australian Communications and Media Authority (ACMA) is responsible for the regulation of broadcasting, the internet, radiocommunications and telecommunications. For more information about the ACMA, visit www.acma.gov.au. The ACMA operates a range of cybersafety and cyber security education and awareness programs designed for children, parents and teachers. To learn more about these programs, visit www.cybersmart.gov.au

available. Updates correct errors in phone operating systems and often address security vulnerabilities.

It is also a good idea to back up the data on your phone before you update, in case anything gets lost. It is important to remember your phone is only as secure as the network and hardware you sync it with, so make sure they are up-to-date too.

It is important to delete all data from your phone before giving it away, throwing it away, selling it, recycling it, or returning a faulty phone.

8. Be careful of the wireless (Wi-Fi) networks you use

Use secure Wi-Fi networks that require passwords where possible. Do not conduct sensitive transactions such as banking or transactions involving sensitive passwords on public wireless networks – save these for when you are using a secure network. Set your phone to ask you before connecting to a new Wi-Fi network. Remember, even secure networks can have risks, so think before you click.

9. Don’t save passwords or PINs as contacts in your phone

With all the PINs and passwords we have to remember, it is tempting to save them in your phone as fake contents in case you forget them. Resist the temptation. You might feel like you have cleverly disguised the number or password, but this is the first place a thief will look. You would be surprised at how easy it can be to figure out.

10. Permanently delete all data from your phone when you throw it away

It is important to delete all data from your phone before giving it away, throwing it away, selling it, recycling it, or returning a faulty phone. It is not as easy as you might think to delete data from your phone. Often when you delete messages and files they are not permanently erased. To fully wipe your phone, you will need to follow the manufacturer’s instructions and make sure you remove your SIM card as well as any inserted memory card from your phone.

FOR MORE INFORMATION
➤ For more information about mobile phones and privacy, visit www.privacy.gov.au/topics/technologies
➤ For more information on securing mobile phones and using public wireless networks safely, visit www.staysmartonline.gov.au/secure-smartphone
➤ For more information about online safety and security for children, parents and teachers, visit www.cybersmart.gov.au

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
**PHOTOS AND SURVEILLANCE**

*A quick guide to the laws relating to using images and recordings of a person from the Office of the Australian Information Commissioner*

There are Commonwealth, State and Territory laws that relate to taking and using images of a person without their permission, or recording their conversations or movements. Which law applies will depend on the circumstances, in particular:

- Where the surveillance occurred or the photos were taken
- What was being monitored or photographed
- Who was responsible for the surveillance or images.

The Privacy Act does not cover individuals acting in a personal capacity, such as a neighbour taking photos of you.

For general information on State and Territory laws that relate to privacy – including surveillance and listening devices – see www.privacy.gov.au/law/states

**Someone has taken photos of me without my permission. What can I do?**

Consider contacting the police. The Privacy Act is unlikely to apply in this circumstance as it does not cover individuals acting in a personal capacity.

**My photo has been posted online without my permission. How can I get it removed?**

The first step is to ask the person who posted the photo to the site to take it down. If the person refuses, or you don’t know who it is, you may wish to contact the administrator of the site and ask them to remove the image.

If the photo was posted online by an agency or organisation, or the site is hosted by an agency or organisation that is covered by the Privacy Act, you may be able to complain to our Office.

For information on what agencies or organisations need to consider when posting photos to the web, see www.privacy.gov.au/faq/business/gen-q5

**There’s an image on Google StreetView that I feel breaches my privacy. What can I do about this?**

You should contact Google. Click the ‘Report a problem’ function available on the photo you are viewing on Street View to submit your request.

**Is my employer allowed to monitor my activities in the workplace?**

Some monitoring of staff activities in the workplace may be reasonable to ensure that staff are performing their duties and using resources appropriately. Where the monitoring includes retention of a record of the staff activity e.g. a CCTV video recording or a computer record of emails or a web surfing trail, then the privacy principles in the Privacy Act may apply.

Generally, monitoring of staff’s use of email, the internet and other computer resources, where staff have been advised about that monitoring, would be allowed. The Office has issued advisory guidelines on Workplace Email, Web Browsing and Privacy. These recommend steps that organisations can take to ensure that their staff understand the organisation’s position on this issue through the development of clear policies.

There are some other laws that deal specifically with the use of surveillance or listening devices. For example the Telecommunications (Interception and Access) Act 1979 (Cth) relates to rules around intercepting telephone communications. For some relevant State and Territory monitoring and surveillance legislation see www.privacy.gov.au/law/states

A FAQ regarding the recording or monitoring of telephone conversations is available at www.privacy.gov.au/faq/individuals/q1

**A photo of me has appeared in the media without my permission. Who can I complain to?**

The Privacy Act does not cover the acts and practices of media organisations in the course of journalism.

For information about complaints processes for media see:

- The Australian Press Council for print media
- The Australian Communications and Media Authority for television and the internet.

**Other places to go**

- A listing of Australian case law and legislation on privacy and surveillance can be viewed at www.austlii.edu.au/au/special/privacy
- For the relevant State and Territory surveillance legislation, go to www.privacy.gov.au/law/states
- If you think an agency or organisation has misused your personal information, you can make a complaint. To find out more, see www.privacy.gov.au/complaints
Being watched constantly is too high a price for safety

Our privacy matters very much, even when we have nothing to hide, observes Julian Burnside QC

The human instinct for privacy runs deep. All people have a need to be private, but privacy is not coherently protected in Australia, except in Victoria and the ACT.

Like most human needs, the desire for privacy has to yield to competing interests. Traders need our names and contact details; banks need our financial details; doctors need a lot of personal information; governments expect us to tell them our income and, of course, law enforcement agencies need all manner of information when investigating crime.

Balancing legitimate rights to information against legitimate expectations of privacy is a difficult and delicate task.

But just as a reasonable expectation of privacy has its limits, so also does the right of others to acquire information about us. Balancing legitimate rights to information against legitimate expectations of privacy is a difficult and delicate task. The difficulty increases as techniques for surveillance become more sophisticated.

The first CCTV surveillance camera in a city was installed at Olean, New York, in 1968. In 1981, a CCTV camera was installed in a major road leading into Melbourne. Its purpose was to help with traffic during a forthcoming Commonwealth heads of government meeting. It was a novelty that many did not welcome. It caused a high degree of anxiety – and not just among civil libertarians. The Victorian government assured the public that the camera would be removed after the meeting was over. It wasn’t.

All major cities now have thousands of CCTV cameras watching public spaces. They are so pervasive that most people have stopped thinking about them. In most cities in Australia, the average citizen is likely to be captured on film about 15 times a day. Like most civil liberties, the right to privacy is hard to regain when it has been lost. All we can do is preserve what little privacy is left to us. So beware the beguiling arguments of governments intent on knowing everything about you.

In Britain, there are more than 6 million CCTV cameras. Not many people seem to care, but it is worth reflecting that most of the cameras we see around town are monitored all the time. If the cameras were replaced by spies, we might react differently. Imagine a society in which the citizens were regularly watched by 6 million human observers. It sounds like East Germany under the Stasi, or the system of surveillance foreshadowed by George Orwell in Nineteen Eighty-Four.

Few governments would survive politically if they put an army of informers on the streets. CCTV cameras watch us all the time, but they do not cause the same fuss. When questions of privacy are raised, there are two standard answers. First: if you’ve nothing to hide, you have nothing to fear. And second: it is necessary to fight crime. Both arguments are wrong.

The argument that “if you have nothing to hide you have nothing to fear” goes to the heart of what the need for privacy is about. Privacy is not about hiding wickedness. It is an expression of the basic need to be left alone. Most people draw the curtains at night. It’s not because they have something to hide, but because they need to feel that they are not being watched. They are not trying to hide guilty secrets: they need to feel private.

Governments in Australia have never tried to justify the argument that CCTV cameras are necessary, or even effective, in reducing crime. It is as if the matter is too obvious to need proof. But in Britain, figures released last year showed that just one crime per year was solved for every 1,000 CCTV cameras in use. Some local authorities in Britain have justified the cost of installing CCTV cameras by saying that surveillance drives prospective criminals into other areas. In other words, they do not prevent crime, they simply move it elsewhere.

Let us suppose that the use of CCTV surveillance is effective to some extent in reducing crime. Let’s be more extravagant and assume, against the evidence, that CCTV surveillance is highly effective in reducing crime. Would that justify increased use of CCTV surveillance? Try this little thought experiment: a great deal of criminal activity happens at home – child abuse, spouse abuse, sexual assault and so on. We could reduce those forms of criminal conduct by a simple device. Let every room of every house in the land be equipped with a CCTV camera.

The argument that “if you have nothing to hide you have nothing to fear” goes to the heart of what the need for privacy is about.

Let the cameras all be connected to a large database, so that anything that happens anywhere in any house will be recorded. If a crime is committed, video evidence of it will be available.

The effect on crime figures is likely to be dramatic. But how many of us would support such an idea? We would all spend our lives knowing that some nightmare ministry was watching every detail.

This might reduce crime, but most people, I suspect, would think the price was too great. Because our privacy matters very much, even when we have nothing to hide.

First published in The Age, 5 July 2010
Governments have a duty to protect the rights, lives and safety of people within their territory from legitimate threats of terrorist attacks. However, protecting the community from terrorism and protecting human rights are not mutually exclusive. The Counter Terrorism White Paper makes this point clearly.1

Both have the ultimate objective of protecting and promoting the inherent dignity and safety of human beings.

In its 2010 Counter-Terrorism White Paper,2 the Government stated its intention to use or expand the use of certain national security measures such as a biometric-based visa system (using fingerprints and facial images), increased sharing of biometric data between government agencies and internationally, and increased border security measures, including body scanners at international airports.

In his December 2009 report to the UN Human Rights Council, the Special Rapporteur on Human Rights and Counter-Terrorism highlighted the erosion of the right to privacy that has occurred in the global fight against terrorism (the Special Rapporteur’s report).3 The Special Rapporteur identified certain measures as being potentially incompatible with the right to privacy, many of which are the very surveillance and border control measures proposed in the Australian Government’s White Paper.4

The Special Rapporteur provides a framework for protecting Australia from terrorism while simultaneously protecting the community from undue violations of privacy rights. In short, the Special Rapporteur urges States to assess how counter-terror laws, policies and practices that intrude on privacy are necessary and proportionate by implementing the following principles:

➤ Minimal intrusiveness: public authorities should exhaust the least intrusive techniques before resorting to others
➤ Restrictions on secondary use: public authorities should only use information for the purpose for which it was obtained, and should provide a legal basis for any reuse of information
➤ Oversight and regulated authorisation of access: states should establish independent scrutiny of surveillance practices and techniques to ensure accountability and proportionality
➤ Transparency and integrity: public authorities must be open about surveillance practices, and
➤ Effective modernisation: public authorities should use tools such as privacy impact assessments to ensure that new technologies are utilised appropriately and effectively.

The Special Rapporteur’s report is an opportunity for Australia to take the lead both nationally and internationally on national security and privacy issues.

➤ The Special Rapporteur recommends that the Human Rights Council take measures to create a new declaration on data protection and data privacy in light of the impacts of counter-terrorism measures.5 Australia has the opportunity to play an international leadership role in the development of a new international instrument for the protection of privacy.6

➤ Leadership by Australia on protection of privacy in the counter-terrorism context would reinforce two pillars of Australia’s bid for a seat on the UN Security Council, namely: building a secure future; and respecting human rights.7 It would also underline Australia’s commitment to the UN counter-terrorism conventions and protocols.8

➤ Protecting human rights and privacy in accordance with the Special Rapporteur’s report would bolster and enhance the Government’s aims and objectives as set out in the Counter-Terrorism White Paper, in particular:
  − Pursuing a principled and proportionate response to terrorism that promotes the values we seek to protect and ensuring that, in responding to terrorism, Australia meets its obligations under the ICCPR.9
  − Building resilience in our community by maintaining our open democratic society and supporting and protecting the values and freedoms from which all Australians benefit,10 and
  − Ensuring that domestic efforts to counter terrorism are informed by best practice models internationally.11

It is imperative that Australia act now because:

➤ There is growing concern about the privacy implications
of the development and use of new technologies, such as the collection of biometric data and the use of body scanners at airports.13 The measures proposed in the Counter-Terrorism White Paper have already raised concerns in the community about the impact on privacy.14

The legal safeguards of privacy in Australia remain limited. Neither the Australian Constitution nor any state or territory constitutions contain any express provisions relating to privacy. The unauthorised collection and disclosure of private information is only protected in a limited way, and intelligence agencies are generally exempt from these laws.15

Australia is bound by its international obligations to take all legislative, policy and other measures to properly respect the right to privacy in Australia.16

Over the last decade, the Australian Government has enacted almost 50 pieces of anti-terrorism legislation and the intelligence gathering and surveillance powers of intelligence agencies have been broadened significantly. In the absence of any comprehensive human rights framework there has been insufficient parliamentary or other scrutiny of the human rights impacts of these laws, including the right to privacy.17

RECOMMENDATIONS FOR ACTION

The Australian Government should become a world leader in protecting the rights of its people to be safe from both terrorism and from undue interference with privacy. The Australian Government should implement the report of the Special Rapporteur in the following ways:

International action

1. Australia should adopt the best practices and recommendations set out in the Special Rapporteur's report as the underlying principles of Australian policy in relation to counter-terrorism and privacy protection

2. Australia should champion the development of a new global declaration on data protection and privacy, working through the Human Rights Council, and in consultation with like-minded States.18

3. As an aspect of Australia’s candidacy for the UN Security Council, it should commit to further mainstreaming human rights considerations, including the right to privacy, in the work of the UN Security Council Counter-Terror Committee

4. Australia should support the development of a programme for global capacity building on privacy protection, with the intention of counterbalancing the global trend of counter-terrorism laws that infringe on privacy.19

Domestic action

For Australia to have credibility in its international position, it must ensure that its own house is in order. To that end, Australia should take the following steps to improve the protection of the right to privacy in domestic laws and policies:

1. The National Security Legislation Monitor should immediately review all counter-terrorism, intelligence gathering and surveillance laws to ensure that they are precise and proportionate to the security threat and contain appropriate safeguards against abuse.20

2. The Australian Government should strengthen privacy protection in Australian law, by ensuring that the law provides not only comprehensive data protection, but broader personal privacy protection, in a manner that reflects international human rights standards. Such a law could regulate, for example, the use of intrusive border control measures such as body scanners, and apply the principles of necessity and minimal intrusiveness.

To the extent it does not do so currently, the law should:

- Ensure that there are clear legal protections for individuals that prevent excessive collection of personal information
- Impose restrictions on secondary use of information and regulate the storage and sharing of information
- Require individuals to be notified of how information is used, and
- Provide rights of access and remedies for improper violations of privacy.

The Government might either expand the scope and function of the Privacy Act (Cth) or create a new stand alone privacy law.

3. In relation to Australia’s intelligence and defence intelligence agencies, the Government should implement the Australian Law Reform Commission’s (ALRC) recent recommendations by:
Requiring that the privacy rules and guidelines applicable to Australia’s intelligence and defence intelligence agencies be updated to include rules that deal with the incorrect use and disclosure by those agencies of all personal information, the accuracy of records and the storage and security of personal information

Requiring that the National Security Legislation Monitor, the Inspector General of Intelligence and Security, the Privacy Commissioner and the Minister responsible be consulted in the process of making the privacy rules and guidelines, and

Ensuring that the privacy rules and guidelines governing Australia’s intelligence and defence intelligence agencies be made accessible to the public.21

All current and new Government policies, including the policies contained in the Counter-Terrorism White Paper, should be subject to Privacy Impact Assessments (PIAs). The Government should implement the ALRC’s recommendation that the Privacy Commissioner be empowered to request and oversee PIAs and that the Privacy Commissioner produce guidelines to assist departments and agencies in the preparation of PIAs. 22

PIAs would:

Consider how the policy and any technologies used create privacy risks

Contain an assessment of the principles of proportionality and necessity in accordance with human rights standards, and

State measures taken to guard against abuse of privacy in the policy.

Assessments at policy development stage would also ensure that privacy is considered at the earliest stage of policy formulation. 23

The policies and practices of Australia’s security and intelligence agencies should be subject to particularly strong oversight given those agencies’ use of intrusive surveillance techniques and the processing of personal information. The oversight should take specific account of the proportionality of any intrusive measures and whether the intrusion on rights is the minimum necessary to achieve the security or intelligence outcome. Oversight should be as transparent as possible and should be conducted by an independent body that is properly resourced and has appropriate human rights and privacy expertise. Appropriate bodies to conduct this function may include the Inspector-General of Intelligence and Security, the Privacy Commissioner, the Information Commissioner or the Australian Human Rights Commission. Any decision made by that body should be subject to merits review in the Administrative Appeals Tribunal, with rights to appeal questions of law to the Federal Court.

6. Given that new technologies both enhance the ability of Australia to protect its people from terrorism but also threaten to violate privacy, the Government should invest in any features of new surveillance or other technologies that make the technologies less restrictive on the right to privacy.

The Human Rights Law Resource Centre is a leading national community legal centre. The Centre promotes and protects human rights in Australia. We contribute to the alleviation of poverty and disadvantage, and the promotion of equality and fair treatment.

ENDNOTES

1. The Counter-Terrorism White Paper clearly states that in responding to terrorism Australia is committed to meeting its obligations under the ICCPR (56), including the right to privacy (58).


4. The Special Rapporteur pointed to the global increase in stop and search powers; the increasing use of biometric techniques such as facial recognition, fingerprinting and iris scanning; the circulation of secret watch lists; and, increased monitoring, regulation, interference and control of movement at State borders.

5. Special Rapporteur’s Report, [73].

6. A number of countries have expressed positive interest in such a declaration, including China, Norway, France and Finland.

7. These are two of four pillars upon which Australia has built its candidacy: www.dfat.gov.au/un/unga.html

8. As expressed in the Counter-Terrorism White Paper: 56.

9. Counter-Terrorism White Paper, [3.2.4].


13. The ALRC stated that ‘rapid advances in information, communication and surveillance technologies have created a range of previously unforeseen privacy issues’. The introduction of body scanners created intense media scrutiny in January and February 2010, and drew condemnation from a broad range of stakeholders, including airlines, see www.theaustralian.com.au/travel/backlash-to-airport-body-scans/story-e6frg8sf-1225817485755


15. The Privacy Act 1988 (Cth) is the key federal law that protects against unlawful interference with personal information. Australia’s intelligence and defence intelligence agencies are either partially or wholly exempt from the operation of the Privacy Act. Acts of ASIO, ASIS and the DNA are completely exempt by virtue of sections 7(1)(a)(b) and (2)(a) of the Privacy Act.

16. Australia is a party to the ICCPR. Article 17 of the ICCPR protects the right to privacy.

17. There is bipartisan recognition of the need to review and possibly recriminalise the relationship between counter-terror measures and privacy: see, e.g. the Hon Joe Hockey MP, ‘In Defence of Liberty’, Address to the Grattan Institute, Melbourne, 11 March 2010 at http://joehockey.com/useruploads/File/InDefenceOfLiberty.pdf

18. This is the Special Rapporteur’s recommendation at [73].

19. See Special Rapporteur at [72].

20. This reflects the recommendation of the Special Rapporteur at [60].


22. Ibid, recommendations 47-4 and 47-5.

23. See Special Rapporteur at [63] and [67].

Human Rights Law Centre
www.hrlc.org.au
Every day we leave our digital fingerprints all over the online world. How much of it should be available to police and intelligence services without a warrant? Commentator Stilgherrian discusses if Australia accedes to the Council of Europe Convention on Cybercrime as the Government intends, the answer is shiploads. Our politicians seem incapable of balancing our civil liberties against continual demands for more surveillance.

The convention is the first international treaty on crimes committed via the internet, and so far it’s the only binding one. It started as a European initiative in 2001, entered force in July 2004, and since then a total of 43 nations have signed on, including Canada, Japan, South Africa and the US.

More than 100 nations are using the convention as an example to help them strengthen their own legislation.

On 30 April 2010 the Australian Government announced its intention to join too. In February 2011 the Attorney-General’s Department kicked off the necessary public consultation.

Now as more and more of our everyday lives are conducted online, crime has moved there too. The internet’s cross-border nature means that law enforcement agencies need cross-border arrangements. Clearly they need new tools, and the convention contains plenty of good stuff about creating a framework for cooperation, facilitating information exchange and setting up 24/7 mutual-assistance hotlines for investigators.

There’s also quite reasonable requirements like criminalising attacks on internet infrastructure, hacking into systems or disrupting them – although those acts are already crimes in Australia. No one would disagree with criminalising ‘content-related offences’ when that vague term in the covering notes is attached to the phrase ‘including child pornography’. And while some might disagree with the convention requiring copyright and trademark infringement to be criminalised, again such things have already been turned into crimes in this country, so it’s not unreasonable for online laws to match.

Our politicians seem incapable of balancing our civil liberties against continual demands for more surveillance.

Indeedy, one of the key arguments in favour of acceding to the convention is that it helps apply the same rules to online communications as already apply to traditional telecommunications.

Take the telephone. In Australia, under powers granted by the Telecommunications Act, police can routinely access your telco’s call records – the numbers you called and when. To further invade your privacy and listen to the contents of a phone call requires a warrant signed off by a judge.

Similarly, goes the explanation, under the requirements in the convention’s handy companion document, the European Directive on Data Retention, internet service providers (ISPs) would maintain records of your online communications for later access by law enforcement. This includes matching a specific internet address to the customer using it at the time, records of email sent and received, records of which websites you visited and when, and so on. For the police to access the contents of your email, or see specifically which pages of a website you visited, or monitor live internet traffic – all that would still require a warrant.

“I think people need to realise that there isn’t a great deal of change from the current status quo. Australia as a jurisdiction would be 90-95 per cent compliant with Council of Europe recommendations,” cybercrime specialist Nigel Phair told the 7 March edition of the Patch Monday podcast.

However digital rights advocacy group Electronic Frontiers Australia thinks the convention is a terrible document. Just one concern is that it would criminalise the selling of tools that could be used for cybercrime, yet are often the very same tools used by systems administrators to ensure the security of their networks.

“Do we want to end up in a situation where police are able to get in and monitor the internet activity of any Australian based on an Albanian warrant?” EFA vice-chair Colin Jacobs
told ABC Unleashed.

"And we don’t think police have yet made the case that a database of all our communications activity really needs to be kept whether or not we have been suspected of a crime."

Personally, I’m not convinced all this is such a simple mapping of traditional procedures onto the internet either.

Australia Post doesn’t keep a record of every letter and postcard you send and receive. Libraries don’t record who comes in to read books. Convenience stores don’t record the names of everyone who pops in for milk and a packet of fags. No one records the names and addresses of people pausing on a street corner to have a chat. Yet now, for the equivalent activities on our digital streets, that’s precisely what is being proposed.

The Government’s attitude to all this can be further divined from three facts.

First, how many times does the Attorney-General’s Department’s discussion paper mention the word privacy? Zero. And while it notes that powers and procedures developed to conform to the convention should provide for “the adequate protection of human rights and liberties”, this point isn’t discussed and further.

Second, the convention requires that the information gathered under ISP data retention be kept for 90 days. The Attorney-General wants it kept for a full year – although it must be said that there’s an argument for that. “Not every law enforcement investigation is kicked off in 90 days, and if you don’t have the retained data often that is critical,” Phair said, who would personally prefer a two-year retention period.

Third, the Government continues to extend the powers of law enforcement and intelligence agencies without public debate and without any counterbalancing extension to the oversight. ASIO’s powers have been extended at least twice during 2011 alone, with The Greens’ attempts to introduce oversight blocked with the now-standard excuse that such measures would “reveal operation details”. The Coalition is no better: they didn’t ask a single question during the entire Senate debate. They didn’t even ask for a cost benefit analysis.

In June 2011, the Government introduced the Cybercrime Legislation Amendment Bill 2011, intended to change our laws so that we can accede to the Council of Europe Convention. The discussion paper’s requirement for ISPs to log everything was dropped. Instead, police can issue ISPs with a retention order, requiring them to start logging the data for specific, named customers. Police can only access this information with a warrant.

Despite this clear improvement, a parliamentary committee found that the Bill has major problems. The committee’s recommendations were ignored. However the government has to move a few technical changes because the Bill was so hastily drafted that they’d left out key requirements for accession to the Convention.

The Cybercrime Legislation Amendment Bill has already passed third reading in the House of Representatives. The final third-reading debate in the Senate will be the last chance for fixes.

Increasingly, we are simply recording data because we can and because it costs next to nothing, from car number plates using a freeway to the location of mobile phones. Simply because the data is there, law enforcement agencies want access. Sure, it’d be convenient. But in an age when we’re already the safest we’ve ever been and, tabloid beat-ups notwithstanding, crime levels are steadily falling, is the trade-off worth it?

And why aren’t our politicians considering us citizens and our rights?

Stilgherrian is a freelance journalist, writer, commentator and producer with a strong interest in information security and cybercrime issues.

No one records the names and addresses of people pausing on a street corner to have a chat. Yet now, for the equivalent activities on our digital streets, that’s precisely what is being proposed.
1.1 INTRODUCTION

Privacy issues in the communications sector are increasingly prevalent as new technology and new applications enter the market, such as social networking and the use of location-based information. These new technology privacy issues add to the existing privacy issues in the sector, such as spam, telemarketing and the misuse of silent telephone numbers.

Complaints are a vital element in privacy protection – indeed, the entire system of privacy protection in the communications sector is built on the receipt and management of complaints.

There are few proactive requirements to protect privacy in the sector, and the volume and scale of business in the sector is so large that no regulator could hope to monitor compliance without relying heavily on complaints. Proactive steps are necessary and crucial, but this report focuses on complaint paths.

The aim of this study is to analyse and compare common communications privacy complaint paths in order to obtain optimum outcomes for consumers through the development of a more straightforward, fairer system for managing privacy complaints in the sector.

1.2 METHODOLOGY

This study examines and compares three commonly used complaint paths for privacy complaints in the Australian communications sector:

1. Complaints to the Office of the Privacy Commissioner (OPC) – typically general privacy complaints, telemarketing complaints and internet-related complaints
2. Complaints to the Australian Communications and Media Authority (ACMA) – typically spam and Do Not Call complaints, plus a small number of general privacy complaints

The study has included the collection of data and case studies from the three complaints bodies, plus interviews with key staff and a brief survey of community organisations who assist complainants. A more detailed description of the methodology is contained in Appendix 1 of Communications privacy complaints: in search of the right path.

The communications sector generates around 21,000 privacy complaints each year, although these are not evenly spread across the three complaints bodies.

1.3 KEY FINDINGS AND RECOMMENDATIONS

All three complaint paths receive hundreds of privacy complaints each year from consumers of telecommunications and internet products and services. Despite the similar nature of privacy complaints, the outcome for both consumers and industry varies to a significant degree, depending on the complaint path chosen by the consumer.

This study has found that there is disparity in complaint numbers across complaint bodies. The communications sector generates around 21,000 privacy complaints each year, although these are not evenly spread across the three complaints bodies. The Australian
Communications and Media Authority receives around 16,000 communications sector privacy complaints and the Telecommunications Industry Ombudsman receives around 5,000 communications sector privacy complaints. The Office of the Privacy Commissioner only receives around 110 communications sector privacy complaints despite its broad and in some cases unique jurisdiction, high profile and significant resources.

Any privacy complaint in the communications sector lodged with any complaints body should be able to achieve all of the outcomes that are desirable in a best practice regulatory environment.

In some respects the three complaints bodies treat the management of communications sector privacy complaints as if the three regulators were acting as a single entity. For example, a complaint to one regulator may preclude the individual from complaining to any of the other complaints bodies, yet there is only a system of informal referrals between them. However, in many other respects, the three complaints bodies act independently, and display very different approaches to complaints management.

The study has found that there is inconsistent resolution times and process issues. A significant disparity exists, for instance, in the complaint resolution times between the Office of the Privacy Commissioner and the other complaints bodies. Further, information given to potential complainants can be inconsistent and ad hoc, and complaint services challenging to access. In terms of action on complaints, the complaint bodies differ again on the range and focus of remedies employed. Some remedies focus to varying degrees on resolution for consumers, including compensation, and others to varying degrees on business conduct.

These and other factors result in inconsistent and diverse outcomes for consumers depending on the complaints path they have selected, or the path that has been chosen for them by jurisdictional issues. This situation is unacceptable and is not delivering efficient or effective regulation of privacy complaints in the sector. It is not the result of a careful or planned policy decision to treat communications privacy complaints in this way. It is the result of ad hoc complaints processes, overlaps in jurisdiction, and the individual culture and approach of the three complaints bodies.

This study therefore makes a number of recommendations aimed at delivering a more consistent and higher quality outcome for all privacy complaints in the communications sector.

These include (see Section 10 of Communications privacy complaints: in search of the right path for full details):

- Improvements in complaint resolution times, specifically by the Office of the Privacy Commissioner
- Frank and consistent information given to consumers, especially regarding resolution times
- Collection of demographic profiles of complainants to better target services
- Better coordination between the three complaints bodies
- Consistent messages to complainants on where to complain, and to industry on compliance
- A full range of regulatory tools and remedies on offer and used – any privacy complaint in the communications sector lodged with any complaints body should be able to achieve all of the outcomes that are desirable in a best practice regulatory environment:
  - Compensation for the individual
  - An apology for the individual
  - Prompt correction or removal of personal data
  - A change to business practice at the individual company
  - A change to broader industry practice for systemic issues
  - Occasional naming of individual companies as a warning to other consumers and a lesson for industry, and
  - Occasional enforcement action in order to promote compliance.

Executive summary from Communications privacy complaints: in search of the right path, published in 2010
Cyberspace Law and Policy Centre | www.cyberlawcentre.org
Reaction to the widening News of the World scandal has again highlighted the lack of protection against invasion of privacy by the media in Australia.

Former Prime Minister Paul Keating renewed his attack on the Australian print media’s self-regulation calling it a joke and suggested that rather than have a right to appeal to a body funded by print organisations, the Australian Press Council, they should have a legal remedy.

The United States has had a legal remedy for invasion of privacy for many years, and the United Kingdom – notwithstanding the current crisis in confidence in the Murdoch media – has seen some celebrities successfully sue newspapers over privacy invasion and others attempt to prevent material from being published about them by legal means.

Australia has no law guaranteeing an individual privacy against a media ever-so-willing to intrude into their private lives. This is perhaps difficult to understand, given that politicians are often the ones on the receiving end of the media’s unwanted attention.

While an argument can be made for exposing politicians’ immoral behaviour on the basis that if they cheat on their spouse they might bring the same morality into their public life, the argument carries little weight when applied to justifying intrusion into the private lives of celebrities, like sportspeople and those from the arts, like actors, authors or singers.

The Journalists’ Code of Ethics contains only one reference to respecting privacy, calling on journalist members of the union to “Respect private grief and personal privacy” adding that they have a “right to resist compulsion to intrude”.

But this clause has more to do with the ‘death knock’ where a journalist seeks information from a grieving family than it does to considering the privacy of an individual or celebrity. There are similar clauses in various media codes of practice, but they mean little when the media is camped outside a person’s home reporting and recording their every move.

Journalists do not enjoy a high reputation for honesty and ethics. The latest survey of professions by the Roy Morgan polling organisation showed only 11 per cent of respondents thought print journalists were honest and ethical.

The figure for TV journalists was not much higher – 16 per cent. A recent international survey of 127 journalists in 46 countries, including Australia, found that most faced ethical dilemmas at work and most admitted to having behaved unethically. They blamed, among other things, internal pressures from their editors and employers for their behaviour.

Since the advent of the 24-hour television news services like Skynews and the ABC’s News 24, immediate
access to news through innumerable sites on the internet, the circulation of information via Twitter and Facebook, and the fact that everyone with a phone can be a citizen journalist, the traditional role of the newspaper as the “first draft of history” has changed. More newspaper content these days consists of background of the already-known news of the day and opinion pieces from a raft of journalists and commentators. At the tabloid end of the media scale often this amounts to entertainment in the form of the latest celebrity scandal.

In 2008 the Australian Law Reform Commission recommended a statutory right to privacy, and suggested that the Privacy Act be strengthened to require the media to deal with privacy issues.

Since then there have been a number of invasions into the privacy of individuals, like the ‘outing’ of New South Wales politician David Campbell and revelations about another NSW politician, John Della Bosca. But while there may be a case in some instances for exposure of such conduct for the reason mentioned above, what possible reason can there be for the media’s hounding of various celebrities? For a fortnight in March, 2010, Australia’s media followed every move by that nation’s “sporting royal couple”, Australian cricket vice-captain Michael Clarke and bikini model Lara Bingle as their engagement unravelled. (The author has been investigating the newspaper coverage of the incident as part of his doctoral research).

Clarke rushed home from a tour of New Zealand to be with Lara after a partially-nude photo of her appeared in a weekly gossip magazine. Between then and his raising his bat in triumph after scoring a hundred in a test match back in New Zealand nearly two weeks later, the capital city newspapers in Brisbane, Sydney, Canberra, Melbourne and Adelaide had written about the break-up (and used it as cartoon fodder) about 230 times.

While newspapers argue media freedom is a cornerstone of a democratic society, with that freedom to publish comes the responsibility not to abuse it.

At a time when the young couple deserved some privacy, they dominated the news not only in print, but also on TV, radio and the internet (and social networking sites). Although they are both public figures, even they deserved some privacy at that time.

As a journalism ethics lecturer at Bond University, this author often asks students: “How would you feel if such material was written about you, or someone you care about?” It is a question many tabloid journalists – including television current affairs journalists in that category – appear to give scant thought to.

Much of this reporting is not telling the public what “they need to know”, but rather what “they want to know”. Because celebrity scandal and gossip is supposedly popular with the public, does that mean the media needs to continuously cater to that popularity? Because the public attends the game, buys the book or CD, or attends the sell-out concert, does that give them the right to know every detail of a celebrities’ private life?

The News of the World built their circulation on celebrity scoops, but they have been caught out going too far in catering to their audience’s perceived interest in gossip and scandal. No one has suggested that the sort of activities undertaken by the NorW reporters to get stories (phone hacking and paying for telephone numbers etc.) are being used in their sister publications in Australia.

The concentration of ownership of newspapers in Australia – or put another way, the dominance of the Murdoch mastheads across the country – mitigates against the intense competition and “get the story at all costs” culture of the British tabloids.

News Limited’s Chairman and Chief Executive in Australia, John Hartigan, has said he is confident practices like those exposed in the News of the World scandal have not occurred in Australia, and has ordered a review of editorial spending over the past three years to confirm that payments made to third parties were for legitimate services.

The leader of the Greens, Senator Bob Brown, whose party often feels the sting of News Limited attacks on their policies, has suggested a Senate inquiry into media ownership and journalism ethics.

While the newspapers argue media freedom is a cornerstone of a democratic society, with that freedom to publish comes the responsibility not to abuse it by, among other things, unwarranted invasion of individual’s privacy.

The News of the World scandal might provide added momentum to the push for a legal remedy for privacy invasion. A balance needs to be found addressing genuine public concern about invasion of privacy and further media regulation.

Roger Patching is Associate Professor of Journalism at Bond University.

Published in The Conversation, 20 July 2011
http://theconversation.edu.au

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
What happens when you extend the idea of public interest to privacy?

Andrew Dodd from Crikey examines the government’s proposed laws and how they might address the ‘public interest’ versus personal privacy

It is totally unsurprising the News of the World scandal in Britain has triggered the likely introduction of privacy laws in Australia.

For several years the Australian media has been anticipating this day, and is almost psyched ready for some loss of freedom in this most vexed area of media law.

Today Justice Minister Brendan O’Connor announced the “government will seek the views of the public on introducing a right to privacy in Australia”. That’s a polite way of saying it will legislate to create a statutory tort for breach of privacy, paving the way for the public to sue the media for foot-in-the-door and other intrusive forms of journalism.

The idea hasn’t come out of nowhere. It has been on the table since the Australian Law Reform Commission made this recommendation, along with 294 others, in a wide-ranging review of privacy in 2008.

Although the government concedes there are already adequate laws to prosecute phone hackers, it’s grabbing the moment while News Limited is so unpopular to push for this as well. Or as O’Connor’s media release put it: “We know that privacy is a growing concern for everyday Australians – whether it is in our dealings with individuals, businesses, government agencies or the media.”

Former prime minister Paul Keating made the call for privacy laws following the News of the World scandal. He told Lateline last week:

“Well there’s one thing that’s clear for sure comes out of this and that is self-regulation by the media is a joke. A joke. You know, I notice tonight John Hartigan talking about the Press Council of Australia. I mean, people shouldn’t have a right to appeal about invasions of their privacy to some body funded by newspapers; they should have a right at law.

“What we need, what we seriously need, which has been now recommended by the Commonwealth Law Reform Commission, the Victorian Law Reform Commission and the New South Wales Law Reform Commission is a separate right-of-action in privacy, a separate tort.

“So in other words, you don’t have a right of appeal to some body, you have a right to action, you have a right to the law. In the end, the only regulator of this bad behaviour is the law.”

Michael Gawenda of the Centre for Advanced Journalism at the University of Melbourne says he has mixed feelings about privacy laws but is ultimately opposed to them. He concedes it is a difficult and vexed area but he believes the emergence of new media makes the job of framing and enforcing privacy laws extremely difficult.

“We live in a landscape where it is almost impossible to see how they’d be enforced,” he said. “There is a new generation for whom the notion of privacy is completely different to what it was a generation ago.”

The government has promised to release a discussion paper on the issue, which will address some of the privacy challenges posed by social and online media.

The new laws will inevitably include a public interest test, meaning reporters will need to demonstrate some public good is derived from intruding on someone’s personal privacy. This means the public will claw back some of the rights it lost with the introduction of the uniform Defamation Act in 2006. Under the old laws the media in several states had to prove there was a public interest for defaming someone. But since 2006 the media has not had to stop and ask itself the fundamental question: “Does the public really need to know this stuff?” Truth alone is now a defence in defamation actions.

So what happens when you extend the idea of public interest to privacy? Gawenda says the problem with a public interest test is who defines it? “It is a very slippery term.” Does it mean what the public is interested in? Who will define it and how will the legislation define it? Do we want lawyers or judges to define it?

He asks rhetorically: “Were the revelations in the WikiLeaks documents in the public interest? Lots of politicians said they weren’t.”

The new laws will also build on some heavy-duty case law in recent years. In the 2007 case of Jane Doe versus the ABC, the Victorian County Court upheld an action for breach of privacy from the victim of a sexual assault because the ABC had identified her in several radio news bulletins. The judge felt emboldened to make the ruling because the High Court had effectively invited lower courts to do so in the 2001 case of Lenah Game Meats versus the ABC.

The state and federal law reform bodies have also joined in with recommendations that the parliaments legislate to create a tort enabling people to sue. Since then media company lawyers have been advising their clients to be very careful, especially when the victim has a “reasonable expectation of privacy”.

So if the proposed law codifies ethical and professional practice it would probably be good for all concerned. But if the government is seizing the opportunity provided by the News of the World to erode the legitimate rights of the media to report openly, then that would be a very bad thing indeed.

Dr Andrew Dodd is a Senior Lecturer, Faculty of Life and Social Sciences at Swinburne University of Technology, Hawthorn, Melbourne.

How the media will react to a right to privacy

So, nearly three years on from the original Australian Law Reform Commission report recommending a statutory right to privacy, the government is finally moving, albeit slowly, towards adopting it, with a ‘public issues paper’, reports Crikey’s Bernard Keane.

No one could accuse the government of rushing things, but in fairness to Brendan O’Connor, who is the first Minister for Privacy, the ALRC report on privacy was a magnum opus, with 74 sets of recommendations, and the government is already dealing with many of them (197 individual recommendations) with the first tranche of its response. Having waited this long, the government has correctly seized on the phone-hacking debacle to go on the offensive.

The mainstream media (honourably excepting the ABC’s Mark Scott) are virtually alone in opposing a right to privacy, and will offer two reasons.

The first is that a right to privacy automatically clashes with freedom of speech. This has been repeated so often that any debate is already heavily skewed in favour of the media. But rights always have to be balanced against each other, as the rights to privacy and free speech are in the European Convention on Human Rights. The media doesn’t argue for an absolute right to free speech elsewhere – indeed, News Ltd, for example, has adopted a habit of taking legal action and threatening legal action to curtail others’ right to free speech where it threatens the company. And the media voluntarily self-censors on matters such as suicide, where they accept that harm may result from certain types of free speech. Virtually no one argues for an absolute right to free speech – we all accept limits in areas such as defamation or causing harm, even if we debate where those limits should be.

So asserting that a right to privacy is at odds with a right to free speech isn’t an argument that gets us very far: the issue is how those rights, like other rights, are balanced. The ALRC proposal sets the bar on a right to privacy very high, proposing that only actions that are “highly offensive”, and where a person has a “reasonable expectation of privacy” be captured, and that a public interest test apply.

But the ALRC also recommended that the list of remedies available to plaintiffs include injunctions, raising the prospect that injunctions could be used to prevent publication even of material that is defensible under the law. That’s not a new threat – pre-emptive injunctions are already used to try to silence media outlets – but extending it is a problem. This will be a key section of the government’s discussion paper.

The clearest problem about the purported conflict between a right to privacy and a right to free speech can be seen in the UK. There is no statutory right to privacy in the UK, but courts have extrapolated one from the Human Rights Act, which imposed on public institutions a requirement to observe a right to privacy. In doing so, they have inflicted significant collateral damage on free speech, including via super-injunctions. That is, a failure by the British Parliament to debate and establish a narrowly framed right to privacy has seen judges go off and create their own, without any of the protections of policy making or public debate.

The second argument the media will run is that a right to privacy will merely be used by the wealthy. The sleight-of-hand with this argument is that it assumes that the legal system isn’t already comprehensively biased towards those with the financial resources to go to court. Other rights aren’t curtailed simply because it’s easier for the wealthy to exercise them – you don’t see the media campaigning against the right to private education, for example, just because it’s easier for the wealthy to exercise it. And again, what’s been the UK experience? What has led judges to make common law about a “right to confidentiality” on the run? The very expensive legal actions of Naomi Campbell, Michael Douglas and Catherine Zeta-Jones and innumerable soccer players covering up their affairs with glamour models.

But just to play devil’s advocate, if the mainstream media want an argument to run with, they could do worse than point out the hypocrisy of a government willing to extend a right to privacy in relation to the media, but engaged in a rolling campaign to restrict privacy elsewhere. The recent and unexplained extension of ASIO’s surveillance powers regarding foreign intelligence will soon be followed up by Cybercrime Legislation Amendment Bill 2011, designed to enable Australia to accede to the Council of Europe Convention on Cybercrime, described by US civil liberties groups as “the world’s worst internet law” because of its potential to require states to restrict online behaviour that is legal in their country but illegal somewhere else (although there’s a carve-out for political activity).

The Bill will allow ASIO and the AFP – subject to some limited safeguards – to demand ISPs and telcos preserve non-content user data, such as billing records, and content such as emails, voicemail and SMSs, and to do so on the request of foreign law enforcement agencies. Rupert Murdoch’s companies may not be allowed to hack your voicemail, but the AFP will be able to do so at the request of foreign government.

Meanwhile, the attempt by the US government, at the behest of copyright cartel, to impose draconian copyright restrictions on other countries via the Trans-Pacific Partnership treaty under negotiation continues.

These issues won’t get a look-in during the ensuing debate over a right to privacy, of course. But a government that can invade your privacy poses a greater threat than any media company.

First published in Crikey, 21 July 2011
www.crikey.com.au
Every so often there’s a scandal that captures the attention of not just a nation but the world. The News of the World phone hacking drama is making people across the world sit up and think about their own media landscape: what’s acceptable and what’s not.

And it’s not surprising that this reprehensible behaviour by some sections of the overseas media is receiving so much public interest.

The invasion of one’s privacy is a very personal attack. If you’ve had someone invade your privacy, you’ll be familiar with the overwhelming feeling of violation.

Privacy is undoubtedly a growing concern for everyday Australians, whether it is in our dealings with individuals, businesses, government agencies or the media.

Privacy is emerging as a defining issue of the modern era, especially as new technology provides more opportunities for communication, but also new ways to compromise our private information.

Right now, when a person believes there has been some misuse of their personal information, the Privacy Act provides an avenue for complaint to the Australian Information Commissioner, who can ask individuals or businesses to address a privacy breach.

There are also laws in place that cover certain types of privacy violations; for example, the Telecommunications (Interception and Access) Act outlaws phone tapping and other misuse of communications services.

But there is no general right to privacy in Australia, and that means there’s no certainty for anyone wanting to sue for a breach of privacy.

The recommendations of the Australian Law Reform Commission report on privacy supported additional privacy rights, including a statutory right to privacy. The government will release an issues paper soon to progress the debate.

The debate will necessarily involve talking with the media, as well as with interest groups and the public. Critical to achieving robust and effective privacy protection is balancing the public’s right to know with our individual right to privacy. These ideals can sometimes pull in opposite directions and striking the right balance may not be easy.

This government believes in a free media and freedom of expression, and we also believe in the right to a private life. For us, this debate won’t be about curbing the rights of the media but enhancing the rights of us all. I believe there is strong support for the introduction of a clear right to privacy and, if introduced, I believe we can grant greater certainty to Australians about how their personal information is accessed and used.

The great irony, of course, is that a newspaper famed for its coverage of scandal is the greatest story of scandal in the world. But maybe there’s a silver lining: greater privacy protection for us, thousands of kilometres away from the pages that sparked the change.

First published in The Australian
21 July 2011
During the last three years, the federal, NSW and Victorian Law Reform Commissions have all concluded that a statutory tort is necessary to deal with aspects of privacy that are currently unprotected in Australia.

Previous attempts at a reasoned discussion of the proposals have been thwarted by firestorms unleashed by media outlets. On July 21, the federal government took the opportunity provided by widespread revulsion at phone-hacking by journalists in the UK to announce a discussion paper to build on the 2008 Report of the Australian Law Reform Commission.

The Australian media reacts with vitriol when they judge, or just imagine, that their freedom to gather and publish information is under threat. The News Limited stable often leads the charge, and this week has filled pages with articles on the government’s proposal and loosely related topics. There are myths in the debate that need to be corrected …

The Australian media reacts with vitriol when they judge, or just imagine, that their freedom to gather and publish information is under threat.

THE TORT IS TARGETED AT THE MEDIA

A primary misrepresentation is that the tort is targeted at the media. Yet, in discussing the scope of the right of action, the ALRC, at multiple points, makes clear that the scope is very wide. For example:

“… the types of acts or conduct that could constitute an invasion of privacy … include where there has been a serious interference with an individual’s home or family life; an individual has been subjected to unauthorised surveillance; an individual’s correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; and sensitive facts relating to an individual’s private life have been disclosed.”

Interviews published in The Australian itself have disclosed that “the recommendation to establish a legal right to privacy [is] not just about the media” and “[the ALRC] took pains to emphasis [sic] the media were not a particular target for the recommended course of action for a serious invasion of privacy”.

THERE IS NO EVIDENCE OF A PROBLEM

As everyone in the debate agrees, the role of the media is rather special. But the second misrepresentation that has been perpetrated is that there is no evidence of abuses by the media that need to be addressed. This has been raised in various forms, including this editorial in The Oz:

“… neither Mr O’Connor nor any other minister has been able to cite a case in which the media breached individuals’ privacy … [O’Connor is] floating hypothetical examples of how Australian newspapers could invade individuals’ privacy, because he has no real examples.”

Yet Media Watch had no trouble finding prominent people to use as examples, nominating Lara Bingle, David Campbell, Candice Falzon, Jess Origliasso, Nick Riewoldt and Sonny Bill Williams. And that list omitted several others that come quickly to mind, such as Andrew Ettinghausen, Pauline Hansen and Nicole Kidman, plus myriad tabloid radio and television programs that have ignored “the public interest” and pandered to “what the public might be able to be interested in”.

Media commentator Richard Ackland was in no doubt, as long ago as February, that the Campbell breach by Channel Seven was alone sufficient to tip the balance.

THE TORT IS UNSAFE AT ANY SPEED

A third cluster of unreasonable accusations depict the proposal as being unsafe in various ways. A particularly egregious misrepresentation is “as the ALRC has argued previously, the concept of a general tort of privacy is vague and nebulous”. The full quotation from the ALRC is:

“In its later report, Privacy (ALRC 22), the ALRC declined to recommend the creation of a general tort of invasion of privacy. In the ALRC’s view at that time [1983], ‘such a tort would be too vague and nebulous’.”

PRIVACY EYE: MEDIA PARANOIA DISTORTING FACTS ON PRIVACY TORT

Australians all believe in the freedom of the press as much as the media, observes Roger Clarke, chair of the Australian Privacy Foundation.
Michael Stutchbury has teleported a statement across a 28-year gap to provide spurious support to his contention. Further, as pointed out in a blog post by barrister Peter Clarke, Stutchbury justified his argument by distorting comments by a Chief Justice.

The ALRC’s proposal was first depicted as “unreasonable”:
“It would be better if the media worked with government to help propose a reasonable law, with robust mechanisms to allow for the full and proper protection of the public interest.”

Then the proposal was lambasted as being “an extremist ‘tort of invasion of privacy’” and part of “an extremist rights agenda”.

All of this appears to be intended to justify a claim that the tort would seriously harm freedom of the press. But in fact, the ALRC took great care to identify the competing interests, to place great weight on freedom of the press, to place the onus of proof very firmly on the claimant, and to structure multiple, high hurdles.

The ALRC settled for “characterisation of the cause of action” as a “serious invasion of privacy” that is “highly offensive to a reasonable person of ordinary sensibilities”. How high the bar is set is indicated by the example that “disclosure [by a medical practitioner] of the claimant’s HIV status will not be ‘highly offensive’”. The design of the ALRC’s tort ensures that only the most extreme or repeated actions will result in a case even getting off the ground. How can even the term “unreasonable” be justified, let alone the highly pejorative tag “extremist”?

THERE IS NO PUBLIC INTEREST DEFENCE
But perhaps the prize for the most blatant misrepresentation should go to The Australian’s Legal Affairs Editor Chris Merritt:

“The inclusion of a public interest defence will allow the media to publish material that would otherwise be a breach of privacy so long as it concerns a matter that is in the public interest.”

So the implication is clearly conveyed that the ALRC’s proposal does not include a “public interest defence”. That impression is reinforced by the statement: “The only defences under the ALRC scheme would have enabled the media to avoid liability if it published private material while relying on a legal right such as privilege.”

Even the minuscule number of people familiar with this small segment within the ALRC’s lengthy report would have easily fallen for this one.

It’s technically true that the list of ‘defences to the statutory cause of action’ does not include “the public interest”. But that expression is a term of art in this context.

The ALRC explained that:
“Rather than attempt to protect other rights through a defence, the ALRC agrees it would be better in principle and in practice to add an additional element to the cause of action for a serious invasion of privacy. This would ensure that privacy interests are not privileged over other rights and interests” (74.147).

That explanation is difficult to overlook, because it is repeated in the discussion of the defences: “the ALRC considers that the defence of disclosure in the public interest or fair comment on a matter of public interest should form part of the elements of the cause of action” (74.170).

In short, the claimant can’t establish that they have a case unless they convince the court that “the claimant’s privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression)”.

The ‘defence’ that Merritt pretended doesn’t exist is there alright – up front, rather than down the back end.

The media as a whole have got to get over their desperate paranoia. Your worst enemies aren’t actually out to get you. We all believe in the freedom of the press as much as you do.

Ultimately, the privacy right of action has been a long time coming. The need for a tort has been discussed in learned reports and articles since the 1960s. The ALRC proposed a tort of “unfair publication” in 1979. In 1987, the (then Liberal-dominated) Senate passed an amendment to the Privacy Bill to provide for a (limited) action for breach of privacy; it was rejected by the (then Labor-dominated) House of Representatives.

Moreover, International Covenant on Civil and Political Rights (ICCPR) – which Australia signed in 1972 and ratified in 1980 – arguably obligates us to provide legislative protections for all forms of privacy, not just data privacy, and a tort of this kind is one straightforward way to achieve some level of compliance. I wish I, as an individual, could deliver on my obligations over 30 years late.

The media as a whole have got to get over their desperate paranoia. Your worst enemies aren’t actually out to get you. We all believe in the freedom of the press as much as you do.

And The Australian, of all of the News Ltd outlets in Australia, needs to stop compromising broadsheet standards and get back to the quality journalism that newspaper devotees expect. (We’re still here, still reading).

Roger Clarke is a 40-year veteran of the IT industry, and Principal of Xamax Consultancy. For the last 20 years his consultancy focus has been on strategic and policy aspects of advanced technologies. He is a Visiting Professor in the Cyberspace Law & Policy Centre at the University of NSW, and a Visiting Professor in the Research School of Computer Science at the Australian National University. He has also been active in consumer and privacy advocacy since the 1970s, and is currently chair of the Australian Privacy Foundation.

First published in Crikey, 1 August 2011
www.crikey.com.au

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
How do we protect privacy in the digital age?

The culture of over-sharing personal information on social networking sites presents the greatest challenge to privacy, observes Thomas Tudehope

There is a compelling case for a considered debate on the need for privacy laws in Australia. Rather than trying to establish some faux connection between the operations of News Corp here and in the UK, a debate on privacy must focus on the protection of the individual rather than the celebrity and the culture of international news outlets.

How do we define privacy and to whom should it extend? Would a privacy law have prevented the airing of Channel 7’s grubby piece about former New South Wales minister David Campbell? Will privacy laws protect children from online predators? Should employers be prevented from prejudging future employees based on social media profiling?

Individual privacy is and must continue to be a basic human right.

But, the greatest challenge to privacy is not from governments or international media outlets but social networking sites such as Facebook, Twitter and Google, whose stock and trade is dealing with and extracting personal data.

In reality, social networking sites have demonstrably diminished our privacy. Email addresses, personal connections, employment history, interests and travel patterns are now all easily accessible through Facebook searches. However, the collapse of personal privacy has been user-driven. New and old Facebook users alike freely give away personal information, whether prompted or not.

The culture of over-sharing personal information is all-too-obvious with each week bringing a new social media scandal – be it an offensive tweet, a viral video or an unhinged rant. Public embarrassment is one thing but over-sharing personal information endangers the privacy of individual users, especially the young and vulnerable. Online predators, behind veils of anonymity now lurk behind every online corner.

Potential employers now routinely scour social networking sites to see just how much personal information they can obtain about prospective employees. For some, the digital footprint of any given user can be far more valuable in making a character evaluation than a 10-minute sit-down.

At the recent meeting of Attorneys-General in Adelaide, the South Australian Government, through Attorney-General John Rau, was pushing for parents to have access to their children’s Facebook accounts and for the prohibition of select material on online networks.

Allowing parents to access a child’s Facebook account would be impossible to legislate, difficult to police and unachievable to implement. Does a parent ask their child for their Facebook password? If declined, do the parents then ask the police to access the account? Will the Government then come to an agreement with Facebook for universal access?

Such a policy is not only unrealistic but would be bad governance and poor parenting.

The simplest, most cost-effective and regulation-free way to protect people’s privacy is through education. Governments, employers and parents must promote an online culture of responsibility and restraint.

Commonwealth Attorney and Minister for Privacy, Brendan O’Connor, put it perfectly in Adelaide last week when he said that education is key in protecting privacy online: “Educating and informing young people about being careful about what they upload, what they put onto their Facebook or their social websites generally, so that they are not prone to being in any way vulnerable to that information then being misused.”

Social networking is here to stay. It has drastically altered the way in which we communicate and share information. It can be a powerful force for good in driving change and empowering the voiceless. But it has also altered our own perception of what we can and can’t share and provided a haven for bullies and predators.

If we want to protect privacy online we should be fostering an online culture of responsibility and restraint, where self-regulation is the best regulation and online communities determine what information they want to give away and to whom.

Thomas Tudehope is a director at leading social media risk management company SR7. From 2004-2009 he was digital director for Malcolm Turnbull.
Australian law is in a poor state when it comes to protecting our privacy. It should recognise that people are entitled to keep their lives out of the public domain and the reach of big business. There should also be consequences for a serious breach of privacy, including a right to compensation.

Unfortunately, the federal government has gone about this reform in the wrong way. It should not be sold as a response to the News of the World scandal – a hard sell when no local evidence has emerged of anything like those grievous, systematic breaches of trust. This leaves privacy reform in Australia open to attack as a knee-jerk reaction to events overseas.

It also casts the Australian media as the villain. Not surprisingly, this has provoked a furious response, with one headline in The Australian reading “Tort a hate-filled strike on liberal democracy”.

Privacy must also be balanced against the need to publish material in the public interest and freedom of expression and of the press.

The government has not actually said it will legislate, only that it will “release an issues paper soon to progress the debate”. This does not suggest conviction, especially when a right to privacy has already been recommended in 2008 in a 2,700-page report by the Australian Law Reform Commission.

The current debate needs a reality check. The 1988 Privacy Act is a lengthy, complex law that is often a toothless tiger. It is riddled with exemptions, including for politicians who have carved out an entitlement to amass data on voters and their families. As recommended by the commission, this self-serving exemption should be struck from the act.

The commission also found Australians should be able to sue for a serious invasion of their privacy. This might occur when a person is filmed using a hidden camera in a toilet, medical records are revealed or when someone posts online a video of a former partner engaged in sexual activity.

Such a right to privacy could have a chilling effect on freedom of speech. But the problem can be overcome, and has been in other nations such as the US and Canada. Following the same path, Australian law should limit compensation to serious violations. Privacy must also be balanced against the need to publish material in the public interest and freedom of expression and of the press.

Even in this form, a right to privacy will affect the media. Where a story reveals a person’s intimate affairs for profit and without justification, the media company may be liable. This might cause a rethink. For example, it is one thing to report on the lifestyles of celebrities, and another again to infringe the privacy of their children.

Despite the focus on the media, a right to privacy will have a greater impact elsewhere. The real problem lies with serious breaches of privacy by large corporations, and as a result of new technologies. There should be a remedy when a corporation acts negligently and criminals gain access to our credit card details or the information needed to steal our identity. There should also be checks on the information that companies can collect from us without our knowledge through our use of computers and websites.

Much of the current debate has concerned how a right to privacy might go too far, without also recognising its limits. It is expensive to sue anyone, let alone a well-resourced corporation, so the right may only be invoked in a few extreme cases.

In addition, a new law cannot overcome a lack of commonsense. No compensation can or should follow when a person fails to respect their own privacy. When it comes to one of the largest problems of privacy in Australia today – people posting their own intimate and potentially damaging information online – the solution will lie in education and not new laws.

George Williams is the Anthony Mason Professor of Law at the University of NSW.
Former Prime Minister Paul Keating takes issue with those who assert that privacy in modern times is dead. Mr Keating supports Australian Law Reform Commission recommendations that the law should provide recourse in the event of an unwarranted serious breach of an individual’s privacy. Here is an extract from a speech he delivered to the Centre for Advanced Journalism at the University of Melbourne on 4 August 2010.

Just about any day in the tabloids and any night on A Current Affair or Today Tonight you will see examples, including foot-in-the-door interviews, claimed to be necessary and justified by the media’s right to know, and to publish just about anything they like.

The issue of the media and privacy is also topical owing to proposals in a 2008 report by the Australian Law Reform Commission (ALRC) on Australia’s privacy laws. The report, the result of two years’ research, consultation and analysis, runs to 2,700 pages in three volumes. It put forward 295 recommendations for change with the general aim of modernising, simplifying, and streamlining laws that are generally seen to be dated, complex, confusing, fragmented and full of gaps and inconsistencies.

Media organisations should not be left entirely to themselves in setting standards.

Four recommendations are of direct relevance to the media. None have yet received a response from the Government. They propose changes to, but continuation of, the largely self-regulatory arrangements that are a condition for the exemption media organisations enjoy from privacy law ... and legislation to establish a general statutory cause of action for breach of privacy subject to a number of qualifiers to ensure the protection of other public interests.

The framework of media self-regulation

Managing privacy is part of a broader framework concerning ethics and values in journalism; an essential framework given the media’s exercise of significant public power, privilege and the potential to cause harm. This framework is, in fact, key to the conditional exemption media organisations enjoy from the Privacy Act.

The case for reform

The ALRC recommended two new limitations to the exemption for acts and practices in the course of journalism: that a definition of ‘journalism’ should be introduced for the purposes of the Privacy Act and a small change made to the definition of ‘media organisation’.

The more significant recommendation was that media organisations should not be left entirely to themselves in setting standards, with the introduction of measures that would continue the exemption only where a media organisation was committed to adequate privacy standards developed in conjunction with the Privacy Commission and the Australian Communication and Media Authority. In the light of the obvious shortcomings in the current system, this seems highly sensible to me.

Scope for change

First, industry leaders and the profession should acknowledge that improvements are needed. Instead of standing aggressively behind the status quo, dressed in the cloak of the Fourth Estate, they need to talk more about responsibility, more about the importance of ethics, more
about improvement in the standards of journalism in all respects. We might not be able to do much about some online players, but those in the mainstream need to provide real leadership in managing themselves and any self regulatory system.

Second, media organisations would be sending an important message about where they stand on these issues if they indicated they are prepared to work with, not against, the modest reforms proposed by the ALRC for continuation of the media exemption from the Privacy Act.

Third, industry and profession leaders should get back to an issue which has defied reformers for years: the idea that with regard to ethics and standards, the media would benefit from unified arrangements, consistent principles and uniform enforcement mechanisms applying to all sides: newspaper companies, journalists, broadcasting companies and internet service providers.

Fourth, more attention to guidance, education and training will continue to be an issue, especially while some senior journalists and those to whom they report, claim that the public interest is anything the public might find interesting.

---

**With regard to ethics and standards, the media would benefit from unified arrangements, consistent principles and uniform enforcement mechanisms.**

The public interest means publication or non-publication guided by what is in the interest of the public as a whole, not what readers or an audience might find interesting or titillating. It’s not always straightforward or easy to apply. But it’s claimed to be at the centre of media’s claimed right to publish generally and said to be a central determinant in deciding that publication of sensitive material is justified.

Rather than abandoning the public interest, the media needs to put more time and effort into fostering a better practical understanding of the term, including the notion of a right to privacy within its own ranks.

---

**REFERENCES**

The Australian Law Reform Commission’s 2008 report *For Your Information: Australian Privacy Law and Practice* (ALRC 108) recommended 295 changes to privacy laws and practices. Briefing notes on ten key areas – including children, credit reporting, health, data breach notification (fraud and identity theft), emerging technologies and creating an action for serious invasion of privacy – can be found at [www.alrc.gov.au](http://www.alrc.gov.au)

You can read Mr Keating’s address in full at [www.caj.unimelb.edu.au](http://www.caj.unimelb.edu.au)

Paul Keating is a former Prime Minister of Australia.
FAR FROM SINISTER, PRIVACY LAWS MIGHT MEAN MEDIA DOES ITS JOB BETTER

In spite of the scaremongering headlines, there is no reason to believe the introduction of privacy protection laws would curtail the fair and free functioning of the media, argues Bruce Arnold

There is a monster under the bed, frightening young and old. That monster is the proposal for a tort of breach of privacy. It is time that we turned on the lights, looked under the bed and looked our fears in the face, something that will make them disappear.

Last week the president of the Rule of Law Foundation, Robin Speed, a distinguished legal practitioner, criticised moves towards establishment of a statutory privacy tort. Speed was reported as worrying that the moves were intended as a way of intimidating the media.

The same article reported that “government plans to encourage people to sue each other using a statutory privacy tort have been denounced as so uncertain as to undermine the rule of law”. (Herald Sun columnist Andrew Bolt attacked it as “a sinister law, planned by a government with sinister motives”).

An attempt to chill free speech would be of concern to all Australians rather than merely media proprietors and journalists whose self-regulation – as evident in recent media scandals in the UK and other parts of Europe – on occasion leaves something to be desired. Do we need to worry?

Bedtime stories about monsters attract attention and calls for monster-slaying. Unfortunately, there’s no evidence that the Gillard Government intends to use updated privacy law to silence the mass media.

Instead, in a belated response to recommendations in separate reports from the Australian Law Reform Commission, the NSW Law Reform Commission and the Victorian Law Reform Commission, the federal Attorney-General Robert McClelland hasforeshadowed the release of a discussion paper seeking public comment about proposals for a privacy tort.

As monsters go, this one looks more like a teddy bear than something with claws, fangs and a lust for blood.

What would the privacy tort comprise? In the absence of the discussion paper we can only speculate.

The three commissions, which drew on extensive public consultation with legal practitioners, journalists, law enforcement personnel and ordinary members of the community, suggested that Australian law needs to protect individuals against injury (that is, tort) associated with an egregious disregard of privacy.

That tort would for example allow a victim to claim compensation for unauthorised video or other surveillance in a bathroom or bedroom, illicit access to medical records, or improper dissemination of sensitive personal information.

The tort would address the sort of abuses that regularly feature in the mass media and that are rightly condemned by editors, politicians and others who respect the notion of private life.

It would reflect recognition of privacy as a fundamental human right, the right to engage in lawful activity without interference from the state, from commercial entities and from prurient neighbours or strangers.

Would a tort silence the media and hobble law enforcement? Is the proposal a toxic teddy, apparently benign but destined to prevent the legitimate exposure of wrongs?

Existing privacy and data protection law specifically allows covert surveillance by law enforcement agencies, the collection of information by government bodies and collection by a wide range of non-government bodies where there is consent by individuals.

Reports over four decades have emphasised that privacy law involves a balance between personal and community interests, along with the importance of a vibrant mass media.

There is no reason to believe that a tort would fundamentally hamper legitimate activity in the public and private sectors or result in an explosion of litigation as neighbour sues neighbour.

What of the media? Reports by law reform commissions over four decades have emphasised that privacy law involves a balance between personal and community interests, along with the importance of a vibrant mass media.

Statements by McClelland and national Privacy Commissioner Timothy Pilgrim on the forthcoming discussion paper have been notable for their caution, even timidity.

There has been no substantive indications – as distinct from speculation by journalists – that any legislation would fundamentally restrict legitimate investigative journalism or reporting in the print/electronic media.

The reports by the commissions have been notable for their emphasis on ‘reasonableness’ and ‘industry practice’, consistent with national, state and territory privacy law that enshrines industry co-regulation and commonsense, rather than aggressive and pervasive supervision by government watchdogs.

Readers might ask whether we value privacy and whether there are times when a tort would be appropriate. Rather than being scared by headlines and hyperbole, we should turn on the lights, look critically at particular claims and discover that there is dust under the bed rather than a monster that will eat our children.

Bruce Arnold is a lecturer, Faculty of Law at the University of Canberra.

First published in The Conversation, 13 September 2011
http://theconversation.edu.au
EXPLORING
ISSUES

ABOUT THIS SECTION

‘Exploring issues’ features a range of ready-to-use worksheets relating to the articles and issues raised in this book.

The activities and exercises in these worksheets are suitable for use by students at middle secondary school level and beyond.

As the information in this book is gathered from a number of different sources, readers are prompted to consider the origin of the text and to critically evaluate the questions presented.

Does the source have a particular bias or agenda? Are you being presented with facts or opinions? Do you agree with the writer?

The types of ‘Exploring issues’ questions posed in each Issues in Society title differ according to their relevance to the topic at hand.

‘Exploring issues’ sections in each Issues in Society title may include any combination of the following worksheets: Brainstorm, Research activities, Written activities, Discussion activities, Quotes of note, Ethical dilemmas, Cartoon comments, Pros and cons, Case studies, Design activities, Statistics and spin, and Multiple choice.

CONTENTS

BRAINSTORM 50
WRITTEN ACTIVITIES 51-52
DISCUSSION ACTIVITIES 53
CARTOON COMMENTS 54
MULTIPLE CHOICE 55-56

WORKSHEETS AND ACTIVITIES

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
Brainstorm, individually or as a group, to develop your understanding of privacy concepts.

1. Privacy as covered by Australia’s Privacy Act relates to the protection of people’s personal information. However, this is just one aspect of privacy. Other types of privacy can include territorial privacy, physical or bodily privacy, and privacy of your communications. Define the following terms and consider how their meanings differ from one another.

   - Privacy of the person (also referred to as ‘bodily privacy’):

   - Privacy of personal behaviour (including ‘media privacy’):

   - Privacy of personal communications:

   - Privacy of personal data:

   - Personal information:
Complete the following activities on a separate sheet of paper if more space is required.

1. List 10 ways you can protect your identity and privacy online:
   1. 
   2. 
   3. 
   4. 
   5. 
   6. 
   7. 
   8. 
   9. 
   10. 

2. List 10 ways you can increase your mobile phone privacy and security:
   1. 
   2. 
   3. 
   4. 
   5. 
   6. 
   7. 
   8. 
   9. 
   10. 

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
3. Cyberbullying is the use of technology to deliberately and repeatedly bully someone else. It can happen to anyone, anytime, and can leave you feeling unsafe and alone. Provide 4 hypothetical examples of cyberbullying online and via mobile phones and describe the possible personal impacts on victims.
DISCUSSION ACTIVITIES

1. Privacy is emerging as a defining issue of the modern era, especially as new technology provides more opportunities for communication, but also new challenges to privacy. Right now there is no general right to privacy in Australia, and therefore no certainty for anyone wanting to sue for an invasion of their privacy. The News of the World tabloid phone hacking scandal in the UK and other recent mass breaches of privacy, both at home and abroad, have put the spotlight on whether there should be such a right. If a statutory cause of action for serious breaches of privacy is to be introduced into Australian law, what considerations are there in striking a balance between the principles of freedom of expression and the right to privacy? Discuss.
Consider the images and text of the two cartoons below and comment on the themes they each raise in relation to privacy rights. Complete your comments on a separate sheet of paper if more space is required.

<table>
<thead>
<tr>
<th>Cartoon 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Cartoon 1 Image]</td>
</tr>
<tr>
<td>© Simon Kneebone</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cartoon 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Cartoon 2 Image]</td>
</tr>
<tr>
<td>© Simon Kneebone</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Comments]</td>
</tr>
</tbody>
</table>

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and Trinity College, East Perth, allan.harris@trinity.wa.edu.au
Complete the following multiple choice questionnaire by circling or matching your preferred responses. The answers are at the end of the next page.

1. Personal information is information that identifies you, or could identify you. Personal information includes which of the following, as defined by Australia’s Privacy Act:
   a. Your name
   b. Your address
   c. Your medical records
   d. Your bank account details
   e. Photos
   f. Videos
   g. Information about what you like
   h. Your opinions
   i. Where you work

2. The following law/s recognise a right to privacy ...
   a. Universal Declaration of Rights
   b. International Covenant on Civil and Political Rights
   d. Privacy Act 1988 (Cth)
   e. Victorian Charter of Human Rights and Responsibilities

3. The technological and other innovations that have encroached on privacy in recent years include:
   a. The internet (able to broadcast personal information instantaneously around the world; spyware; social networking sites)
   b. Mobile phones (with GPS systems that can track your movements)
   c. Smartcard technology (records your movements and profiles spending habits and health details)
   d. Spread of CCTV
   e. Anti-money laundering legislation
   f. Mandatory reporting legislation (e.g. for health care and other professionals)
   g. Copying and scanning technology (e.g. at nightclubs and in taxis)

4. Under the Privacy Act 1988 you can make a complaint about the handling of your personal information by Australian, ACT and Norfolk Island government agencies and private sector organisations covered by the Act. Which organisation is responsible for handling these privacy complaints?
   a. Australian Communications and Media Authority
   b. Australian Privacy Foundation
   c. Civil Liberties Australia
   d. Office of the Australian Information Commissioner
   e. Australian Human Rights Commission
MULTIPLE CHOICE

Complete the following multiple choice questionnaire by circling or matching your preferred responses. The answers are at the end of this page.

5. Match the following terms to their correct definitions:

a. Bodily privacy  
1. Interest an individual has in controlling, or significantly influencing, the handling of data about themselves; also known as ‘data protection’.

b. Communications privacy  
2. Concerns the protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches.

c. Hacking  
3. Covers the security and privacy of mail, telephones, e-mail and other forms of communication.

d. Information privacy  
4. Concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space; includes searches, video surveillance and ID checks.

e. Invasion of privacy  
5. The intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded a right to bring a lawsuit for damages against the person or entity that intruded.

f. Personal information  
6. Our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. This right gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.

g. Privacy law  
7. Information or an opinion, 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.

h. Privacy protection  
8. Finding out weaknesses in an established system and exploiting them.

i. Right to privacy  
9. Laws which deal with the regulation of personal information about individuals which can be collected by governments and other public as well as private organisations and its storage and use.

j. Surveillance  
10. Process of finding appropriate balances between privacy and multiple competing interests.

k. Territorial privacy  
11. The systematic investigation or monitoring of the actions or communications of one or more persons.

MULTIPLE CHOICE ANSWERS

1 = a, b, c, d, e, f, g, h, i ; 2 = a, b, c, e ; 3 = a, b, c, d, e, f, g ; 4 = d ; 5 – a = 2, b = 3, c = 8, d = 1, e = 5, f = 7, g = 9, h = 10, i = 6, j = 11, k = 4.
Privacy’s importance is reflected in the fact that the fundamental documents that define human rights all include reference to privacy or related ideas. (p.1)

Many national Constitutions and Bills of Rights encompass privacy. (p.1)

Interpreted broadly, privacy is about the integrity of the individual. It therefore encompasses all aspects of the individual’s social needs. (p.2)

A serious debasement of the term ‘privacy’ has occurred in the case of US and Australian statutes that have equated it with the highly restrictive idea of ‘data protection.’(p.2)

At the end of the 19th century, United States judges argued that “the right to be let alone ... secures the exercise of extensive civil privileges”. (p.3)

For several decades discussions about privacy protection have been largely focussed on protections for data, instead of the protection of people’s interests. (p.3)

Data protection legislation regulating the Commonwealth public sector was passed in 1988. (p.4)

The world’s ‘data protection’ and ‘privacy’ laws have been very largely motivated by the facilitation of the business of government and private enterprise. (p.4)

The type of privacy covered by the Privacy Act and the Office of the Australian Information Commissioner is the protection of people’s personal information. (pp.5, 9)

You have a right to be granted access to the personal information that organisations and agencies hold about you. (p.6)

The Australian Law Reform Commission’s 2008 report into privacy laws made 295 recommendations for changes to privacy regulation and policy, including a proposal to introduce a statutory cause of action for serious breaches of privacy. (pp.8, 41, 45, 46, 47)

An action for invasion of privacy is seen by some as posing a threat to free expression, artistic freedom, and freedom of the press. (p.11)

The technological and other innovations that have encroached on privacy in recent years include: the internet, mobile phones, smartcard technology, CCTV, anti-money laundering legislation, mandatory reporting legislation, and copying and scanning technology. (p.14)

A common feature of democratic societies is the recognition that all citizens are entitled to a private life and to a wide range of choice about what is kept private. (p.14)

Australia’s defamation laws are some of the most onerous for publishers and we lack the broad constitutional protection for free speech that exists in the US and under the European Convention on Human Rights. (p.18)

With a stolen identity, a person may access your bank account, obtain credit cards or loans in your name or claim welfare benefits, and potentially ruin your credit rating. (pp.19, 22)

Smart phones have a built-in feature called geolocators that can pinpoint your exact location. (p.22)

Once information is online, it is not easy to remove it completely. Even if you remove information from your profile, saved or cached versions may still exist on other computers. (p.24)

Posting something rude, offensive or derogatory about another person or business in a public forum may be used as legal evidence. (p.25)

The aim of the Office of the Privacy Commissioner is to promote awareness and protection of personal information. (p.27)

There are Commonwealth, State and Territory laws that relate to taking and using images of a person without their permission, or recording their conversations or movements. (p.28)

The Privacy Act does not cover the acts and practices of media organisations in the course of journalism. (pp.28, 37)

The first CCTV surveillance camera in a city was installed at Olean, New York, in 1968. (p.29)

In Britain, there are more than 6 million CCTV cameras and figures released in 2009 showed that just one crime per year was solved for every 1,000 CCTV cameras in use. (p.29)

In 1981, a CCTV camera was installed in a major road leading into Melbourne. Its purpose was to help with traffic during a forthcoming Commonwealth heads of government meeting. It was never removed. (p.29)

In its 2010 Counter-Terrorism White Paper, the Government stated its intention to use or expand the use of certain national security measures. (p.30)

The legal safeguards of privacy in Australia remain limited. Neither the Australian Constitution nor any state or territory constitutions contain any express provisions relating to privacy. (p.31)

Over the last decade, the Australian Government has enacted almost 50 pieces of anti-terrorism legislation. (p.31)

The Council of Europe Convention on Cybercrime is the first international treaty on crimes committed via the internet. (p.33)

The communications sector generates around 21,000 privacy complaints each year. (p.35)

A recent international survey of 127 journalists in 46 countries, including Australia, found that most faced ethical dilemmas at work and admitted to having behaved unethically. (p.37)

In 2008 the Australian Law Reform Commission recommended a statutory right to privacy, and suggested that the Privacy Act be strengthened to require the media to deal with privacy issues. (p.38)

The International Covenant on Civil and Political Rights – which Australia signed in 1972 and ratified in 1980 – arguably obligates Australia to provide legislative protections for all forms of privacy, not just data privacy. (p.43)

Existing privacy and data protection law specifically allows covert surveillance by law enforcement agencies. (p.48)
Privacy law
Privacy law refers to the laws which deal with the regulation of personal information about individuals which can be collected by governments and other public as well as private organisations and its storage and use. The current state of privacy law in Australia includes Federal and state information privacy legislation, some sector-specific privacy legislation at state level, regulation of the media and some criminal sanctions. The current position concerning civil causes of action for invasion of privacy is unclear: some courts have indicated that a tort of invasion of privacy may exist in Australia; in 2008, the Australian Law Reform Commission recommended the enactment of a statutory cause of action for invasion of privacy.

Privacy protection
A process of finding appropriate balances between privacy and multiple competing interests.

Right to privacy
The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose. Most of the great human rights instruments marking out the freedoms of democratic societies include a right of privacy: the Universal Declaration of Rights, the International Covenant on Civil and Political Rights, the EU Convention for the Protection of Human Rights and Fundamental Freedoms. The Victorian Charter of Human Rights and Responsibilities gives only limited legal recognition to the right of privacy. There is a patchwork of laws in Australia that requires government agencies and certain other bodies to deal properly with personal information but none of them gives redress of the kind proposed by the Law Reform Commission, i.e. a general right to sue for damages for a serious and intentional invasion of privacy.

Surveillance
The systematic investigation or monitoring of the actions or communications of one or more persons. Electronic surveillance refers to both augmentations to physical surveillance (such as directional microphones and audio bugs) and to communications surveillance, particularly telephone taps. Data surveillance (or dataveillance) is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Dataveillance is significantly less expensive than physical and electronic surveillance, because it can be automated. As a result, the economic constraints on surveillance are diminished, and more individuals, and larger populations, are capable of being monitored.

Closed-circuit television (CCTV)
The use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

Confidentiality
The legal duty of individuals who come into the possession of information about others, especially in the course of particular kinds of relationships with them. Confidentiality is an incidental, and wholly inadequate, substitute for proper information privacy protection.

Hacking
Finding out weaknesses in an established system and exploiting them. A computer hacker is a person who detects weaknesses in the computer and exploits it. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.

Information privacy
The interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves. The term ‘data privacy’ is sometimes used in the same way. ‘Data’ refers to inert symbols, signs or measures, whereas ‘information’ implies the use of data by humans to extract meaning. Hence ‘information privacy’ is arguably the more descriptive of the two alternatives.

Invasion of privacy
The intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded a right to bring a lawsuit for damages against the person or entity that intruded.

Personal information
The Privacy Act 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.’

Phone hacking
The practice of intercepting telephone calls or voicemail messages, often by accessing the voicemail messages of a mobile phone without the consent of the phone’s owner.

Privacy
The interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations. Privacy has several dimensions: privacy of the person (sometimes referred to as ‘bodily privacy’), privacy of personal behaviour, privacy of personal communications, and privacy of personal data (sometimes referred to as ‘data privacy’ and ‘information privacy’).

Privacy Act
The Privacy Act 1988 regulates how your personal information is handled. For example, it covers how your personal information is collected, how it is then used and disclosed, its accuracy, how securely it is kept, and your general right to access that information.
Websites with further information on the topic

Australian Communications and Media Authority  www.acma.gov.au
Australian Privacy Foundation  www.privacy.org.au
Civil Liberties Australia  www.cla.asn.au
Cybersmart  www.cybersmart.gov.au
Department of the Prime Minister and Cabinet  www.dpmc.gov.au
Liberty Victoria  www.libertyvictoria.org.au
New South Wales Council for Civil Liberties  www.nswccl.org.au
Office of the Australian Information Commissioner  www.oaic.gov.au
Office of the Information Commissioner New South Wales  www.oic.nsw.gov.au
Office of the Privacy Commissioner  www.privacy.gov.au
Privacy Victoria  www.privacy.vic.gov.au
Queensland Council for Civil Liberties  www.qccl.org.au
Stay Smart Online  www.staysmartonline.gov.au

For more information about social issues visit The Spinney Press website at www.spinneypress.com.au

ACKNOWLEDGEMENTS
The publisher is grateful to all the contributors to this book for granting permission to reproduce their works.

COPYRIGHT DISCLAIMER
While every care has been taken to trace and acknowledge copyright the publisher tenders its apology for any accidental infringements or where copyright has proved untraceable. The publisher would be pleased to come to a suitable arrangement with the rightful owner.

ILLUSTRATIONS AND PHOTOGRAPHS
Photographs and illustrations courtesy of iStockphoto, except pages 9, 10, 36, 42 and 54 © Simon Kneebone, pages 34 and 41 © Don Hatcher, and page 47 © Angelo Madrid.

THANK YOU
Roger Clarke, Australian Privacy Foundation
Office of the Australian Information Commissioner

DISCLAIMER
The Spinney Press is an independent educational publisher and has no political affiliations or vested interests with any persons or organisations whose information appears in the Issues in Society series. The Spinney Press seeks at all times to present variety and balance in the opinions expressed in its publications. Any views quoted in this book are not necessarily those of the publisher or its staff.

Advice in this publication is of a general nature and is not a substitute for independent professional advice. Information contained in this publication is for educational purposes only and is not intended as specific legal advice or to be used to diagnose, treat, cure or prevent any disease. Further, the accuracy, currency and completeness of the information available in this publication cannot be guaranteed. The Spinney Press, its affiliates and their respective servants and agents do not accept any liability for any injury, loss or damage incurred by use of or reliance on the information made available via or through its publications, whether arising from negligence or otherwise.

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong> anti-terrorism legislation 31 artistic freedom 11 Australia Card 4, 16</td>
</tr>
<tr>
<td><strong>B</strong> bodily privacy 2, 5 body scanners 30-32 breach of confidence 9, 12-13, 15, 17</td>
</tr>
<tr>
<td><strong>C</strong> CCTV 14, 16, 28, 29 Charter of Fundamental Rights of the European Union 1 communications privacy 19-36 complaints 35-36 Council of Europe Convention on Cybercrime 33, 40 Counter-Terrorism White Paper 30-32 cyberbullying 8, 20 cybercrime 33-34, 40 Cybercrime Legislation Amendment Bill 2011 34, 40</td>
</tr>
<tr>
<td><strong>D</strong> data privacy 2, 30, 43 data protection 2-4, 9-10, 30-31, 48 Defamation Act 39 digital age 44 digital fingerprint 33-34 digital reputation 21</td>
</tr>
<tr>
<td><strong>E</strong> European Convention for the Protection of Human Rights and Fundamental Freedoms 1, 13, 14-15, 17-18, 40</td>
</tr>
<tr>
<td><strong>F</strong> Facebook 12, 16, 19, 23, 24, 38, 44 freedom of expression 8, 11, 41, 43, 45 speech 12-13, 16, 40, 45, 48 the press 8, 11, 16, 37, 41, 42, 43, 45</td>
</tr>
<tr>
<td><strong>G</strong> geolocators 22 GPS 14, 26</td>
</tr>
<tr>
<td><strong>H</strong> hacking 15, 18, 25, 33, 39, 42 human rights 1-4, 10-11, 14, 30-32, 34 Human Rights Act 13, 40</td>
</tr>
<tr>
<td><strong>I</strong> identity theft 7, 19, 22, 23, 25 information age 14, 46 information privacy 2, 4, 9 International Covenant on Civil and Political Rights 1, 10, 14, 43 internet 12, 14, 24, 27, 28, 33-34, 35, 38, 40, 47 see also online internet-related complaints 35</td>
</tr>
<tr>
<td><strong>J</strong> Journalists’ Code of Ethics 37 journalist shield laws 11</td>
</tr>
<tr>
<td><strong>L</strong> location-based information 35 see also geolocators, GPS</td>
</tr>
<tr>
<td><strong>M</strong> Maslow’s Hierarchy of Needs 2 media privacy 2-3, 46 Medicare cards 16, 19 mobile phones 14, 22, 26-27, 34 protection 26-27 Murdoch media 8, 12, 16, 37-38, 40 MySpace 13, 23, 24</td>
</tr>
<tr>
<td><strong>N</strong> national security 1, 11, 16, 30-32 News of the World scandal 8, 17, 37-38, 39, 40, 41, 42, 45</td>
</tr>
<tr>
<td><strong>O</strong> online communications 20-21, 23, 24-25, 33, 40 privacy 7, 19, 20-21, 24, 39, 44 protection 19, 23, 24, 44, 45</td>
</tr>
<tr>
<td><strong>P</strong> personal behaviour 2 personal communications 2-3 personal data 2-3, 22, 36, 44 phishing 22, 25 phone-hacking scandal see News of the World scandal photos and surveillance laws 28 Privacy Act 5, 6, 7, 9, 28, 38, 41, 45, 46, 47 privacy breaches 8, 10 privacy, definitions 1-5 privacy laws 8, 9, 12-13, 14-15, 17-18, 31, 39, 44, 45, 46, 48 privacy of the person see bodily privacy privacy policy 6, 19, 22, 24 privacy protection 1, 3, 9, 12-13, 18, 31, 35, 41, 48 privacy rights 7, 11, 30, 41 privacy settings 19, 20, 22, 24-25 public interest 13, 18, 39, 42, 43, 45, 47</td>
</tr>
<tr>
<td><strong>R</strong> right of action 17, 42-43 right to privacy 8, 16, 29, 30, 31, 32, 39, 40, 41, 42, 45, 47</td>
</tr>
<tr>
<td><strong>S</strong> security settings 26 sexting 20 shopping, online 21-22 smartcard technology 14 smart phones see also mobile phones social networking 14, 19, 20-22, 23, 24-25, 35, 38, 44 protection 23, 24-25 statutory cause of action 8, 9-11, 12, 13, 43, 46 statutory privacy tort 12-13, 17, 42-43, 48 surveillance 1, 16, 28, 29, 30-32, 33, 40, 42, 48</td>
</tr>
<tr>
<td><strong>T</strong> tax file numbers 4, 16 Telecommunications (Interception and Access) Act 8, 17, 28, 33, 41 terrorism 30-32 Twitter 12, 16, 24, 38, 44</td>
</tr>
<tr>
<td><strong>U</strong> Universal Declaration of Human Rights 1, 14</td>
</tr>
<tr>
<td><strong>W</strong> wireless (Wi-Fi) networks 27</td>
</tr>
</tbody>
</table>

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: Trinity College, East Perth, allan.harris@trinity.wa.edu.au