Australian Government | acma

Australian Communications and Media Authority

Submission by the Australian Communications and Media Authority to the Australian Law Reform Commission Inquiry into Serious Invasions of Privacy in the Digital Era – Issues Paper 43

NOVEMBER 2013

communicating | facilitating | regulating

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

Written enquiries may be sent to:
Manager, Editorial and Design
PO Box 13112
Law Courts
Melbourne VIC 8010
Tel: 03 9963 6968
Email: candinfo@acma.gov.au

Contents

Overview

The Australian Communications and Media Authority (the ACMA) is responsible for the regulation of broadcasting, the internet, radiocommunications, and telecommunications.

The ACMA's responsibilities are outlined in detail in Part 2, Division 2 of the *ACMA Act 2005* and include:

> promoting self-regulation and competition in the telecommunications industry, while protecting consumers and other users

> fostering an environment in which electronic media respects community standards and responds to audience and user needs

> managing access to the radiofrequency spectrum, including the broadcasting services bands

> representing Australia's communications and broadcasting interests internationally.

The ACMA operates across a diverse, complex and rapidly changing media and communications landscape. Ubiquitous networks, complex connections and digital content bring exciting options for individuals as consumers and citizens, as well as many new business opportunities. In this environment it has also become more challenging for individuals to manage their communications and content experience. One element of this communications and content experience is privacy. The ACMA administers legislation providing a range of privacy safeguards specific to media and communications-related matters. The ACMA also undertakes research to identify the dimensions and impacts of technological developments, and to understand changes in behaviours and expectations of digital citizens.

The concept of privacy endures in the media and communications environment and citizens remain highly sensitive to intrusions on their privacy and how information about them is collected and shared. Community perceptions of privacy in relation to broadcast media are complex and nuanced and privacy issues are evaluated by individuals on a case-by-case basis.

The ACMA considers that existing privacy regulatory measures covering the media and communications sectors and the proposed statutory cause of action, should be viewed as complementary avenues for protecting privacy interests. As this submission sets out, the industry-specific regulatory framework administered by the ACMA has a role to play that is distinct from that of the proposed statutory cause of action. For example, the ability of the ACMA to investigate breaches of a broadcasting code of practice and to take action as a result fulfils the public policy objective of encouraging broadcasters to reflect community standards in the provision of program material.[1] The ability of the ACMA to undertake investigations and to take action remains an important element of the regulatory toolkit, and would be complemented, rather than replaced, by the ability of affected individuals to also seek personal redress for serious invasions of privacy.

[1] Paragraph 1(h) *Broadcasting Services Act 1992*.

The broadcasting co-regulatory regime, for example, provides for industry codes of practice which are directed at meeting the interests of the broader community, and any concerned citizen may make a complaint. This contrasts with the proposed statutory cause of action where it would generally be the aggrieved individual, or another body on their behalf, that raises a claim.

Media and communications industry regulation is aimed at industry-wide practices, addressing systemic issues relating to privacy rather than providing redress for affected individuals. Examples include Spam, Do Not Call, the privacy provisions of the *Telecommunications Consumer Protection Code C625:2012* (TCP Code) and the protection of communications and personal information related to the communications contained in Part 13 of the *Telecommunications Act 1997* (Telecommunications Act).

The ACMA also fulfils a community education role relevant to matters of privacy. This role includes the provision of advice, especially to children and young people, on cybersafety issues including the protection and management of their digital identities and the trails of data they create when online.

This submission:

> sets out information on the operation of the media and communications industry-specific privacy safeguards provided by legislation administered by the ACMA, including examples drawn from recent ACMA investigations and activities

> provides a discussion of issues in relation to a number of the questions posed by the Issues Paper

> includes an outline of research conducted by the ACMA relevant to communications and media privacy.

The ACMA welcomes the opportunity to provide a submission to this Inquiry.

The ACMA's privacy role in media and communications

Australia's media and communications legislation gives the ACMA a multi-faceted role in relation to privacy practices in media and communications.

A key policy intent of the *Broadcasting Services Act 1992* (BSA) is that the broadcasting and internet sectors be regulated in a way that 'does not impose unnecessary financial and administrative burdens' on industry.[2] A key policy intent of the Telecommunications Act is that the sector be regulated in a manner that 'promotes the greatest practicable use of industry self regulation' and 'does not impose undue financial and administrative burdens on [industry participants]'.[3] The relevant legislative framework therefore requires the ACMA to provide industry with the opportunity to develop co and self-regulatory solutions, before other forms of intervention are considered.[4]

Other areas of regulatory focus include online content, online safety, education and advice and unsolicited communications. These areas are regulated by legislation such as the *Spam Act 2003* (Spam Act) and the *Do Not Call Register Act 2006* (DNCR Act).

The regulatory frameworks for the radiocommunications, telecommunications and broadcasting sectors each contain clear privacy objectives and measures. The ACMA has observed common elements of communications and media privacy that provide insights to the framing of privacy protections (see Figure 1). These elements include:

> identity—to protect a citizen's or consumer's personal or private information

> location activity—to protect information about an individual's location, activities or movements

> intrusion—to protect a citizen or consumer's personal space from unwanted intrusions

> reputation—to protect a citizen's name or reputation

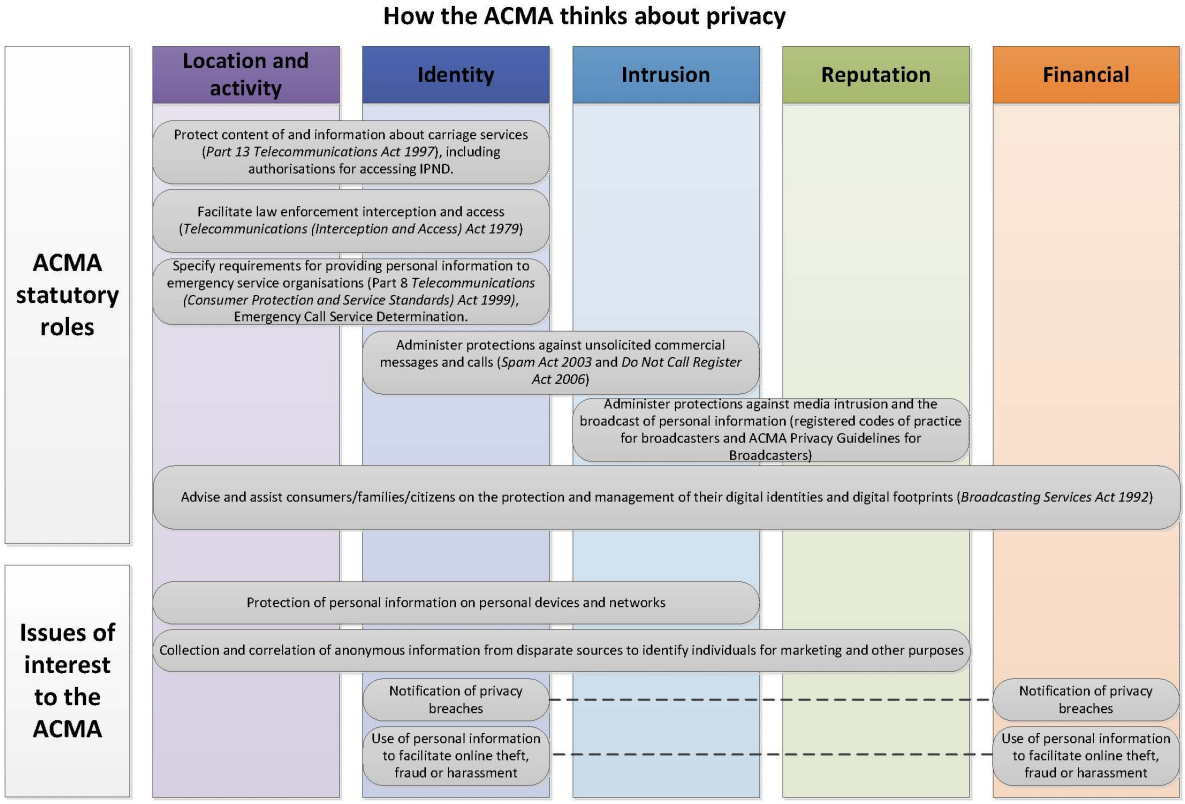
> financial—to protect a citizen or consumer's financial or transactional information.

[2] Paragraphs 4(2)(a) and 4(3)(a) *Broadcasting Services Act 1992.*

[3] Section 4 *Telecommunications Act 1997.*

[4] The ACMA maintains what are essentially reserve powers to intervene where self-regulation has not adequately addressed issues of real concern. See Part 6, *Telecommunications Act 1997* and Part 9, *Broadcasting Services Act 1992*.

Figure 1—How the ACMA thinks about media and communications privacy



Source: ACMA, Privacy and personal data, *Emerging issues in media and communications–Occasional paper 4*, June 2013, p. 20.

Of particular relevance to this submission are the ACMA's role and functions relating to:

> administering protections against media intrusion and the broadcast of personal information

> administering protections against offensive or illegal online content, including take-down of prohibited content hosted in or provided from Australia

> advising and educating the community, especially children and young people, on online safety issues

> administering protections against unsolicited commercial messages and calls

> protecting content of, and information about carriage services, including authorisations for accessing the Integrated Public Number Database. Monitoring compliance with privacy provisions of the TCP Code.

These functions are outlined further below.

Broadcasting regulation

Co-regulation and broadcasting industry codes of practice

Broadcasting regulation is based on a co-regulatory approach. In broadcasting, an arguable benefit of the co-regulatory approach is that it facilitates timely adaptation to the ongoing challenges of changes in technology, shifts in business models and community expectations. This is because codes may be amended from time to time without the need for legislative change.

Section 123 of the BSA states the Commonwealth Parliament's intention that industry groups that represent various sections of the industry (i.e. commercial broadcast,

subscription broadcast, narrowcast and community broadcast sections) develop codes of practice applicable to the broadcasting operations of each of those sections. The codes must be developed in consultation with the ACMA and take into account any relevant research undertaken by the ACMA. Subsection 123(4) requires that before registering a code,[5] the ACMA be satisfied that:

- the code provides appropriate community safeguards for the matters that it covers
- the code was endorsed by the majority of providers of broadcasting services in that section of the industry
- members of the public have been given adequate opportunity to comment on the code.

The commercial broadcasting industry codes made under section 123 of the BSA have made conditional provision for protecting the privacy of individuals (conditional, because each is subject to an exception permitting disclosure in the public interest) in code provisions relating to news and current affairs programs. The national broadcasters, ABC and SBS, have also included conditional privacy provisions in codes of practice, which they prepare under their enabling legislation.

The privacy provisions in codes of practice made under section 123 of the BSA reflect a balance between the media's role in informing the public and an individual's expectation of privacy. While the obligations on each broadcaster are dependent on the terms of the code applicable to it, and each code differs, the provisions are substantially similar. The codes currently registered with the ACMA are:

Radio codes

- Subscription narrowcast radio code of practice 2013
- Commercial radio codes of practice and guidelines September 2013
- Community radio broadcasting codes of practice 2008
- ABC code of practice 2011 (Revised 2013)
- SBS codes of practice 2006 (incorporating amendments 12 December 2012)
- Open narrowcasting code of practice (2011)

TV codes

Commercial TV

- Commercial Television Industry Code of Practice 2010 (amendments to July 2013)
- Community Television Codes of Practice
- ABC code of practice 2011 (revised 2013)
- SBS codes of practice 2006 (incorporating amendments 12 December 2012)

Subscription broadcast television (pay TV)

- Subscription broadcast television codes of practice 2013

Subscription narrowcast television (pay TV)

- Subscription narrowcast television codes of practice 2013
- Open Narrowcast Television Codes of Practice 2009.

The privacy provisions in the codes that apply to commercial and subscription broadcasting relate only to news and current affairs programs. In the case of the ABC,

[5] National broadcasters are not required to register their codes with the ACMA, but instead notify the ACMA. Subsection 123(2) provides that such codes of practice may relate to various matters, including preventing the broadcasting of programs that, in accordance with community standards, are not suitable to be broadcast by that section of the industry, as well as matters relating to program content that are 'of concern to the community'.

SBS, community sector and open narrowcasting radio codes, the privacy provisions relate to all programs.

Privacy Guidelines for Broadcasters

In 2011 the ACMA undertook a review of the *Privacy guidelines for broadcasters* (the Privacy Guidelines). The Privacy Guidelines were first introduced in 2005. The introductory notes acknowledged that there was no general right to privacy in Australia, but that there were laws that protected an individual's privacy in certain circumstances.

The Privacy Guidelines are intended to afford guidance to the public and broadcasters seeking to comply with Code provisions relating to privacy in their daily broadcasting operations, and guidance on how the ACMA is likely to interpret and apply those Code provisions when dealing with a complaint to the ACMA under Part 11 of the BSA. The Privacy Guidelines are not a legislative instrument, but are one of several sets of guidelines on various broadcasting obligations which the ACMA publishes for the assistance of broadcasters and the public, and to promote compliance by broadcasters with those obligations.

To inform the development of the Privacy Guidelines, the ACMA undertook research into community perceptions of privacy in the context of broadcast news media and current affairs. Key findings of this research are set out in Appendix A.

In 2009 the ACMA foreshadowed a review of the Privacy Guidelines in an ACMA investigation decision[6] which concluded that the Privacy Guidelines did not provide adequate guidance on broadcasting code elements dealing with material that invades an individual's privacy through an intrusion into a person's seclusion, whether or not in a public space.

The Review considered the effectiveness, efficiency and appropriateness of the Privacy Guidelines within the current environment, and concluded with revised Privacy Guidelines being developed. In particular, the Privacy Guidelines were enhanced to:

- formulate new principles concerning intrusions into seclusion and develop existing principles concerning the disclosure of personal information
- clarify that:
    - invasions of privacy can occur in a public space
    - personal information can include information about sexual activities
    - disclosure of personal information that had been provided on a confidential basis to a limited circle may be an invasion of privacy where its private nature could be implied
- expand consent principles to expand on the meaning of 'informed consent' and to make it clear that material obtained surreptitiously would indicate that there has been no consent
- insert new guidelines concerning special care for children and vulnerable persons, reflecting the special care provisions of broadcasting codes of practice reviewed since the 2005 Privacy Guidelines were developed
- develop principles concerning material already in the public domain, to provide guidance on the use of material obtained from social media sites and make it clear that the absence of access restrictions will not be determinative
- provide that any such disclosure in the public interest should be proportionate and relevant to the public interest issues - the position on public figures was clarified

[6] ACMA Investigation 2027, available at: http://www.acma.gov.au/~/media/Broadcasting%20Investigations/TV%20investigations/pdf/Investigation%20Report%202027%20NEW10%20Ten%20News%20at%20Five.PDF

> review and update case studies, taking into account the ACMA's recent decisions on privacy code provisions.

Following consultation on the draft revised Privacy Guidelines, the ACMA released the revised Privacy Guidelines in December 2011.

Complaints

Complaints relating to broadcasting codes of practice are dealt with under the co-regulatory model. Complaints by members of the public about non-compliance by a broadcaster with an applicable code of practice must, in the first instance, be made to, and dealt with, by the broadcaster. However, if the complainant does not receive a response from the broadcaster within 60 days, or receives a response but considers it inadequate, the complainant may complain to the ACMA about the matter.[7]

Most ACMA investigations are undertaken in response to complaints. As well as investigating complaints relating to an applicable code, the ACMA has the authority to investigate complaints if they relate to a licensee/s compliance with a licence condition or a program standard. In addition, the ACMA can initiate investigations relating to applicable codes, licence conditions or program standards on its own motion, or at the direction of the Minister.

In the 2012-2013 year, the ACMA received 2,178 written complaints and enquiries about commercial, national and community broadcasters. The ACMA completed 212 broadcasting investigations. Of the 67 investigations that resulted in breach findings, 20 related to compliance with codes of practice. The ACMA uses the Privacy Guidelines in decisions concerning privacy provisions of broadcasting codes of practice. Of the 20 investigations which related to compliance with codes of practice, seven investigations raised issues of privacy.

During the 2011-2012 reporting year, five broadcasting investigations were undertaken where the privacy area of the relevant code was considered. The following examples from ACMA broadcasting investigations are relevant to the ALRC Inquiry as they illustrate investigations where the ACMA has considered the privacy provisions in a code and the factors that have been considered.

The ACMA's investigations steps are outlined in the discussion of issues in response to Question 7 of the Issues Paper about how the public interest may be taken into account.

Generally, the codes protect against the broadcast of material that:

> relates to a person's personal or private affairs—for example, by disclosing personal information
> invades a person's privacy—for example, by intruding upon his or her seclusion.

The Privacy Guidelines state that personal information can include factors about a person's health, personal relationships, financial affairs, sexual activities, and sexual preferences. It can also include information about a person's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, criminal record and other sensitive personal matters. This information need not be secret or confidential in order to be private.

[7] Relevant provisions for national broadcasters are set out in Part 11, Division 2 of the BSA, and relevant provisions for other broadcasters in Part 11, Division 1 of the BSA

Example 1

In Investigation 2813,[8] the ACMA considered clauses 4.3.5 and 4.3.5.2 of the *Commercial Television Industry Code of Practice 2010*.

4.3. In broadcasting news and current affairs programs, licensees:

4.3.5 must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, other than where there is an identifiable public interest reason for the material to be broadcast;

4.3.5.2 for the purpose of this clause 4.3.5, licensees must exercise special case using material relating to a child's personal or private affairs in the broadcast of a report of a sensitive matter concerning a child. The consent of a parent or guardian should be obtained before naming or visually identifying a child in a report on a criminal matter involving a child or a member of a child's immediate family or a report which discloses sensitive information concerning the health or welfare of a child, unless there are exceptional circumstances or an identifiable public interest reason to do so;

4.3.5.3 'child' means a person under 16 years old.

The complainant and his family were filmed in and around their house as part of a news story about a midwife who was no longer registered. Although there was some public interest in the midwife's activities, this could have been reported without using intrusive details about the family. The ACMA found that the broadcast breached the privacy of the family involved because the camera was used to pry into the family's home.

Even though the older children's faces were pixilated, the family could be identified through shots of the father and the house, and the naming of their suburb. The father had not consented to the broadcast and the personal information disclosed was not already in the public domain.

By reporting sensitive information about a child, the licensee also failed to exercise special care in using material relating to the baby's privacy.

The licensee argued that the father had consented when he came out onto the footpath to talk to the news crew. However, the father's response was that he had objected to them being outside his house for two days, repeatedly asking them to move and to not use footage of his family.

Under section 5 of the BSA, the ACMA must use its powers to deal with a breach of the BSA or regulations in a manner that, in the opinion of the ACMA, is commensurate with the seriousness of the breach concerned. One of the actions available to the ACMA under the BSA is the imposition of additional licence conditions to achieve compliance. The ACMA may also: informally agree to accept measures by broadcasters to improve compliance; accept an enforceable undertaking; or give the licensee a remedial direction requiring compliance.

These remedies are directed at the broadcast licensee and as such are not directed at providing a specific remedy for the individual. As discussed further in response to Question 25, the ACMA considers these existing regulatory settings as complementary to any statutory cause of action.

[8] Investigation Report 2813 available at: http://www.acma.gov.au/webwr/_assets/main/lib410172/nws-report-2813.pdf

Online content

The ACMA also administers the Online Content Co-regulatory Scheme (the Scheme) established under Schedules 5 and 7 to the BSA.[9] Under the Scheme, the ACMA Hotline investigates valid complaints from Australian residents about offensive or illegal online content and takes action on content determined to be 'prohibited content' or 'potential prohibited content'. These terms are defined with reference to the National Classification Scheme[10] that applies to films and computer games. Content that is classified RC (Refused Classification) or X18+ (Restricted) is prohibited[11] and, in certain circumstances, content classified R18+ (Restricted) or MA15+ (Mature Accompanied) may also be prohibited.[12]

The actions available to the ACMA vary, based on whether content is hosted in Australia or overseas. Where prohibited content is hosted in Australia, the ACMA is required to direct the hosting service provider to remove (take-down) or, in certain circumstances, restrict access to the content. Where prohibited or potential prohibited content is hosted outside of Australia, the ACMA notifies the content to Internet Industry Association (IIA) accredited optional end-user PC-based filters. Regardless of where the content is hosted, if it is deemed to be potentially illegal (for example, child sexual abuse material or material which advocates the doing of a terrorist act), the ACMA notifies the content to the relevant law enforcement agency.

During the period 1 July 2012 to 30 June 2013, the ACMA received 4,633 complaints about online content. Of the investigations completed, 1,853 items of prohibited or potential prohibited content were identified and actioned 99.6 per cent of which were hosted overseas. A total of 556 investigations were terminated because the ACMA was unable to obtain sufficient information on which to base a decision, usually because the content identified in the complaint could not be located.

The actions taken by the ACMA as the regulator are not focused on providing a specific remedy to the complainant or to someone featured in the content without their consent, but are more broadly aimed at encouraging industry self-regulation through codes of practice; preventing inadvertent access to offensive or illegal content by Australian citizens; and ensuring that illegal material is brought to the attention of law enforcement in Australia and around the world.

Privacy Enquiries

The Scheme administered by the ACMA Hotline does not specifically deal with matters relating to privacy or the unauthorised publication of personal information. These matters cannot be taken into account when an assessment is made about whether content is prohibited or potential prohibited.

Prohibited content is defined in reference to the National Classification Scheme that applies to films and computer games. Content that is classified RC and X 18+ is prohibited, while content that is R 18+ and a limited amount of MA 15+ content may be prohibited if it meets other conditions. Prohibited content covers a range of material including child sexual abuse material, pro-terrorist material, abhorrent or revolting phenomena, bestiality, high-impact sex and violence, and explicit sexual content.

---

[9] Schedule 5 regulates content hosted outside Australia; Schedule 7 regulates content with an 'Australian connection'.

[10] The National Classification Scheme is a cooperative arrangement whereby the Classification Board classify films, computer games and certain publications. Further information about the Scheme can be found here: http://www.classification.gov.au/About/Pages/National-Classification-Scheme.aspx#1

[11] These classifications are the restricted categories for adult films.

[12] These classifications are restricted categories for films and computer games.

The ACMA Hotline (as the Scheme is branded) is a complaints mechanism for Australian residents to report online content that may be offensive or illegal. The ACMA Hotline receives a moderate volume of enquiries about online privacy issues. From 1 January 2013 to 30 September 2013, the ACMA Hotline received 564 enquiries; of these, approximately 15 enquiries concerned privacy matters or the publication of personal information online. The ACMA Hotline generally advises people with concerns about privacy to:

> seek independent legal advice about the options available for dealing with the material or persons concerned
> contact the administrators of the website directly to request that the content be removed
> visit the complaints section of the website of the Office of the Australian Information Commissioner for further information about privacy matters
> contact their local police (if they have fears for their safety or property).

The following are examples of privacy enquiries that the ACMA has received, but which are outside the regulatory framework of the Scheme. As such, no further action was taken by the ACMA. Further discussion of the ACMA's role in take-down of prohibited content is provided in response to Question 18 and consideration of possible non-monetary/injunctive remedies.

Example 2

In February 2013, the ACMA received an enquiry from an Australian resident[13] alleging that their privacy had been breached as a personal video they recorded on their webcam had been posted on a video sharing website without their permission.

Example 3

In May 2013, the ACMA received an enquiry from an Australian resident concerned about privacy issues as the price of their house had been listed on a real estate research website.

Example 4

In August 2013, the ACMA received an enquiry from an Australian resident requesting information about privacy laws as their mobile phone number had been incorrectly listed on a classified website for male escorts.

Online safety advice, assistance and education

The ACMA has responsibilities conferred under Schedules 5 and 7 to the BSA to:

> advise and assist parents and responsible adults in relation to the supervision and control of children's access to internet content and content services
> conduct and/or co-ordinate community education programs about internet content, internet carriage services and content services, in consultation with relevant industry and consumer groups and government agencies
> to conduct and/or commission research into issues relating to internet content, internet carriage services and content services.

[13] Under the *Broadcasting Services Act 1992*, only certain parties are eligible to make a complaint to the ACMA about offensive or illegal online content – complainants must be an Australian resident; a business carrying on activities in Australia; or a State, Territory or the Commonwealth.

As part of these roles, the ACMA manages a national cybersafety and cybersecurity education program known as Cybersmart. The Cybersmart program enables children, parents, carers, teachers and library staff to manage online risks, so their experiences are safe and positive. Tailored advice and resources are provided through a website,[14] social media channels, a blog, and an online helpline for young people. In addition, the Cybersmart Outreach program offers face-to-face presentations for students, parents and teachers and professional development programs and training courses for teachers and pre-service teachers. The Cybersmart Outreach program covers a range of issues including the potential risks faced by children and young people when online, including identity theft, cyberbullying and inappropriate content.

Collaboration between the government and other sectors on cybersafety and digital citizenship education is growing in Australia and overseas. The ACMA's Cybersmart Digital Citizens Guide was developed following extensive consultation with eight Commonwealth agencies and fifteen industry stakeholders including Facebook, Google, Yahoo!7 and Microsoft. Its launch on 25 July 2013 was supported by a wide range of industry and community partners, both nationally and internationally, and represents consistent messaging about online safety.

The Digital Citizens Guide highlights the importance of individuals knowing how to protect their digital footprint and how to take action if their privacy is breached. The Guide aims to empower and inform citizens to prevent invasions of privacy online and help individuals to control their online experiences. The Guide encourages citizens to, amongst other things, set privacy and security settings and check them regularly as well as choose consciously when exchanging personal information online and ask permission if the content or image belongs to someone else.

Unsolicited communications

Spam Act 2003 and *Do Not Call Register Act 2006*

The ACMA administers a suite of legislation designed to minimise the impact on Australians of unsolicited telemarketing, fax marketing and commercial electronic messages (or spam), including emails, SMS, MMS and instant messaging.

The Spam Act was introduced to both reduce spam emanating from Australia and reduce spam coming to Australia from other sources. The operation of the Spam Act was reviewed in 2006 and it was found to be operating successfully.[15]

The Do Not Call Register was established in part in response to "rising community concerns about the inconvenience and intrusiveness of telemarketing of Australians, as well as concerns about the impact of telemarketing on individual's privacy."[16]

Privacy is a key concern in both of these types of unsolicited communications. In the case of telemarketing calls, the community concerns focus around intrusion on seclusion, intruding on everyday activities such as "getting the kids ready for school, to making the evening meal".[17] In relation to spam, concerns relate to the manner in which personal information such as email addresses are collected and handled.

The ACMA received nearly half a million direct complaints and reports in the 2012-2013 reporting year from members of the public about unsolicited

[14] www.cybersmart.gov.au

[15] Australian Government Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006).

[16] Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth), 1.

[17] Commonwealth, *Parliamentary Debates,* Senate, 19 June 2006, 82 (Eric Abetz).

communications. In the 2012 – 2013 reporting year, this included 411,017 contacts (complaints, reports and enquiries) from the public about spam and 19,677 telemarketing complaints. The ACMA completed 21 investigations into possible contraventions of the Spam Act and DNCR Act. The actions that the ACMA can take following a breach of the Spam Act, such as issuing a formal warning or issuing a formal warning, are directed at the industry operators rather than remedies for those affected.

The ACMA notes that as part of the 2008 ALRC review of the Privacy Act, the ALRC considered that both the Spam Act and DNCR Act were appropriate responses to public concern about unsolicited commercial electronic messages and telemarketing calls respectively.[18]

Telecommunications regulation

Protecting content of, and information about carriage services, including authorisations for accessing the Integrated Public Number Database

The ACMA has a role in protecting telecommunications consumer information under Part 13 of the Telecommunications Act. Customer information held by telecommunications carriers and carriage service providers (CSPs) is protected under Part 13 of the Telecommunications Act. Carriers and CSPs are prohibited from disclosing that information to other parties except in certain limited and restricted circumstances. These include assisting in investigations by law enforcement or national security agencies, the ACMA, Australian Competition and Consumer Commission, Telecommunications Industry Ombudsman or Telecommunications Universal Service Management Agency, assisting where there is an imminent threat to a person's life or health; and satisfying the business needs of other carriers and CSPs. The prohibition on disclosure is a criminal matter. The ACMA is required to include in its annual report information on disclosures of customer information made during the reporting year.

Part 13 of the Telecommunications Act provides for the ACMA to administer the Integrated Public Number Database (IPND) scheme. The IPND is an industry-wide database of all listed and unlisted public telephone numbers and their associated customer data. It was established in 1998 and is currently managed by Telstra under the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997.*

The ACMA also administers a determination under Part 4 of the Telecommunications Act that requires carriage service providers to undertake customer identity checking processes before activating prepaid mobile carriage services. The Determination[19] has been put in place to prevent the use of anonymous prepaid mobile services so that law enforcement and national security agencies can gain accurate information about the users of prepaid mobile service should they need to do so as part of their investigations. Identity checking requirements for prepaid mobile services also support the requirement on CSPs to contribute accurate information about customers to the IPND. To protect the privacy of individuals, mobile providers are only allowed to obtain the minimum amount of information that is reasonably necessary to verify identity.

Part 13 of the Telecommunications Act allows information contained in the IPND to be disclosed for the operation of law enforcement agencies, the emergency call service

---

[18] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report No 108 (2008) vol 3, 2520 [73.180] and 2522 [73.192].

[19] *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013* (the Determination replaced the *Telecommunications (Service Provider – Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000* with modifications to improve the arrangements for identity-checking of customers of prepaid mobile carriage services.)

and telephone-based emergency warning systems. The ACMA monitors compliance with IPND requirements for accurate customer data and is responsible for authorising access to the IPND, as well as for reporting on disclosure of IPND data for telephone-based emergency warning systems.

The ACMA has a different role in protecting telecommunications consumer information, under Part 26 of the Telecommunications Act relating to its responsibilities administering the telecommunications co-regulatory regime. The ACMA may investigate certain telecommunications matters under Part 26 of the Telecommunications Act. Under paragraph 510(1)(c) of the Telecommunications Act, the ACMA may, where it considers it desirable to do so, investigate contraventions of a code registered under Part 6 of the Telecommunications Act, or indeed any matter relating to the performance of the ACMA's telecommunications functions, or the exercise of the ACMA's telecommunication powers (except to the extent that the matter relates to the content of a content service).

The TCP Code was registered by the ACMA on 31 August 2013 (effective 1 September 2013). Clause 4.6.3 of the TCP Code requires a supplier to ensure that a customer's or former customer's personal information is protected from unauthorised use or disclosure and dealt with by the supplier in compliance with all applicable privacy laws. The TCP Code specifies a number of actions a supplier must take to enable this outcome. Similar privacy provisions have been available for a number of years, contained in the predecessors to the TCP Code.

The ACMA monitors compliance with the TCP Code through education, environmental scanning and investigations. An investigation is the final step before taking enforcement action under Part 26 of the Telecommunications Act. Where a supplier is found to have contravened the TCP Code, the ACMA may issue a formal warning (section 122 of the Telecommunications Act), or give the supplier a written notice (section 121 of the Telecommunications Act) directing the supplier to comply with all or part of the TCP Code.

The ACMA has taken action in response to incidents which have raised concerns about the privacy of telecommunications customer data. In September 2012, the ACMA formally directed a telecommunications provider to comply with the privacy clauses in the TCP Code.[20] This case is set out in Example 5 below. In April 2013, the ACMA issued a formal warning to a CSP for failing to protect the privacy of customer information. This case is discussed in Example 6 below. In response to an earlier incident involving another carrier, in December 2011, the ACMA issued directions requiring it to comply with the TCP Code provisions relating to protecting the privacy of customers' billing and related personal information.[21]

[20] ACMA Media Release, *Telstra directed under new code,* (8 October 2012) available at: http://www.acma.gov.au/Industry/Internet/Licensing--I-want-to-be-an-ISP/Telecommunications-consumer-protection-TCP-code/acma-issues-direction-to-telstra-under-new-code-i-acma

[21] ACMA Media Release, *ACMA issues directions to Vodafone,* (21 December 2011) available at: http://www.acma.gov.au/theACMA/acma-issues-directions-to-vodafone- i-acma

Example 5

The ACMA investigated a CSP's compliance with clause 6.8.1 of the TCP Code 2007, after it was discovered that customer personal information was publicly available on the internet. The incident was due to the CSP's web-based internal customer management tool not having appropriate safeguards or protections in place.

The CSP was found to be in breach of clause 6.8.1 of the TCP Code 2007 for failing to protect the privacy of the names, and in some cases the addresses, of approximately 734,000 customers, and the usernames and passwords of up to 41,000 of these customers. The ACMA issued a direction to comply with the TCP Code 2012 in September 2012.[22]

Example 6

The ACMA investigated a CSP's compliance with clause 6.8.1 of the TCP Code 2007 (a previous version of the code) after a server containing some of the CSP's customer records was hacked into and copied by a third party in July 2012. The data known to be copied included 13 instances of credit card details and 184 records of drivers licence numbers and dates of birth for small business customers. Further personal information on the server that may have been copied included names, Medicare numbers, addresses and email addresses.

The ACMA found that the CSP was in breach of clause 6.8.1 of the TCP Code 2007 by failing to protect the privacy of small business customers whose personal information was stored on the server which was the subject of the data breach. For the purposes of this investigation, the ACMA used the definition of personal information drawn from the *Privacy Act 1988*, as personal information was not specifically defined in the TCP Code 2007.

The ACMA issued a formal warning to the CSP for failing to protect the personal information of some of its small business customers.[23]

The Office of the Australian Information Commissioner (OAIC) also conducted an investigation and found that the CSP had breached the National Privacy Principles which are contained in the *Privacy Act 1988*. The CSP implemented the recommendations made by the OAIC[24] and the ACMA took no further enforcement action.

[22] ACMA Media Release, *Telstra directed under new code,* (8 October 2012) available at: http://www.acma.gov.au/Industry/Internet/Licensing--I-want-to-be-an-ISP/Telecommunications-consumer-protection-TCP-code/acma-issues-direction-to-telstra-under-new-code-i-acma

[23] ACMA Media Release, *AAPT warned about privacy,* (24 April 2013), available at: http://www.acma.gov.au/theACMA/Newsroom/Newsroom/Media-releases/acma-issues-formal-warning-to-aapt

[24] Office of the Australian Information Commissioner Media Release, *AAPT breached Privacy Act*, (15 October 2013) available at: http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/aapt-breached-privacy-act

Discussion of issues

Principles guiding reform

Question 1. What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

There are a number of legislative objectives and matters of regulatory policy underpinning the work of the ACMA that are relevant to the ALRC's proposed principles guiding reform.

As discussed earlier in relation to the ACMA's role in media and communications policy, the regulatory policy objects of both the Telecommunications Act and the BSAare to promote the use of industry co and self regulation and address public interest considerations respectively, in a way which does not impose unnecessary financial and administrative burdens.

In relation to the ALRC's principle of 'the balancing of privacy with other values and interests', the ACMA has direct practical experience in balancing privacy with other interests in the course of its regulatory duties. The following discussion illustrates how privacy interests have balanced against other values such as:

> safety

> informing the public on matters of public interest.

As well as balancing these values the ACMA also considers in the course of its decision-making

> regulatory certainty and consistency

> administrative efficiencies.

In its regulation of the emergency call service, the ACMA has struck a balance between privacy and safety. As discussed above, the privacy of customer data contained in the IPND is governed under Part 13 of the Telecommunications Act and Chapter 4 of the *Telecommunications (Interception and Access) Act 1979.* These Acts protect the privacy of information about telecommunications users whilst allowing for the use or disclosure of information in particular circumstances only, and subject to specific constraints. Such circumstances include law enforcement, national security, the provision of emergency services, approved research or the production of public number directories.

An example where there is a balancing of other interests with the protection of privacy is in the service provider determination requiring identity checks for prepaid mobile services as discussed above. The Determination enhances the privacy protections afforded to customers of prepaid mobile services by providing a range of choices about how their identity can be verified and imposing restrictions on the collection, recording and copying of personal information in the identity-checking process.

Another area where there is a balancing of interests is in the co-regulatory scheme applicable to the broadcasting industry. As explained in the Privacy Guidelines, the privacy provisions of the various broadcasting codes of conduct reflect the balance that must be struck between the media's role in informing the public of matters in the public interest and an individual's expectation of privacy.

The ACMA supports the ALRC principle of 'flexibility and adaptability'. As the Issues Paper notes, this relates to legislative design that is "sufficiently flexible to adapt to

rapidly changing technologies and capabilities without the need for constant amendments".[25] A similar principle is apparent in the regulatory policy of the BSA in relation to Parliament's intention that broadcasting and internet services be regulated in a manner that "will readily accommodate to technological change".[26] In telecommunications regulation, there is a policy concept of 'technology-neutral regulation', which is often referred to in the context of regulatory responses to the challenges of convergence. It refers to equal regulatory treatment of different information and communications infrastructure.

The ACMA also supports the principles of coherence in the law and consistency with other laws or regulatory regimes. Relevant to the principle of consistency is the concept of consistency in approach across the offline- and on-line environments. ACMA research to support its review of the Privacy Guidelines shows that some consumers expect the same privacy protections in both environments. Research participants considered that the privacy protections that apply to television and radio programming should be applied to the same content that is delivered via the internet. Participants did not distinguish between the same programming content that is delivered by different platforms or technologies. See Appendix A for further information about this research.

A statutory cause of action for serious invasion of privacy

Privacy and public interest

Question 7. How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that:

> competing public interests must be considered when determining whether there has been a serious invasion of privacy; or

> public interest is a defence to the statutory cause of action?

In applying the steps below the ACMA generally forms a view as to whether there has been a prima facie breach of privacy, and then considers other matters such as consent and the public interest. As outlined in the Privacy Guidelines, when investigating the alleged breach of a broadcasting code privacy provision, the ACMA, once satisfied that the broadcast attracted code privacy protections, will consider the elements of a breach as follows:

> was a person identifiable from the broadcast material?

> did the broadcast material disclose personal information or intrude upon the person's seclusion in more than a fleeting way?

If the answer to both of the above questions is yes, then there is a potential breach of code privacy provisions.

The ACMA will then consider:

> was the person's consent obtained—or that of a parent or guardian?

> was the broadcast material readily available from the public domain?

> was the invasion of privacy in the public interest?

If the answer to any of these is yes, then there will be no breach found.

[25] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era,* Issues Paper No 43, 9.

[26] Section 4 of the *Broadcasting Services Act 1992*.

Guidance on the meaning of 'public interest' is provided by the ACMA in the context of the privacy provisions of the broadcasting codes of practice, in the Privacy Guidelines. This guidance is informed by case law and ACMA investigations, and provides that:

- whether something is in the public interest will depend on all the circumstances, including whether a matter is capable of affecting the community at large so that citizens might be legitimately interested in or concerned about what is going on[27]
- public interest issues include public health and security; criminal activities; corruption; misleading the public; serious anti-social behaviour; politics; government and public administration; elections; and the conduct of corporations, businesses, trade unions and religious organisations
- not all matters that interest the public are in the public interest
- any material that invades a person's privacy in the public interest must directly or indirectly contribute to the public's capacity to assess an issue of importance to the public, and its knowledge and understanding of the overall subject.[28] The disclosure of the material should be proportionate and relevant to those issues, and not disclose peripheral facts or be excessively prolonged, detailed or salacious.[29]

Below are two recent case examples based on ACMA broadcasting investigations which illustrate how the ACMA considers the public interest, noting that the public interest is inherently considered in all investigations.

Example 7

In Investigation 2800,[30] the ACMA considered clause 4.3.5 of the *Commercial Television Industry Code of Practice 2010:*

> 4.3. In broadcasting news and current affairs programs, licensees:
> 4.3.5 must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, other than where there is an identifiable public interest reason for the material to be broadcast;

This aspect of the complaint related to the broadcast of an international driver's licence showing an individual's name, date of birth, place of birth and residential address in France.

In considering the complaint, the ACMA referred to a previous investigation in which it had taken the view that a person's residential address fell within what can be classified as an individual's personal or private affairs.

On the issue of whether the broadcast was within the public interest, the ACMA considered that the showing of the residential address did not, and could not, contribute to the public's knowledge and understanding of the issues canvassed. The ACMA considered that the inclusion of the street address was unnecessary and that there was no identifiable public interest in the inclusion.

[27] See *London Artists v Littler* (1969) 2 QB 375 at 391.

[28] This test is drawn from case law—*Allworth v John Fairfax Group Pty Ltd* (1993) 113 FLR 254 at 263; *London Artists v Littler* (1969) 2 QB 375 at 391.

[29] *Campbell v MGN Ltd* [2004] UKHL 22 at 164–165.

[30] Investigation 2800 available at: http://www.acma.gov.au/webwr/_assets/main/lib550063/tcn_sydney-report_2800.docx

Example 8

In Investigation 2773,[31] the ACMA considered clause 2.3(d) of the *Commercial Radio Australia Code of Practice 2011:*

2.3 In the preparation and presentation of current affairs programs a licensee must ensure that:

[...]

(d) the licensee does not use material relating to a person's personal or private affairs, or which invades an individual's privacy, unless there is a public interest in broadcasting such information

The complainant complained that their name and address was broadcast.

Having found that the individual was identifiable from the broadcast material, and that the material related to the person's personal or private affairs, the ACMA considered whether there was a public interest in the broadcast of the information.

The complainants name and address were announced in the course of describing an altercation outside the studio involving the complainant and the announcer. The ACMA found that there was no public interest in disclosing the identity of the complainant, particularly in the matter in which the complainant was described.

Example 9

In Investigation 2734,[32] the ACMA considered whether something was in the public interest in the context of considering whether the licensee breached paragraph 7(1)(h) of Schedule 2 of the BSA*:*

(1) Each commercial televisions broadcasting licence is subject to the following conditions:

(h) the licensee will not use broadcasting services in the commission of an offence against another Act or law of a State or Territory;

The complainant alleged that the licensee had breached section 45 of the *Invasions of Privacy Act 1971* (Qld)[33] by broadcasting footage and audio that was filmed with a hidden camera. In order to form a view as to whether the licensee had committed an offence against subsection 45(1), and thereby breached the licence condition in paragraph 7(1)(h) of Schedule 2 to the BSA, the ACMA must be satisfied, on the balance of probabilities, that:

> there was a 'private conversation'

> the licensee, through its employee or agent was a 'party to a private conversation'

> the licensee, through its employee or agent 'used a listening device to...record ...that conversation'

> the licensee subsequently communicate a record of the conversation made by the use of the listening device.

If all of the above criteria are met, the ACMA must be satisfied on the balance of probabilities that the communication or publication of the record of the private conversation was not more than was reasonably necessary in the public interest.[34]

[31] Investigation 2773 available at: http://www.acma.gov.au/~/media/Broadcasting%20Investigations/Radio%20investigations/Word%20document%20pre%202013/2GB%20ACMA%20Investigation%20Report%202773.docx

[32] Investigation 2773 available at: http://www.acma.gov.au/~/media/Broadcasting%20Investigations/Radio%20investigations/Word%20document%20pre%202013/2GB%20ACMA%20Investigation%20Report%202773.docx

[33] See: https://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InvasOfPrivA71.pdf

[34] This is having regard to subparagraph 45(2)(c)(i) of the *Invasions of Privacy Act 1971* (Qld).

The ACMA considered that the public interest in a story as a whole may not justify the broadcast of a private conversation in contravention of subsection 45(1) of the *Invasions of Privacy Act 1971* (Qld). The broadcast of the private conversation must be reasonably necessary to contribute to the public's knowledge and understanding of the issues involved in the overall subject, or be reasonably necessary for the protection of the public, or for some other genuine reason that furthers the public interest.

Briefly the broadcast involved a segment about an individual who had gone to a company to borrow some money, which, unbeknown to her at the time of signing the contract, actually involved the purchase and re-sale of diamonds. The individual concerned then took the matter to the Queensland Civil and Administrative Tribunal which ruled in her favour.

The ACMA considered that the purpose of the broadcasting of the private conversation was to demonstrate that the company was still offering the same type of commercial arrangements. The broadcasting demonstrated that the company and its employees were continuing to offer this particular finance facility and that by broadcasting the private conversation the public would have been alerted to the fact that the company was still engaging in this practice to avoid the operation of consumer credit legislation.

The ACMA found that the communication or publication of the conversation by the licensee was not more than was reasonably necessary in the public interest and therefore the licensee had not committed an offence and had therefore not breached the licence condition.

Defences and exemptions

Question 14. What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?

The Issues Paper outlines suggested defences to the statutory cause of action, which include another remedy being available in respect of the invasion of privacy, and that the information was already in the public domain.

The broadcasting co-regulatory scheme administered by the ACMA serves a different purpose to that of providing redress for the individual victim of a privacy invasion. Rather, it is directed at meeting the concerns of the broader community. Further, while the ACMA has a range of powers available to it in the context of broadcasting investigative process, these do not include the provision of damages for the aggrieved person or persons.

The ACMA's broadcasting investigation process may be relevant to considering the impact of the information already being in the public domain. As set out in the Privacy Guidelines, once a prima facie breach is established, the ACMA will consider whether the broadcast material was readily available from the public domain. If the answer to this is yes, then there will generally be no breach of the privacy code provisions. As outlined in the Privacy Guidelines, material that is already in the public domain includes material from online social media sites, unless access restrictions have been breached. The absence of access restrictions, while an important consideration, will not be determinative. Account will be taken of the nature of the material and the context in which it has been published. As the Privacy Guidelines explain, use by a broadcaster of material that has previously been disclosed by a person on a confidential basis, or to a limited or closed circle of recipients, may be an invasion of his or her privacy. Its private nature may be implied even if there was no express request to keep it confidential.

The issue of consent may be relevant to consideration of defences to a statutory cause of action. The ACMA's consideration of consent in the context of broadcasting investigation steps, discussed earlier above, may be of interest. The Privacy Guidelines explain how the ACMA considers the issue of consent, explaining that:

> if consent is obtained prior to the broadcast of material, then the person waives his or her claim to privacy protection[35]

> consent can be express, such as when obtained in writing. It can also be implied; for example, where a person is a willing participant in an interview

> if a person has actively drawn attention to material that would usually be considered private, this may be taken as consent

> there will be no waiver if consent is obtained by deception

> consent to the broadcast of private information or material that would breach privacy may be withdrawn before it is first broadcast, if in all the circumstances it is reasonable to do so

> the use of material that has been surreptitiously obtained will be an indicator that the person has not (at least at the time the material was obtained) consented to the broadcast. Consent to the use of such material can be obtained after recording but before broadcast

> the absence of an objection will not automatically be taken to be consent.

Consent is also central to the operation of the spam and Do Not Call regimes. For example, under the Spam Act, consent can be inferred from existing (business) relationships, or from the conspicuous publication of contact details. There are restrictions, however, on the use of contact details that have been conspicuously published: they may not be used when their publication is accompanied by a statement that the person does not wish to receive unsolicited communications, and they may only be used where the nature of the communication is directly related to the function, duties, office, position or role of the person.

Consent and the use of material in the public domain have been raised in the context of material sourced from social media websites. This issue has been considered in a recent ACMA investigation concerning a social media 'tribute' page, discussed in the example below, and in the ACMA's *Contemporary Community Safeguards Inquiry* (question 84).

[35] That consent should be 'informed consent'—voluntarily given by a (legally) competent person with an understanding of the matters agreed to.

Example 10

In Investigation 2584,[36] the ACMA considered clause 4.3.5 of the *Commercial Television Industry Code of Practice 2010*. The investigation concerned a news report on the sentencing of Mr X for the murder of Ms Y. The news report broadcast photographs of Ms Y and her family and friends, accessed from an open social networking page in tribute to Ms Y.

In this case, one of the questions for the ACMA was whether the publication of the photographs on an open group social networking website meant that they should not be regarded as relating to a person's personal or private affairs.

In finding that there was no breach of clause 4.3.5 of the code, the ACMA acknowledged the complainant's concern that the photographs were broadcast without the consent of the subjects of the photographs. However, the ACMA was of the view that the nature of the tribute page, the absence of privacy settings and the non-sensitive nature of the photographs meant that on this occasion, the licensee did not use material relating to a person's personal or private affairs.

However, the ACMA stated that this finding did not mean that licensees were free to broadcast any material available on the internet without risk of breaching the code, noting that material on the internet will not cease to be personal or private merely because it has been made publicly available through the absence of privacy settings or otherwise. While the ACMA considers that the use of privacy settings on social networking sites is an important consideration when assessing whether material from these sites constitutes private material, it is not determinative.

Question 15. What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?

The following information about the scope of provisions within the ACMAs areas of regulatory focus may be of interest in the ALRC's consideration of Question 15.

In the context of broadcasting, the ACMA notes that the privacy provisions of the commercial broadcasting codes are limited to news and current affairs programs. The result is that in cases where the complainant claims a privacy breach in other television content, for example reality television programs such as *Border Security,* the matter will be outside of the ACMA's jurisdiction, and cannot be investigated under the relevant Code.

Many of the privacy safeguards that apply to media and communications-related matters that are administered by the ACMA are specific to the particular medium. For example, program standards and codes of practice developed under Part 9 of the BSA do not cover content delivered using the internet or on-demand programs. Different codes and standards may apply to broadcasters and online content providers, even though the actual content and the devices on which it is being viewed may be identical. For example, if either a program or a film is shown on catch-up TV, it then falls under the BSA Schedule 7 definition of content, which means that, apart from MA content, it does not need to be classified or carry classification advice. These different applicable standards for the same content may be relevant to the ALRC's consideration of existing regulatory privacy protections, particularly in the context of the 'online' aspect of the ALRC's reference.

[36] Investigation 2584 available at: http://www.acma.gov.au/~/media/Broadcasting%20Investigations/TV%20investigations/pdf/Investigation%20Report%202584%20STQ%20Seven%20Local%20News.PDF

Growing pressure on the existing regulatory framework for privacy and personal data protection suggests that overall governance of the diverse suite of measures will become increasingly important. Responsibilities are fragmented across different regulatory bodies and levels of government, all of which have legitimate interests in maintaining the effectiveness of safeguards they administer. However, these arrangements mean it is sometimes uncertain where responsibility rests for emerging risks—particularly those associated with the media and communications sector. Emerging privacy concerns associated with technologies such as apps, cloud computing, and data analytics cut across the interests and responsibilities of several regulatory bodies. This can create uncertainty for determining where overall responsibility for privacy outcomes rests in each case.

Other remedies

Question 18. Other than monetary remedies and injunctions, what remedies should be available for serious invasion of privacy under a statutory cause of action?

As outlined earlier and explored further below, the ACMA has a number of different powers available to it. These powers depend on the applicable legislation. The ACMA notes that the Issues Paper mentions possible remedies for serious invasion of privacy under a statutory cause of action such as:

> an order requiring the defendant to apologise to the plaintiff

> a correction order

> an order for the delivery up

> destruction or removal of material

> an order that the defendant rectify its business or information technology practices.

The ACMA has experience in the effectiveness of some related powers, which may be of interest to the ALRC in considering what remedies should be available for serious invasion of privacy under a statutory cause of action. For example, take-down notices with respect to online content, facilitating compliance with requirements relating to business practices in the context of customer data and unsolicited communications investigations.

The ACMA has also undertaken research into community expectations about the applicability of some of these types of powers, for example on-air corrections in the context of broadcasting investigations and expectations generally regarding online content The ACMA's research on community expectations of privacy is set out at Appendix A.

Broadcasting Investigations

As outlined earlier, in the context of broadcasting investigations the ACMA has a range of powers available to it. Where a broadcaster (other than the ABC or SBS) is found to be in breach of the code of practice, the ACMA may:

> agree to measures to improve compliance that are proposed by the licensee

> accept an enforceable undertaking

> impose an additional licence condition.

Where there has been a breach of a licence condition, the ACMA may:[37]

> agree to accept a measure proposed by the licensee to improve compliance

> accept an enforceable undertaking

> issue a remedial direction

> vary or revoke a licence condition, or impose an additional licence condition.

[37] See generally Part 10, Division 3 and Part 14B of the *Broadcasting Services Act 1992*.

The ACMA cannot 'fine' or 'prosecute' a broadcaster for breaching a code, or direct it to do any particular thing (such as broadcast a report of the ACMA's findings, or broadcast an apology).

ACMA research[38] shows most viewers believe on-air corrections are an appropriate response to most breaches of broadcasting regulation, including industry codes of practice.

The ACMA notes that since July 2012 there have been three occasions where broadcasters have agreed to make on-air statements about the ACMA's breach findings. In Investigation 2934, the ACMA recommended to the broadcaster that it make an on-air statement acknowledging the ACMA findings. The broadcaster agreed to do so.[39] On-air statements about the ACMA's breach findings were also made in relation to Investigations 2730 and 2848.

Online content regulation

The ACMA's experience in issuing take-down notices may be relevant to possible remedies concerning the removal of material, although it is noted that where content is not hosted in Australia there may be limitations to potential approaches. Under the co-regulatory scheme that the ACMA administers in relation to online content, content/hosting service provider rules require content service providers to comply with ACMA notices and directions, including take-down notices issued in respect of prohibited online content. In the 2012-2013 reporting year the ACMA issued final take-down notices for five items of Australian-hosted prohibited content. All Australian hosting service providers complied with these notices. An example of an investigation resulting in a take-down notice is provided below. In respect of online content items hosted overseas, the ACMA does not have the power to issue take-down notices. The 1,845 overseas-hosted prohibited or potential prohibited items of content were referred to industry accredited optional end-user PC-based filters, while all illegal content was referred to law enforcement.

Example 11

In late December 2012, the ACMA received a valid complaint from an Australian resident about potential online child sexual abuse material hosted in Australia. As part of its investigation, the ACMA applied to have the content formally classified by the Classification Board (all Australian-hosted content must be formally classified prior to the ACMA issuing a final take-down notice). The content was refused classification (RC) by the Classification Board and was therefore prohibited under the BSA.

Given the nature of the material and in line with legislative provisions, the ACMA sought confirmation from law enforcement that issuing a take-down notice would not prejudice a criminal investigation. Upon receiving this confirmation, the ACMA issued a final take-down notice to the content service provider. The content was removed within hours of the notice being issued.

[38] ACMA, *Community Attitudes to the presentation of factual material and viewpoints in commercial current affairs programs*, August 2009 available at: http://www.acma.gov.au/webwr/_assets/main/lib100068/current_affairs_program_research_part-01_executive_report.pdf

[39] ACMA Media Release, *ACA breach A Current Affair breaches code,* (13 September 2013), available at: http://www.acma.gov.au/theACMA/Newsroom/Newsroom/Media-releases/a-current-affair-breaches-code

Unsolicited Communications

If the ACMA carries out an investigation and makes a finding that a person has breached the DNCR Act, the *Telemarketing and Research Industry Standard 2007*, the *Fax Marketing Industry Standard 2011,* or the Spam Act it has the following enforcement options available:

> issue a formal warning

> accept an enforceable undertaking from a person or company—these undertakings usually contain a formal commitment to review or change business processes to facilitate compliance with the Act. A failure to abide by an undertaking can lead to the ACMA applying for an order in the Federal Court

> issue infringement notices

> commence proceedings against a person or company in the Federal Court.

Under the Spam Act penalties of up to $1.7 million/day apply to repeat corporate offenders.

Example 12

In October 2012, the ACMA accepted an enforceable undertaking[40] and received payment of an infringement notice from a business that had failed to unsubscribe customers from marketing emails.

The failure to unsubscribe customers was despite customers' repeated requests to be removed from mailing lists, as well as several warnings from the ACMA.

In its enforceable undertaking, the business committed to ensuring its unsubscribe facilities are functional and effective.

Privacy of customer data

In response to concerns about a number of incidents and allegations of unauthorised access to customer information, the ACMA wrote to eight carriage service providers.[41] The ACMA wrote requesting information about the business practices that the carriage service providers had in places to address privacy incidents.

The ACMA made use of this information in developing *Better practice privacy tips for service providers*[42] which were released in July 2012 to help carriage service providers and internet service providers formulate privacy policies, initiate and sustain good practice and respond appropriately to a privacy breach. The document complements the provisions in section 4.6.3 of the current TCP Code which compel service providers to protect the personal information of their customers and former customers.

As discussed above, the ACMA has a range of other actions available to it in response to allegations of unauthorised use or disclosure of customer information. The ACMA monitors TCP code compliance through education, environmental scanning and investigations. In response to TCP Code breaches, the ACMA may issue a formal warning or give the supplier a written notice directing the supplier to comply with all or part of the TCP Code.

---

[40] ACMA Media Release, *Tiger Airways breaches Spam Act,* (25 October 2013), available at: http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/tiger-airways-breaches-spam-act

[41] For example, a report on 9 January 2011 in the Sydney Sun Herald alleging personal details of Vodafone customers had been made available on the Internet.

[42] Available here: http://www.acma.gov.au/theACMA/better-practice-privacy-tips-for-service-providers

The ACMA considers that these alternative actions which focus on facilitating compliance provide good regulatory outcomes and good outcomes for consumers.

Systemic breaches

The Issues Paper[43] canvasses the scenario whereby a serious invasion of privacy may result from systemic problems with processes or technology. As indicated in the examples provided above (see Examples 5 and 6), the ACMA has experience in investigating matters relating to systemic problems, particularly in relation to customer data held by carriers and CSPs. Similarly, because of the nature of spam, investigations under the Spam Act often result in findings that breaches are indicative of broader systemic issues.

The ACMA considers that as part of developing a coherent approach to regulation, the existing regulatory schemes should be carefully examined in designing the proposed statutory cause of action. If systemic issues are covered by the proposed cause of action, and where a systemic issue is in fact identified, there may be benefit in allowing the court to consider remedies which may include an order that the defendant rectify its business or information technology practices. However, as the Issues Paper suggests, it may be more appropriate for systemic breaches to be addressed by regulatory schemes where compliance can be monitored.

As discussed earlier, the ACMA undertakes compliance monitoring and has the ability to take enforcement action in relation to the unauthorised disclosure of telecommunications customer information, which has recently been exercised in relation to a number of systemic issues with CSP business processes and information technology systems. Further, the ACMA's investigations of potential contraventions of the Spam Act and DNCR Act may result in an enforceable undertaking which requires a business to audit information contained in its contact databases, or the processes under which it engages in e-marketing or telemarketing (as illustrated in Example 12 above).

Who may bring a cause of action?

The argument is sometimes made that because there are existing laws on certain matters there is no need for broadcasting code interventions in relation to those matters.

However, the current drafting of complaint provisions in the broadcasting codes of practice allows any person to complain under the codes–whether or not they have been directly affected by the broadcast content (for example, even if it was not their privacy that was impacted). This broad right to complain is consistent with the provisions of the BSA relating to encouraging broadcasters to meet *community* standards, by allowing individuals to complain on behalf of the community. The complaint is an important mechanism which enlivens the regulatory safeguards and frameworks that are embodied in the codes.

The broadcasting codes of practice therefore serve a different purpose to that of legal proceedings brought by an individual. For example, under (non-broadcasting) legislation, the power to complain is generally limited to victims, who can show that they have a grievance that is beyond that which will be suffered by an ordinary member of the public. In this example, the non-broadcasting legislative interventions prioritise resolving claims as individual, interpersonal disputes, whereas the industry-specific codes of practice are aimed at meeting community concerns, which may be raised by any person, not just the affected individual.

[43] At paragraph 100.

Question 20. Should the Privacy Commissioner, or some other independent body, be able to bring an action in respect of the serious invasion of privacy of an individual or individuals?

Providing for some independent body such as the Privacy Commissioner to bring an action in respect of a serious invasion of privacy of an individual or individuals in certain circumstances may reflect a similar approach to that of the industry-specific regulation administered by the ACMA; in that it acknowledges that there is a broader public interest in the protection of privacy beyond the interest that the aggrieved individual or individuals may have.

Interaction with existing complaints processes

Question 25. Should a person who has received a determination in response to a complaint relating to an invasion of privacy under existing legislation be permitted to bring or continue a claim based on the statutory cause of action?

The ACMA receives and investigates privacy complaints under the broadcasting co-regulatory scheme, the spam and Do Not Call schemes, and the privacy provisions of the TCP Code. In certain areas, the ACMA may instigate its own investigation without having received a complaint from a member of the public, for example the ACMA initiated an investigation into the protection of customers' personal information (as required by the TCP Code) by a CSP following media reports that some customer data had been 'stolen'.[44] In another example, the ACMA decided to exercise its discretionary powers under section 170 of the BSA to commence an 'own motion' investigation in relation to the broadcast of a prank radio call.[45] The overarching consideration for the ACMA in deciding whether to exercise its discretion to open an 'own motion' investigation under section 170 of the BSA is whether it is in the public interest to do so. While the discretion is broad, matters that the ACMA could consider relevant to that question might include:

> whether the matter is most efficiently and effectively dealt with by an 'own motion' investigation
> whether the matter is serious or significant, or the conduct ongoing
> whether the licensee involved has been the subject of prior action by the ACMA
> whether the conduct suggests a poor compliance culture on the part of the licensee.

Even in circumstances where a matter is relatively low profile or routine, the ACMA might consider an 'own motion' investigation to be appropriate in the circumstances. However, it is the ACMA's experience that, in most circumstances, the public interest can be served by allowing the normal co-regulatory complaint processes to proceed.

The nature of ACMA processes is relevant in considering the potential interaction between a statutory cause of action and the existing regulatory regime governing privacy in Australia. In contrast to legal proceedings, there is no 'onus of proof' or 'burden of proof' in investigations undertaken by the ACMA under the BSA. These are concepts which arise in judicial processes. Judicial processes are typically adversarial

[44] ACMA Media Release, *AAPT warned about privacy,* (24 April 2013), available at: http://www.acma.gov.au/theACMA/Newsroom/Newsroom/Media-releases/acma-issues-formal-warning-to-aapt

[45] ACMA Media Release, *ACMA to investigated 2DayFM prank call broadcast,* (13 December 2012), available at: http://www.acma.gov.au/Industry/Broadcast/Radio-Commercial--ABC--SBS/Radio-content-regulation/mr-972012-acma-to-investigate-2dayfm-prank-call-broadcast

in nature. The courts have established rules and procedures, which include rules of evidence, that apply to their proceedings.

In the context of the ACMA's role in broadcasting investigations, the interaction between ACMA investigative processes and other formal legal proceedings is contemplated. For example, clause 7.16 of the *Commercial Television Industry Code of Practice 2010* applies when a matter raised by a complainant becomes the subject of legal proceedings. Clause 7.16 provids that the licensee (broadcaster) is not required to provide a substantive written response in respect of the matter, but must acknowledge the complaint in writing and inform the complainant that they may make a complaint to the ACMA.

Further, the BSA[46] provides that in the context of publication or report on investigations, the ACMA is not required to publish, or disclose to a person to whose affairs it relates, a report if it would be likely to prejudice the fair trial of a person. Similar provisions apply to the inclusion of material in reports on hearings.[47]

The ACMA considers that the ability to investigate breaches of a broadcasting code of practice and take action is a complement, rather than replacement of the ability of the individuals who suffered to also seek individual redress.

Other legal remedies to prevent and redress serious invasions of privacy

Given the challenges in providing adequate forms of redress for invasions of privacy, innovative approaches for providing redress and preventing privacy invasions are particularly important. The ACMA suggests that harmonisation, self-regulation, and education programs may provide examples of innovative ways in which the law, or alternative approaches, might assist in providing redress or preventing serious invasions of privacy in the digital era.

[46] See section 179(3)(b) of the *Broadcasting Services Act 1992*.

[47] See section 199(3) of the *Broadcasting Services Act 1992*.

Appendix A – ACMA Privacy Research

Recent ACMA papers have explored media and communications technological developments and associated changes in consumer behaviour, and the changing context this provides for privacy and digital data protection. ACMA research has also examined community perceptions of privacy and expectations regarding regulatory safeguards for privacy.

Insights from ACMA research are provided below. Unless indicated otherwise in the footnotes, all publications are available on the ACMA website at: http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/acma-research-and-publications

The changing context for privacy

Research from the ACMA and other sources shows that Australians are undertaking an increasing range of social and economic activities online, including the creation of significant amounts of digital content. Australians are going online more frequently, and are spending more time online.[48] Seventy-three per cent of Australians access the internet more than once a day as at June 2012, up from 61 per cent in June 2010. Social networking and user-generated content sites account for a large proportion of the time spent online by internet users in Australia, with 34 per cent of the population accessing Facebook and spending an average of seven hours and 41 minutes per person on it during June 2012.[49]

Digital data is an underpinning for social and economic transactions in the networked society and information economy. Internet-connected devices such as smartphones and tablets are now often equipped with audiovisual recording capabilities, sensors for location data and near-field communications, and new wireless networking capabilities. These devices allow data about individuals' behaviour and preferences to be recorded, related to other data stored on the devices and to be exchanged on a near-continuous basis.

With the rapid update of smartphones and tablets, app purchase and usage are quickly becoming mainstream media and communications activities.[50] The number of Australian adult consumers with a smartphone who downloaded apps increased by 85 per cent from 2.41 million in June 2011 to 4.45 million in June 2012. Mobile apps are shaping the ways citizens share their personal information. Privacy-related concerns for apps mirror those in the wider online environment, with the added dimension of the personal and portable nature of the devices on which the apps run.

The nature of personal information is changing, with information about an individual's search history, social connections, interests, purchasing history, location, calendars and contact sources able to be stored on digital devices. Increasingly, this personal data is being stored in the cloud, with 71 per cent of Australians now using a cloud service to share digital information online.[51]

---

[48] ACMA, *Communications Report 2-Australia's progress in the digital economy: Participation, trust and confidence,* November 2012.

[49] ABS, ABS 8153.0-Internet Activity, Australia, June 2012.

[50] ACMA, *Mobile apps, Emerging issues in media and communications, Occasional paper 1,* May 2013.

[51] ACMA, *The cloud: services, computing and digital data, Emerging issues in media and communications, Occasional paper 3,* June 2013.

Personal information has a particular meaning for the purposes of privacy and communications data protections.[52] Digital data that underpins this information can be categorised three main types:

> volunteered—that is, data created and explicitly shared by the individual, such as data posted on social networking services (SNSs)

> observed—includes data harvested about an individual, such as their current location, or data harvested from third parties, such as an individual's purchasing history

> inferred—individuals volunteered and observed data that is processed to produce a new source of information and anonymised data that relates to groups of individuals, such as groups of individuals who 'like' the same activity.

Current data practices now support inferred information about personal behaviour and preferences. This does not directly or indirectly identify a person and is a category of digital data which has ambiguous status within the privacy regulatory framework.

ACMA research on community perceptions of privacy

Community attitudes to broadcasting privacy issues

This research explored privacy issues that arise in broadcast news and current affairs programs and radio competitions, with some coverage of online media content.[53] This was a major research project that informed the review of the ACMA's *Privacy Guidelines for Broadcasters*. The research examined attitudes to potential intrusions of privacy in broadcasts that:

> occur in public spaces

> involve highly sensitive personal situations

> involve children and other vulnerable people

> involve public figures

> use private material or information from online social media sites and public records

> use hidden recording devices

The qualitative phase of the research revealed that community attitudes to these scenarios are complex and nuanced. The research indicated that privacy issues are evaluated by individuals on a case-by-case basis. They are influenced by individual ethics, and particular circumstances such as whether consent was given.

In terms of scenarios involving digital technologies or surveillance, it was found that:

> many research participants do not consider the broadcast of personal material from a social networking site to be an intrusion of privacy, unless privacy controls had been set by the individual and overridden by the broadcaster. This was supported by the quantitative research.

> participants considered that the same privacy protections that apply to television and radio programming should be applied to the same content that is delivered via the internet. Participants do not distinguish between the same programming content that is delivered by different platforms or technologies.

> in the quantitative research, the majority of media users believe that showing extensive footage of a person grieving, using a hidden camera, or revealing

[52] For a more detailed discussion see: ACMA, *Privacy and personal data: Emerging issues in media and communications, Occasional paper 4*, June 2013.

[53] ACMA, *Community Research into Broadcasting and Media Privacy,* August 2011 and ACMA, *Australian's views on privacy in broadcast news and current affairs: Complementary survey report,* August 2011.

information about a person's sexual preferences are 'very intrusive' of personal privacy.

Young Australians' attitudes towards privacy and social media

The ACMA's 2013 report, *Like, Post, Share: Young Australians experience of social* media indicates that Australian children and young people are taking steps to protect their privacy when they use the internet and social media.[54] The majority of 12 to17-year-olds are setting their social networking profiles to private and the proportion who are doing so increases with age. Young people are taking steps to protect their privacy by using privacy settings, deleting tags and comments as well as thinking twice before posting things they may regret.

In the qualitative first phase of the research, it was found that risks to privacy are generally only seen in the 'immediate', as relating to here-and-now personal safety questions. Most felt they were pretty much in control of their privacy, and demonstrated a strong theoretical understanding of what to do and what not to do. However, some opted not to put limits on their personal information, believing that risks are not difficult to avoid. There was a view expressed that online risks are not significant unless they move into the offline space.

Key findings from the quantitative phase of the research include:

> seventy per cent of eight to nine year olds have not posted any personal information online

> fifty eight per cent of 14 to 15-year-olds have their profiles fully private; and a further 21 per cent are partially private

> sixty six per cent of 16 to 17-year-olds have their profiles set to fully private, with a further 26 per cent partially private

> the use of private messaging is becoming increasingly commonplace, especially among older teens, with 89 per cent of 16-17 year olds surveyed reporting they had sent private messages in the last four weeks.

> most young people reported having taken action to protect their privacy on social network services. Older teenagers were more likely than younger teenagers to report managing their privacy by taking actions such as removing tags from photos, deleting people from friends list and deleting comments.

The research indicated that, on the whole, it seems that many Australian children and young people are aware of the need to stay safe and secure online. They acknowledge the importance of protecting their online privacy, and are actively taking steps to stay in control of the personal information they make public.

However, the research also found that while many are putting practical measures into place—setting their profiles to private, sharing passwords predominantly with parents rather than with others—children and young people from eight to 17 years of age are taking privacy risks such as sharing personal information and looking for new friends on the internet, and adding people they have never met face-to-face. While some of this may be inadvertent (for example, through unfamiliarity with the location-based capabilities of their smartphones or the actions of their friends) a significant proportion is self-initiated.

---

[54] ACMA, *Like, post, share–short report: Young Australians and online privacy,* May 2013. Available on the ACMA website at:
http://www.cybersmart.gov.au/About%20Cybersmart/Research/~/media/Cybersmart/About%20Cybersmart/Research/Research%20from%20the%20ACMA/Like-post-share-Young-Australians-and-online-privacy.pdf

The full report, to be published later this year, sets out the findings from the qualitative and quantitative phases of the research.

The research points to the importance of ensuring that children are given the information, skills and tools they need to be safe and secure digital citizens, through programs such as the ACMA's Cybersmart, working in partnership with families, schools, industry and other stakeholders.

Digital identities and footprints – community attitudinal research

This research examines citizens' attitudes towards the management of their digital identities and digital footprints.[55] Attitudes to different types of personal information and risks in the online environment were also explored.

Australians are establishing digital identities comprised of the credentials they use to identify themselves to service providers and the digital footprints that are created as a by-product of their various online transactions. Individuals may maintain several digital identities, each to be used in specific transactional, professional or social contexts. The vast majority of participants (80 per cent) indicated that disclosure of private information that resulted in damage to their reputation would be sufficient to cause them to stop using a service.

Almost half of Australians adopt a 'digital disguise' as a protective strategy to manage their digital footprint, by sometimes giving incorrect personal information to use a site, application or service. With 64 per cent of 18 to 24-year-olds saying that they would provide incorrect personal details to some services, this may erode the value of data collected during transactions.

Nearly all survey participants acknowledged they had some degree of control over their privacy through tools made available by providers of devices, browsers and applications. Around 40 per cent of survey participants were confident in using their preferred privacy settings, almost as many 'hope they work' (37.9 per cent), and 19 per cent are less confident.

Community experiences of unsolicited telemarketing calls and spam

The majority of Australians has received one or more unsolicited telemarketing calls in the past 6 months, and one or more email or SMS spam in the past month.[56] The majority of those receiving such unsolicited communications perceived them as a problem.

There were a variety of reasons why unsolicited communications were considered to be a problem. 'Invasion of privacy' was a reason given by 10 per cent of those who received SMS spam, and 'interruptions to peace and quiet' was a reason given by 9 per cent of those who received unsolicited telemarketing calls. Telemarketing calls and SMS spam were seen are more intrusive than email spam.

---

[55] ACMA, *Digital footprints and identities,* November 2013. Available at: http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/digital-footprints-long-report-landing

[56] ACMA, *Unsolicited telemarketing calls & spam: Consumer experiences,* November 2013. Available at: http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Research/pdf/Telemarketing%20and%20spam_Consumer%20experiences_Final%20pdf.pdf