Australian Government | acma

Australian Communications and Media Authority

Red Building
Benjamin Offices
Chan Street
Belconnen ACT 2617

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555

acma.gov.au

Chair and Agency Head

Privacy Act Review
Integrity and Security Division
Integrity and International Group
3-5 National Circuit Barton ACT

Email: PrivacyActReview@ag.gov.au

ACMA file reference: ED20/62442

Submission to Privacy Act Review

The Australian Communications and Media Authority (ACMA) welcomes the opportunity to make a submission to the Attorney-General's Department Privacy Act Review (the Review). The ACMA is actively engaged with the delivery of public policy outcomes in a technologically dynamic environment and, in this context, administers consumer safeguards that complement or directly intersect with the *Privacy Act 1988* (Privacy Act) and are relevant to the matters raised in the Review Issues Paper.

This submission is primarily focussed on information relevant to the part of the Review focussed on the interaction of the Privacy Act and other regulatory schemes and, to that end:

> sets out ACMA research data of potential interest to the Review
> outlines key safeguards administered by the ACMA with strong privacy-related considerations
> discusses privacy-related issues concerning the current unsolicited communications frameworks regulated by the ACMA.

Background

The ACMA is the independent statutory authority responsible for the regulation of broadcasting, radiocommunications, telecommunications and certain online content. This includes responsibility for regulating spam, telemarketing, and interactive gambling.

The ACMA regulates in accordance with four principal acts – the *Radiocommunications Act 1992*, the *Telecommunications (Consumer Protection and Service Standards) Act 1999*, *Broadcasting Services Act 1992* (Broadcasting Services Act), and the *Telecommunications Act 1997* (Telecommunications Act). It also has key responsibilities under the *Interactive Gambling Act 2001* (Interactive Gambling Act), the *Spam Act 2003* (Spam Act) and the *Do Not Call Register Act 2006* (DNCR Act).

ACMA Research and experience

As the Review Issues Paper identified, with Australians spending more of their time online and new emerging technologies changing the way people interact and do business, regulatory frameworks and settings must be contemporised so that they remain fit-for-purpose in the changing digital environment.

Communications services are essential and are increasingly at the centre of our economy and society. Access to telecommunications is deeply ingrained in the way Australians live, work, learn and play.

Recent ACMA research and consumer survey data showed that in the preceding six months to June 2020:

> 98% of Australian adults had used a mobile phone to make a call

> 92% had sent a text message

> 77% had used an app to communicate via messages, voice or video calls (up from 67% in 2019).[1]

In 2020, more Australian adults accessed viewing and listening services over the internet compared to 2019. From 2019 to 2020, watching online subscription services and catch-up TV increased, while viewing 'live' free-to-air TV continued to decrease. In particular, 77% of Australian internet users had a subscription and/or pay-per-view service in their household in 2020 (up from 70% in 2019).[2]

Telecommunications networks now deliver a multitude of highly attractive services, supplied by over-the-top providers and facilitated by increasingly sophisticated devices, such as smart phones and smart TVs. These services also collect data, much of it being personal data, to further refine and target their service offerings. The increasingly widespread deployment of Internet of Things networks and devices is expected to support new service delivery.[3]

Privacy is a matter of enduring relevance in the media and communications environment. While digital technologies and social media may be changing the 'privacy environment' and presenting challenges that legal experts have grappled with in recent times, the community continues to value privacy safeguards in broadcasting and telecommunications.[4]

In addition to the factors identified in the Issues Paper, ACMA data and research reveals Australians are sensitive to breaches of privacy and how information about them is collected, shared and monetised. Consumer research conducted in 2018 identified that Australian consumers want more control over when and how they give consent.[5]

The ACMA also sees strong indications (through compliance data and enforcement outcomes), that consumers and industry are confused by the current complexity and inconsistencies in the way consent is dealt with across the unsolicited communications laws and Australian Privacy Principle 7 (APP7) – which covers direct marketing.[6]

Collection and sharing of personal information and device privacy/security

Recent ACMA research specifically explored levels of awareness and concern around data privacy, and the sharing and use of personal information that is collected from users of mobile phone and mobile broadband services.[7]

Consumers had high levels of concern about sharing personal information. Around three quarters of Australian adults with mobile services were concerned about sharing personal information online (79%), or that the organisation they provided their data to might share it (73%).

---

[1] ACMA, 2020, *Trends in online behaviour and technology usage: ACMA consumer survey 2020*, viewed 13 November 2020.

[2] ibid.

[3] ACMA, 2020, *Communications report 2018–19*, viewed 16 November 2020.

[4] For example, the Australian Law Reform Commission Final Report into Serious Invasions of Privacy in the Digital Era (September 2014).

[5] ACMA, 2018, Unsolicited calls in Australia Consumer research, viewed 13 November 2020.

[6] ACMA, 2018, *Report on industry self-regulation of commercial electronic messages, the Do Not Call Register and the Integrated Public Number Database*, viewed 12 November 2020.

[7] ACMA, 2020, *Telco consumer experience – Australian adults and households: Phone and internet services*, viewed 12 November 2020.

Two thirds of Australian adults with mobile services were concerned about the ability for their device's location to be shared or that their mobile phone was listening to their conversations (62%). Less than half (45%) agreed that they were aware of what happens to their personal information after it is shared online, with 39% not aware.

For the two thirds of households with at least one smart device, there were low to moderate levels of awareness of how to manage their smart devices. Around 6 in 10 (63%) agreed they knew how to make their smart devices private and secure, with 25% not aware. A similar proportion (60%) were concerned about the amount of information smart devices were collecting. Just over half (54%) agreed that they would know how to remove personal information before disposing of a smart device, with 35% not aware. Nearly half (48%) agreed that they are aware of the amount of information smart devices are collecting, with 37% not aware.

Only 3 in 10 (28%) households with smart devices agreed that there was enough transparency to understand how smart devices use information, and 54% disagreed.

The application of consent within the unsolicited communications frameworks

Mobile phones are the most common telecommunication device for Australians. Nearly all Australian adults are using their phones beyond calling and messaging; using them for activities such as navigating with maps, doing their banking and paying bills, accessing emails, social media, news and/or audio content. While use for these activities is often higher in younger age groups, many older Australians are also engaging in these activities.[8]

The intrusion of telemarketing calls and commercial electronic messages remains a key concern for people. Consumers see poor alignment between the commercial and public interests involved in unsolicited communications; they feel that industry should do more, with government's role to ensure this happens through regulation.[9]

Preferences and expectations for managing unsolicited communications have evolved as consumers are influenced by the rapid developments in technology and the convergence of communications services. Consumers want increased personal agency in managing communications, especially as they can be received on devices at any time.

Consumers also expect privacy protections to be in place on connected digital platforms. They want to choose the communications they receive. Consent – express, implied, inferred, withdrawal – and its duration is confusing to many consumers as they are often not clear when and to whom they gave consent, and how it may then be used across multiple platforms and channels. The challenges consumers face in understanding the application of their consent, along with their desire to exert more individual control, present a driver for consideration of regulatory reform and harmonisation of consent arrangements as they apply to data and marketing.

Privacy in the media and communications frameworks

The ACMA has significant experience regulating privacy matters given its responsibilities under the Broadcasting Services Act, Telecommunications Act, Spam Act, the DNCR Act, and associated industry standards and codes in force. These provide substantial privacy safeguards for Australians who use media and communications services. Key examples include:

[8] ibid.

[9] ACMA, 2018, *Report on industry self-regulation of commercial electronic messages, the Do Not Call Register and the Integrated Public Number Database*, viewed 12 November 2020.

- Privacy protections specific to broadcasting are set out in various codes of practice that are developed in accordance with the Broadcasting Services Act by industry and registered by (or, in the case of the national broadcasting codes, notified to) the ACMA.[10] Some codes offer express privacy protections only in the context of news and current affairs broadcasts. Other codes offer privacy protections for all broadcast content. Some codes also provide that a complaint about privacy matters can only be made by the person (or a representative of the person) who considers their privacy was intruded upon.[11]

- Both the ACMA and the Office of the Australian Information Commissioner (OAIC) have responsibilities in respect of compliance with Part 13 of the Telecommunications Act. The OAIC is responsible for monitoring compliance with Division 5 of Part 13, while the ACMA has the power to investigate contraventions to determine if a telco has complied with carrier licence conditions or service provider rules. Privacy protections under Part 13 of the Telecommunications Act include prohibiting the use and disclosure of personal information, including any information relating to the contents or substance of a communication in the telecommunications industry.

- Specific and related provisions apply to carriers and carriage service providers under the Telecommunications Consumer Protections Code (C628:9019)[12] to protect customer personal information from unauthorised use or disclosure. This code is registered by the ACMA under section 117 of the Telecommunications Act.

- The Telecommunications Integrated Public Number Database Scheme 2017 and Telecommunication Regulations 2001 provide access to personal information held in the Integrated Public Number Database (IPND) to specific entities, including emergency services, research entities and public number directory publishers. The latter two entities access IPND data by authorisation granted by the ACMA upon application. Due to the nature of the information held and its potential uses, both instruments contain various privacy-related provisions including that applicants conduct privacy impact assessments.

- The objectives of the DNCR Act and Spam Act (and associated instruments) are to prevent unwanted intrusion on the privacy of individuals. Both are framed around constructs of consent that mirror the consent provisions within privacy legislation, noting that there are subtle, but important, distinctions (see below for discussion on this point). Schedule 1, clause 7 to the Privacy Act, that deals with Australian Privacy Principle 7 (APP7) – direct marketing – sets out that the principle does not apply to the extent that the DNCR Act and Spam Act apply.

- APP7 also does not apply to the extent that Division 5 of Part 7B of the Interactive Gambling Act applies. This part of that act sets out prohibitions against direct marketing by licenced interactive wagering providers to individuals registered on the Nation Self-Exclusion Register (NSER). The ACMA is currently developing the NSER.

[10] The various broadcasting codes of practice can be accessed on the ACMA website.

[11] Commercial Television Industry Code of Practice 2015; SBS Codes of Practice 2014 (revised in July 2019). The Commercial Radio Code of Practice 2017 provides that complaints about privacy may only be made by the person (or an *authorised* representative of the person) who considers their privacy was intruded upon. The ABC Code of Practice 2019 limits complaints in relation to privacy provisions to people who have 'sufficient interest in the subject matter of the complaint'.

[12] The Telecommunications Consumer Protections Code can be accessed on the ACMA website.

In relation to broadcasting matters, the ACMA publishes guidance[13] on the application of privacy provisions. These explore how the ACMA has applied privacy code rules in compliance investigations including in relation to the privacy of children, privacy of people experiencing trauma or grief, and the use of video and other material from social media, mobile phones and messaging apps containing personal information or divulging matters related to an individual's private affairs.

The ACMA also directly interacts with the Privacy Act and OAIC in the undertaking of a broad range of its functions. For example, before the ACMA can register a telecommunications industry code which deals directly or indirectly with a matter dealt with by the Privacy Act, it must consult the Information Commissioner to ensure he or she is satisfied. Section 116A of the Telecommunications Act also specifies that 'Neither an industry code nor an industry standard derogates from a requirement made by or under the *Privacy Act 1988* or a registered APP code (as defined in that Act)'.

Opportunity for harmonisation of consent frameworks

The ACMA regulates unsolicited communications primarily under the Spam Act and DNCR Act – which are complemented by the Do Not Call Regulations 2017, the Spam Regulations 2004, the Telecommunications (Telemarketing and Research Calls) Industry Standard 2017 and the Fax Marketing Industry Standard 2011 – while other forms of direct marketing are regulated under APP7. Specifically:

> the DNCR Act allows consumers to 'opt-out' of receiving telemarketing calls by placing their numbers on the Do Not Call Register

> the Spam Act prohibits the sending of commercial electronic messages unless the sender has consent in relation to the recipient

> the Telecommunications Act provides compliance and enforcement powers, and specifies mandatory industry standards for all telemarketing and fax marketing

> APP7 in the Privacy Act regulates direct marketing – to the extent the DNCR Act and Spam Act do not apply.

Consent, consent duration and withdrawal of consent are framed differently and, in some cases, inconsistently across the relevant acts. For example, the DNCR Act and Spam Act provide for 'express' and 'inferred' consent, while the Privacy Act provides for 'express' and 'implied' consent. The privacy regime sets out specific principles that apply to consent, while the unsolicited communications regimes do not.

The differences can be incongruous and confusing for consumers, especially when marketing communications are received on the one device.[14] This is evident through the ACMA's compliance and enforcement work, which shows consumers do not always understand when they have given consent, for what purposes, its duration and how it can be withdrawn.

Further, the convergence of communications channels has led to the blurring of traditional business marketing models across platforms to create consumer and industry confusion about the application of current unsolicited communications safeguards. Specifically, an increasingly complex array of consent-based marketing practices and business relationships ('affiliate marketing') are being regulated under arrangements that contemplated more direct relationships (essentially, much shorter supply chains), including in relation to obtaining and using consent.

[13] The ACMA's Privacy guidelines for broadcasters can be accessed on the ACMA website.

[14] ibid.

There is currently no uniform or universal rule requiring entities to provide consumers with the opportunity to opt-out of telemarketing calls and commercial electronic messages.

The ACMA has previously found[15] that there are strong drivers for the existing rules in the DNCR Act, Spam Act and related powers and functions in the Telecommunications Act to be consolidated and harmonised to align with the consent arrangements in the Privacy Act. Such an approach could consist of a universal consent-based framework under which marketing contact could only occur where either consumer consent has first been obtained, or where a public interest exemption is applicable. Importantly, it could explicitly set out principles that apply to consent across all frameworks. In this regard, the ACMA notes that the framing of consent under the European Union's General Data Protection Regulation (GDPR) may provide insights for a new Australian framework for consent.

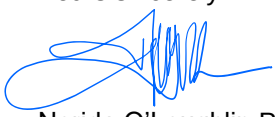
Under such a framework, certain public interest exemptions could remain; however, with an additional safeguard via an obligation on all entities to provide a direct and one-step 'unsubscribe' or ‘opt-out’ functionality – regardless of the size of the entity, marketing channel used or whether the entity is otherwise exempt. This would preserve the public interest in the case of first marketing contacts from all entities but would give consumers additional agency to prevent subsequent contact.

Such a revised framework would be broadly consistent with the model in the Spam Act and would, effectively, remove the need for a Do Not Call Register (given that consumers would, by default, be opted out of receiving unsolicited communications until such time as they provide their consent).

The ACMA remains agnostic about where the safeguards are enacted; however, should APP 7 be extended to all direct marketing activities, it should align with international approaches and be underpinned by strong, consistent consent protections across all relevant marketing channels.

The ACMA looks forward to the progress of the Review and further opportunities to engage in due course. The ACMA contact for this matter is Jeremy Fenton, Executive Manager, Consumer, Consent and Numbers Branch on [redacted].

Yours sincerely



Nerida O’Loughlin PSM

4 December 2020

[15] ibid.