Contents

Executive summary 1

Introduction 3

The evolving apps environment 5
Apps provide the functionality on smartphones, tablets and other devices 5
A significant and growing market 7
The rapid take-up of smartphones and tablets is translating into rapid growth of apps take-up 7
Social networking, games and weather the most popular apps 8
The apps marketplace and business models 10
The apps supply chain is complex and global 10
Free and low-cost apps continue to dominate the apps market 11
Apps provide a mechanism for advertising on mobile devices 11
Collection of users’ personal information part of the app experience 12
Apps enable citizens to be constantly connected 12
Apps facilitate personalisation of media consumption 12
App game-like social and economic activity 12
Constantly connected citizens use apps to create media content 13

Regulatory consequences 14
A complex mix of industry-specific and economy-wide regulation 14
Public interest outcomes remain relevant in the apps environment 15
Complex and global supply chains challenge the application of market standards and redress mechanisms 16
Apps shaping the ways citizens share their personal information 18
The apps environment creates challenges and opportunities for the application of content safeguards 20
Apps are changing citizens’ expectations of how public protections such as access to emergency services are delivered 21
Future management of the apps market will rely on a mix of regulatory and non-regulatory strategies 21
Regulatory or co-regulatory interventions may be appropriate for regulating some aspects of the apps supply chain 22
Facilitating industry self-regulatory responses 22
Communicating with consumers to manage the apps experience 24

Conclusion 25
Executive summary

Mobile applications (apps) represent one of the most significant developments in media and communications in the past five years. Apps are software programs that may be installed on smartphones and other communication devices. At the heart of this evolution is the transformation of mobile telephony from a voice- and text-based platform, into one where a diverse range of media and communications activities is available from a single device. Developments in software applications have turned these devices and networks into productivity tools, communication channels and sources of information and entertainment.

The apps environment brings together a number of previously distinct sectors—telecommunications, radiocommunications, broadcasting, computing, publishing and financial services. These were traditionally separate service markets, which are now available on one device, on one platform.

In Australia’s networked society and information economy, these innovations bring significant benefits. They also challenge traditional approaches to regulation where apps, and the shift in communications and media usage they represent, are not reflected in existing legislative or regulatory concepts. The widespread take-up and use of apps is also raising new issues in the protection of digital citizens.

Within this changing environment there are ongoing points of public interest that can inform discussion about the design of any regulatory responses. The particular matters of ongoing interest in the apps context concern:

> market standards and redress mechanisms
> management of personal information in a digital environment
> content safeguards which protect children and reflect community values
> access to emergency services to protect individuals and communities.

Addressing these matters of public interest may require the regulator to respond differently when developing solutions to assist citizens in managing their digital content, identity and reputation associated with the use of apps.

To date, a combination of industry self-regulatory measures, technical tools, economy-wide safeguards and other sector-specific measures appears to have been effective in managing emerging risks associated with the apps environment. However, existing regulatory frameworks did not anticipate the surge in mobile data availability, the capabilities of apps and the business models through which they are distributed. Consequently, there is potential for citizens to be dissatisfied or disadvantaged where market responses are not adequate or safeguards are not in place.

With the ongoing development of separate responses to emerging apps practices there is the risk of an overall loss of regulatory coherence with consequences for industry participants in terms of increased compliance costs. For consumers, increased complexity can make it more difficult to manage their apps experience.

As apps become a mainstream activity in the Australian communications market, there would be benefits in apps issues being addressed within a single coherent regulatory framework.

The Australian Communications and Media Authority (the ACMA) undertakes research to identify the dimensions of digital technological change, and changes in the behaviour and expectations of digital citizens. Apps developments are at the forefront of changing communications technology, market structures and consumer behaviour. The ACMA is examining the impact of these changes on current regulatory settings.
This is the first of four occasional papers this year, which examines emerging issues in contemporary media and communications. It updates the ACMA’s May 2011 occasional paper, *Emerging business models in the digital economy—the mobile applications market.*
Introduction

Mobile applications (apps) are becoming available for an increasing range of consumer devices. With the rapid take-up of smartphones and tablets, app purchase and usage are quickly becoming mainstream media and communications activities.

Apps and the devices on which they operate are facilitating a shift toward increasingly mobile, personal and game-like engagement with media content and communications services. The number of Australian adults with smartphones more than doubled between June 2011 and June 2012. Social networking, game and weather apps are the most popular. While being constantly connected offers convenience and other benefits, there are significant implications for the collection and management of personal information. The global apps supply chain also presents challenges for consumer protection and the application of other safeguards which citizens may expect.

As apps become embedded in an increasing range of consumer and industrial devices, future management of the apps environment is likely to require a mix of regulatory and non-regulatory interventions. While some may be specific to the apps market, many of the issues posed by apps—including consumer and personal data protection—span a range of online activities and offline activities. These new issues may require different responses to assist citizens in managing digital content, identity and reputation across whole-of-economy and whole-of-networked society levels.

The ACMA is examining how these changes affect current regulatory settings, including those aspects of regulation that remain relevant in the apps market, and how regulatory and non-regulatory strategies can be adapted to address identified areas of business and consumer concerns about the apps environment.

This paper is the first this year in a series which examines emerging issues in contemporary media and communications. It updates the ACMA’s May 2011 occasional paper, Emerging business models in the digital economy—the mobile applications market.¹ This paper examines:

> the apps environment including developments in the supply and use of apps  
> regulatory challenges raised by the mainstreaming of apps  
> the suite of citizen and consumer safeguards that represents an enduring basis for continuing regulatory attention  
> regulatory and non-regulatory strategies available assist in managing consumers’ apps experience.

The ACMA would welcome further discussion from interested parties on the following questions:

1. Are there other aspects of apps supply and use that should be considered by the ACMA and are not covered in the discussion?  
2. Are there current barriers to further innovation occurring in apps that need to be considered by the regulator?  
3. In a globalised communications market, what are the most effective methods of supporting consumers’ confident and productive engagement with apps?  
4. Are some regulatory or non-regulatory strategies better suited to facilitating further innovation in apps while supporting consumer engagement with the app market?

Feedback on the issues discussed in this paper can be directed to regframe@acma.gov.au.

Forthcoming papers in the series will discuss:
> near-field communications
> cloud computing
> privacy and digital data protection.
The evolving apps environment

This chapter explores recent changes in the apps market and consumer use and expectations of apps. The changing market dynamics and consumer expectations are important factors in the ACMA’s assessment of the impact of emerging issues in communications and media on current regulatory settings.

Since the ACMA last examined the mobile apps market in May 2011, it has continued to grow rapidly. So has the range of devices on which apps can be used, and the take-up and use of these devices by Australian consumers. Between June 2011 and June 2012, there was a 104 per cent increase in the number of adults with smartphones. As these devices all use apps to provide functionality, there is a corresponding impact on the usage of apps. The number of adult smartphone users who downloaded additional apps increased from 2.41 million in June 2011 to 4.45 million in June 2012—an increase of 85 per cent.

Given the current take-up rates for smartphones, there is still room for significant growth in the apps market.

Apps provide the functionality on smartphones, tablets and other devices

Apps are software programs that may be installed on smartphones and a growing selection of other devices, including tablets, home entertainment devices, laptops or desktop computers. While computers and computer software have been a part of the lives of Australian consumers for more than three decades, it is now around 20 years since households and businesses began connecting to the internet. More recently, mechanisms that securely process online electronic payments have enabled distribution of online content on a commercial basis using personal, portable devices.

While apps perform many different functions, they have some common characteristics:

> they are downloaded once and stored on a device until the user deletes them
> they enhance the device’s practical and entertainment functions
> they are operating system specific (although versions of most popular apps are available for multiple operating systems)
> they may be free (excepting data usage costs) or paid
> they are designed for access with touch screen devices
> they are designed to work with, and may adjust, internet or other material for screen sizes smaller than those of some fixed devices.

Device capability and functionality is increasing, and the gap between mobile computing capability and desktop capability is closing. Apps take advantage of this trend by allowing users to have many functions similar to those that they would use on a desktop computer available on a mobile device. While some apps, like weather reports or maps, may be pre-installed on a smartphone or tablet, many other apps are

---


4 ibid, p. 2.

purchased separately to access a range of online content sources. Examples of the latter include the apps now produced by many media outlets to complement their broadcasting and publication activities.

In the near future, the increasing take-up of ‘smart televisions’, and other home entertainment devices and appliances, is likely to see use of apps for these devices grow.\(^6\)

Figure 1 Example of the functionality provided by apps

Apps are not unique to mobile devices and much of the online activity that occurs on apps mirrors the online interactions that take place using desktop computers. As consumer migrate their use from one device to another, they may carry similar expectations. For example, where a consumer accesses a service, like a voice service through a telephone, to contact emergency services, they may expect a similar ability to contact emergency services through an app, Twitter or Facebook. These changing expectations have implications for the design of important safeguards, like emergency service access.

In addition to providing users with a wide range of communications, entertainment and productivity capabilities (see Figure 1), apps and the devices they run on provide a new capacity for collecting detailed information about consumers and their behaviour. An app which purports to perform a limited range of basic functions for a user may also access a range of other data on the consumer’s device that is unrelated to the ‘primary’ function of the app. This is a growing source of privacy-related concerns for some consumers.

A significant and growing market

The rapid take-up of smartphones and tablets is translating into rapid growth of apps take-up

Smartphones and other mobile devices are being taken up by Australian consumers in increasing numbers. There has also been an increase in the percentage of Australians who are regularly downloading apps. The percentage of Australians (online Australians 16 years and over) who accessed the internet via a mobile device and have downloaded apps is represented below in Figure 2.7

Figure 2 Downloads of apps on mobile phones and tablets, 2011 and 2012 comparison

The average number of apps downloaded in the last three months (report date February 2013) by online Australians who had ever downloaded an app was eight free apps and four paid apps.8

It has been reported that 80 per cent of American consumers’ time on mobile devices is spent in apps and that that every minute 47,000 apps are downloaded by users worldwide.9 One study predicted that downloads would reach 82 billion worldwide in 2013,10 while another predicted 44 billion cumulative downloads by 2016.11 Apple reports that their customers have downloaded over 50 billion apps, with nearly 20 billion in 2012 alone (excluding re-downloads and updates).12

---

7 Nielsen, Australian Connected Consumers: Evolving Patterns of Media Consumption in the Digital Age, February 2013, p. 63.
8 Ibid, p. 65
9 http://venturebeat.com/2013/04/03/the-mobile-war-is-over-and-the-app-has-won-80-of-mobile-time-spent-in-apps/#u2hLOvxYcu7M6vpM.02
Although predictions vary, a common industry view is that the number of app downloads will continue to increase. In Australia, the continued take-up of high-speed fixed and mobile broadband, and growing interest from a number of sectors seeking to deploy 4G communications networks and long term evolution (LTE) networks across Australia, will further facilitate consumer access to greater amounts of information as speeds increase.\textsuperscript{14}

As the network speeds increase and the apps market further evolves to extend to non-traditional ‘devices’ such as fridges and cars, there is likely to be rising demand for spectrum to support these communications.\textsuperscript{15} Also, as apps are developed which facilitate increased machine-to-machine communications, the growth in the market may place demand on numbering resources.

Overall consumer satisfaction with the apps market appears to be high, although some aspects of apps marketing are raising concerns with consumer organisations, such as the Australian Communications Consumer Action Network (ACCAN). ACCAN recently lodged a complaint with the Australian Competition and Consumer Commission (ACCC) over promotion of in-app purchasing in games marketed to children. Despite the level and pace of apps take-up, between 1 April 2012 and 31 March 2013, the ACCC received around 30 contacts from consumers about apps.\textsuperscript{16} The Telecommunications Industry Ombudsman reported 221 new complaints about mobile apps from 1 July 2012 to 31 December 2012 and 85 enquiries about mobile apps from 1 July 2010 to 31 December 2012. This is likely to be due to a range of factors.

The main participants in the global apps market have invested in building and maintaining long-term relationships with consumers. They also have governance arrangements and business processes aimed at securing consumers’ trust and confidence. The ease with which consumers can download and remove apps, and the relatively low financial risk of app purchases, are also likely to be factors that have contributed to relatively low complaint levels to date.

**Social networking, games and weather the most popular apps**

The app store is the main way consumers access apps. Each app store has created ways of categorising apps for consumers. In 2012, a survey of online Australians showed that Facebook, games, weather, maps/directions and email were the most-used apps on mobile phones, tablets and mobile media players.\textsuperscript{17} The top free apps downloaded in Australia during March 2013 from the Apple App Store and Google Play Store are shown in Figure 3.

\begin{itemize}
  \item[16] Australian Competition and Consumer Commission, unpublished data.
  \item[17] Nielsen, op.cit, p. 66.
\end{itemize}
The top paid apps in Australia during March 2013 downloaded from the Apple App Store and Google Play Store are shown in Figure 4.

Other popular categories of apps for mobile phones and tablets include:
- social networking and messaging
- games
- photo-taking, editing and sharing
- navigation and location-tracking
- banking and financial management.

Consumers participate in the apps market not only as customers but also as a source of advice about which apps may meet an individual’s needs. App stores incorporate peer recommendation systems where consumers can review and rate apps they have downloaded, commonly rating the app on a scale (for example, 1 to 5 stars). They also

---

have the opportunity to comment. Other users can view these ratings to inform their decision-making process. Feedback can be powerful, for example, Public Transport Victoria re-introduced the previous version of its public transport iPhone app after a large number of negative reviews about the new version.20

The apps marketplace and business models
Apps combine the sophisticated functionality of mobile, portable and desktop computing devices. They offer a wide range of possibilities for software developers to create software products for digital consumers. While some traditional communications business models are under threat, the apps market has enabled new business models that exploit the characteristics of this functionality.

The apps supply chain is complex and global
An important characteristic of the apps environment is that the supply chain is global, with responsibilities for different elements of a consumer’s experience fragmented and shared between the various entities in the supply chain.

App stores associated with device and operating system brands continue to be the dominant channel for distributing apps. There are four main models of app stores used by Australian consumers:

> device manufacturers
> operating system developers
> mobile network operators
> independent.

In Australia, 44 per cent of smartphones use the Android operating system, with 43 per cent using Apple’s iOS operating system.21 Over the past three years, there has been a sharp increase in the Android’s market share, a moderate decrease in market share for Apple with a loss in market share of the Nokia Symbian operating system which Nokia ceased in 2011.22 The primary app store for Android devices is Google Play, and the Apple App Store for devices running iOS.

While mobile network operators in Australia were previously excluded from the apps supply chain and business model (other than as providers of the data connections utilised by apps), they are becoming increasingly involved in the apps market. Optus launched its apps store in November 2009 and, in 2012, introduced the option of carrier billing for Blackberry apps purchased by Optus mobile account holders.23 Telstra announced in December 2012 that customers with Android smartphones can charge purchases from the Google Play store to their mobile bills.24

---

22 Nielsen, op.cit. p. 46.
As the industry has seen the potential for revenue from these new streams of operation, a number of app stores, independent of the network operator or device brand, have been established (for example Mobango).

While the customer experience is fragmented across the complex supply chain, app store reputation mechanisms (led by the dominance of the two leading app stores Google Play and Apple App Store) are likely to have had the effect of a market self-regulatory tool. Additionally, the free or low price point of the majority of apps may have impacted on consumers decisions about whether to seek redress.

**Free and low-cost apps continue to dominate the apps market**

The two main business models for app stores are those which are open and those which are closed. Closed models are those which are proprietary app stores linked to a particular brand of device, such as an Apple iPhone and the Apple App Store. Open models are not linked to a particular device brand or app store. The Android platform is an example of an open model where the Android operating system can operate on a number of different device brands. Android users can download apps from Google Play as well as other independent operators, such as Mobango.

Both models of app stores provide both free and paid apps and a variety of revenue-sharing arrangements with app developers. Most apps continue to be relatively low-priced or free. However, as device capabilities continue to evolve and developers identify new business cases, more advanced apps, with higher prices, have begun to emerge. Figure 5 provides a graphic representation of price distribution. Apps priced at US$49.99 and above make up only 0.22 per cent (2,166) of all apps available in the Apple App Store.

![Figure 5 Price distribution of apps in US Apple App Store in US dollars as at 29 April 2013](http://148apps.biz/app-store-metrics/?mpage=appprice)

**Apps provide a mechanism for advertising on mobile devices**

Advertising has continued to penetrate the apps market as advertisers seek to capitalise on the personal and individual nature of the mobile platform and the potential for mobile devices to facilitate impulse purchases. The personal and individual nature of mobile devices, and the circumstances in which they are used, make them an important new channel through which advertisers are able to reach

---

target markets. It is reported that mobile advertisements accounted for around one-third of Facebook advertising revenue in the March 2013 quarter, up from around one-quarter in the December 2012 quarter.\(^{26}\) Predictions are that in 2013 in the US market, Facebook will account for three out of every 10 dollars spent on mobile advertisements.\(^{27}\) With the increasing tendency for consumers to access Facebook through a mobile device, and through a Facebook app, growth in advertising delivered via apps has the potential to reshape the apps service model.

### Collection of users’ personal information part of the app experience
Increasingly sophisticated tools are being developed to collect and analyse information about citizens and their online behaviour for marketing purposes. Many apps developed for mobile phones and tablets are used to collect, aggregate and analyse personal information and data about online behaviour. How apps handle personal information is often unrelated to the primary or stated purpose of the app.\(^{28}\) These practices raise potential concerns about the extent to which citizens are aware of the data that is being collected and the uses to which it may be put. They also raise concerns about the ongoing viability of traditional approaches to personal data protection.

### Apps enable citizens to be constantly connected
Developments in technology are allowing citizens to connect and interact with one another, anywhere and anytime. For example, the number of users checking Facebook on mobile devices is greater than the number of users checking Facebook via the internet.\(^{29}\) At the same time, many smartphones users are never without them. For example, within the first 15 minutes of waking up, four out of five smartphone owners are checking their phones. Of these, almost 80 per cent reach for their phone before doing anything else.\(^{30}\)

### Apps facilitate personalisation of media consumption
Apps allow consumers to personalise their communications experience. As well as apps which allow the personalisation of the look and features on the phone, apps may personalise the content experience of the consumer. For example, the Pandora Radio app, launched in 2008, is an automated music recommendation service which plays songs of a genre based on which artists the user selects. The user can then indicate whether they like or dislike a song and this information is used to select and deliver more songs.

Personalisation exists already for consumers, often without them being aware that it is occurring. For example, Google personalises search result based on past search information using cookies or Google Web History (if a consumer is signed into a Google Account). This means that if two consumers were to search the same terms, the results displayed may be different. Apps which can access information from the consumers’ devices, similar to the information collected by cookies, are likely to facilitate further development of apps which personalise news and other content.

### App game-like social and economic activity
‘Gamification’ is being used in a variety of social and economic contexts to improve consumer engagement by using game mechanics. Customer loyalty and reward programs, educational games and health and fitness programs are all examples of how game principles and concepts can be directed towards achieving business and personal goals. The apps platform is aiding this process by leveraging device

---

\(^{26}\) Cutler, K., About 30% of Facebook’s Advertising Revenue, or $375M, Came From Mobile Platforms, reported on Tech Crunch, 1 May 2013, at http://techcrunch.com/2013/05/01/facebook-mobile-ad-revenue/.

\(^{27}\) http://venturebeat.com/2013/04/03/facebook-mobile-ads-2013/.

\(^{28}\) Ovum, Personal Data Futures: The Digital Ecosystem, 25 February 2013.

\(^{29}\) http://edition.cnn.com/2013/01/30/tech/social-media/facebook-mobile-users

\(^{30}\) https://fb-public.box.com/s/3iq5x6uwng7q7ki4q8wk
functionality, portability and individuality to provide apps which gamify a range of
day-to-day activities. For example, Four Square is a location-based app which allows
users to locate and check in at hotels, bars, cafes and other venues, and earn points
and status badges. Mayorship is awarded to a user who has checked into a venue on
more days than anyone else in the past 60 days. Venues may also directly reward
consumers who visit and check in regularly.

Constantly connected citizens use apps to create media content
Apps which utilise the increasingly sophisticated audiovisual capabilities of mobile
devices are enabling citizens to create media content and engage with mainstream
media in new ways. The popularity of smartphones means that mainstream media
coverage of issues and events of public importance frequently incorporates content
created by citizens on their own devices. The use of these first-hand accounts has a
range of implications for citizens’ expectations of media coverage.
Regulatory consequences

This chapter examines the impact that apps innovation, changing market structures and user behaviour have on the current media and communications regulatory framework. It also identifies points of ongoing public interest that can inform discussion about the need, or not, for intervention in the apps market.

The apps market did not exist when the current regulatory frameworks for telecommunications and broadcasting were introduced. Similarly, the apps environment has introduced business models and business practices that did not exist when measures covering personal information and consumer protection were developed. This challenges the effectiveness of current models for implementing and ensuring compliance with regulatory safeguards. There are also business impacts in terms of compliance costs, where incremental measures have been adopted to address different aspects of the apps market operation.

A complex mix of industry-specific and economy-wide regulation

To date, there has been a piecemeal approach to accommodating technological and market developments in the regulatory framework, preserving technology- and sector-specific approaches. The apps market is currently subject to a range of whole-of-economy and sector-specific regulatory measures, including:

> Australian Consumer Law, administered by the ACCC and state and territory fair-trading agencies, which provides for refunds for faulty goods; consumer guarantees to ensure that items are fit for any particular purpose, which is represented by the supplier; and protections where suppliers engage in activities that are likely to mislead or deceive consumers.

> The e-Payments Code and related measures administered by the Australian Securities and Investments Commission, which covers the online electronic payments associated with app purchases.\(^{31}\) The code includes remedies for credit card charges associated with goods and services that were not received. This includes a situation where a charge was imposed by application store but no application was received by the consumer.

> The Privacy Act 1988, which provides protection for citizens in the way entities covered by the Act handle personal information through the lifecycle of collection, use (including data matching and analytics), disclosure, storage and destruction. App developers whose business model relies on using personal information to sell advertising are likely to be covered by the Privacy Act.\(^{32}\) Recent amendments to the Act provide enhanced protections for personal data that is collected from Australian citizens and stored outside Australia.

> The Online Content Scheme, established under Schedule 5 and Schedule 7 to the Broadcasting Services Act 1992, which provides mechanisms for dealing with apps and other online content, with reference to the National Classification Code. The arrangements for classification of content were recently reviewed by the Australian Law Reform Commission, which has recommended reforms aimed at achieving greater consistency across offline and online platforms.

---


> The Telecommunications Act 1997, which establishes a regulatory framework for specific segments of the market. For example:

> regulating providers of communications infrastructure (for example ‘carriers’)\textsuperscript{33} in a particular way

> regulating providers of communications services in a particular way (for example ‘carriage services providers’)\textsuperscript{34}

> regulating providers of content service in a particular way (for example ‘content service providers’)\textsuperscript{35}

Previously discrete service sectors, such as communications and financial payments, are also merging in the apps business model. This can create uncertainty about:

> which entity in the supply chain may have particular regulatory obligations

> the coverage of safeguards, such as those dealing with personal information and privacy.

Both consumers and business benefit from regulatory certainty and clarity. While the apps market is subject to a range of regulatory measures, how they are applied may not always be clear to consumers and industry participants. For industry there are additional costs in dealing with multiple agencies and different regulatory frameworks. For a consumer, knowing how to take action, who to complain to and how to resolve their apps concerns is complex. This is further complicated by an environment where there are multiple agencies involved and potential gaps in the safeguards that address their issues of concern.

With the ongoing development of separate responses to emerging apps practices, there is the risk of an overall loss of regulatory coherence with consequences for industry participants in terms of increased compliance costs. For consumers, increased complexity can make it more difficult to manage their apps experience. As apps become a mainstream activity in the Australian communications market, there would be benefits in apps issues being addressed within a single coherent regulatory framework.

**Public interest outcomes remain relevant in the apps environment**

Apps illustrate some of the disconnect between traditional regulatory concepts and contemporary communications. However, there are points of ongoing public interest that can inform discussion about the need, or not, for intervention in the apps market. The ACMA’s consideration of the apps environment has identified the following particular matters of interest relevant to the delivery layers of an information economy (see Figure 6):

> market standards and redress mechanisms, including those which apply to apps payment mechanisms

> digital information management, particularly as it relates to users’ personal data

> content safeguards, which protect children and reflect community values

> ensuring access to emergency services to protect individuals and communities.

\textsuperscript{33} Defined in Section 7 of the Telecommunications Act 1997 as a holder of a carrier licence.

\textsuperscript{34} Defined in section 87 of the Telecommunications Act 1997.

\textsuperscript{35} Defined in section 97 of the Telecommunications Act 1997, see also section 15 which provides for the definition of content service to be amended by ministerial determination.
Complex and global supply chains challenge the application of market standards and redress mechanisms

Market standards that incorporate effective and transparent redress mechanisms are important for a well-functioning digital economy.

The fragmentation of roles and responsibilities has implications for resolving any consumer dissatisfaction that may arise. Seeking redress in response to a payment issue may be a complex experience for the consumer if the app store does not have a legal presence in Australia or legal representatives in Australia. Consumers should have confidence that safeguards exist that provide them with effective and accessible avenues of complaint and redress. Consumers may instinctively seek redress from the institutions of which they are aware, such as the ACMA or the Telecommunications Industry Ombudsman, and may be less aware of other whole-of-economy safeguards, which may provide avenues of redress, such as the Financial Ombudsman Service.

An integral component of the online apps market is the mechanism by which payments for apps are processed. Previous ACMA experience with the mobile premium service market has shown that lack of transparency in mobile phone-based payment mechanisms can lead to significant consumer dissatisfaction and detriment. Consumers’ participation in the apps market will be enhanced if they are confident that appropriate safeguards exist.

The non-cash payment mechanisms introduced in the 1970s have evolved into the online electronic payment systems, which today facilitate online purchases. Two common app payment pathways are illustrated in Figure 7—payment by credit card and payment by direct account billing.
Consumer protection for payment by credit card is provided by the e-Payments Code and associated measures.

The application of this code is voluntary and applying it to emerging methods of online payment is subject to the entities, which provide payment facilities, becoming subscribers to the code. As new methods of mobile phone-based payment begin to emerge, particularly those which permit charges for goods and services to be billed to a customer’s mobile phone account, questions are arising about the consumer protection arrangements that will apply. Consistent protections for online electronic payments is desirable, regardless of whether these are made by credit or debit card, billed to a mobile phone account or made using another payment facility.

The ACMA has advised Australian mobile carriers that it expects any who offer payment facilities that are covered by the code to subscribe to that code. Some mobile carriers are now offering their customers the ability to purchase apps and have the charge billed to their mobile phone accounts. This amounts to the provision of a payment facility covered by the code. However, Australian mobile carriers have yet to subscribe to the code.

Maintaining consumers’ trust and confidence in mobile phone-based payments will require robust safeguards to be put in place. It is also desirable that these apply consistently across all forms of online electronic payment, regardless of the technology or platform used in making a payment. Sector-specific arrangements were developed for mobile premium services (MPS)—an early form of mobile phone-based payment—to address the lack of transparency in this market when services were first launched. These measures have been successful in addressing consumer dissatisfaction and detriment.

As the MPS market is succeeded by the apps market, it will be important to ensure that the associated payment mechanisms are transparent and protected by appropriate safeguards. Clarity about the rights and responsibilities of market
participants, and clear avenues for redress if there are issues with app payment mechanisms, will further enhance consumers’ experience of apps and should have positive impacts on an information economy. Streamlining the current sector-specific and whole-of-economy measures into a coherent framework for apps would help clarify relevant applicable safeguards.

**Apps shaping the ways citizens share their personal information**

Apps allow citizens to perform an increasing range of social and economic activities online and the way apps treat personal information becomes increasingly important to consumers. The ACMA’s May 2011 occasional paper on the emerging apps market recognised the increasing complexity of protecting personal information in the digital environment and highlighted specific issues relevant to the apps environment.\(^{36}\)

The privacy-related considerations associated with apps mirror those in the wider online environment, with the added dimension of the personal and portable nature of the devices on which apps run. Many apps make use of location information and apps have become the dominant platform for collection and use of location information. However, findings from ACMA research in 2012 point to issues for consumers.\(^{37}\) Key findings of this research included that:

- Greater use does not equate to a greater understanding.
- The majority of respondents generally understand what location information is being collected. However, there is a broad lack of awareness about the sharing of this information and how personal data may be shared when using such services. As a result, many respondents lack the ability to choose appropriate protection options.
- Risks are poorly understood. More than two-thirds respondents had concerns about the level of information they share when using location services, with 71 per cent concerned about information being sold to a third party.
- When considering protective measures to manage these risks, knowledge of simple actions, such as turning off location services when they were not in use, was limited. Respondents also did not regard information contained in terms and conditions as an effective mechanism for informing themselves, either because they ignored them or adopted a ‘tick and flick’ approach in their haste to access the service or app. This highlights the need for further work, particularly focused on the design of mechanisms that would allow consumers to become better informed about the terms and operation of their service.
- Respondents want information to help them protect personal data.

These findings point to a significant gap in citizens’ ability to manage location information—an important item of personal information—in the apps environment, as well as other types of personal information collected by location services, one subset of the apps available. Citizens may also be unaware of the third parties involved in the apps ecosystem who may receive and use their personal information, for example, as outlined in Figure 8.

---


Protection of citizens’ personal information in the media and communications environment again is currently achieved through a combination of whole-of-economy and sector-specific measures. These measures are established by the Privacy Act, administered by the Office of the Australian Information Commissioner; state- and territory-based measures, administered by authorities in those jurisdictions; and the Telecommunications Act and subordinate instruments, administered by the ACMA.

Existing privacy-related regulatory measures do not map easily to the emerging personal data ecosystem, of which mobile devices and apps are an integral part. Concerns are emerging around data usage practices that did not exist when current privacy measures were developed; and apps are involved at various points in a number of these. For example:

> Widespread adoption of online social networking using mobile devices has resulted in citizens voluntarily sharing significant amounts of information about themselves and their activities, but with limited awareness of the uses to which the information is being put.

> Many apps serve as mechanisms for storing different types of personal information on ‘cloud computing’ services, resulting in increasing amounts of personal information being disclosed to cloud service providers.

> Numerous technologies have been developed to record online activities undertaken in mobile device browser apps, social networking apps and multimedia apps, often without their awareness or informed consent. This information is being commercially exploited and traded for marketing purposes. For example, it has been claimed that some popular Android apps upload mobile numbers to third parties without notification and others access browsing histories on phones. 38

> Kaspersky researchers have recently discovered malware which is represented as an app to free memory from the Android operating system. If the phone is then

---

connected to a computer, the malware will infect the desktop computer as well.\(^\text{39}\) Of concern to consumers is that this app was distributed through the Google Play store, with consumers usually being advised to only download apps from reputable stores, which Google Play is considered to be.

While technical tools can be a useful way to assist individuals in managing their digital information, it is likely that other measures may prove beneficial. This could include communicating the changing nature of personal information risks, as well as improving consumers’ skills and understanding in their self-management of the apps environment.

The apps environment creates challenges and opportunities for the application of content safeguards

The nature of the online environment, and the range of content that it provides access to, mean that some apps will be unsuitable for children, especially younger children, and potentially harmful to them. In addition, location-based social networking apps introduce additional risks associated with the potential for them to facilitate inappropriate contact between children and adults.

Content safeguards for the public, and particularly children, are currently achieved through a combination of measures contained in numerous pieces of legislation administered by the ACMA and other regulatory bodies, as well as law enforcement agencies. The Australian Government has agreed in principle that, to the extent possible, the National Classification Scheme should apply equally to all content. On 5 April 2013, the government announced that legislation will be introduced into parliament to enable the use of automated classification decision-making systems. This will commence with a pilot covering mobile and online computer games. Existing content classification measures were developed to cover the sale, exhibition and hire of physical media products and services. The application of these measures was extended to online content by Schedule 5 and Schedule 7 to the Broadcasting Services Act which provides a complaints framework for dealing with online content that would restrict its availability in other formats.

The primary mechanisms for delivering content safeguards for the apps market continue to be the content-rating measures used by app store operators and education initiatives aimed at app and smartphone users. Both Apple’s App Store and Google Play have their own classification systems for advising consumers. These classifications apply globally. To date, rules for app developers have included restrictions on apps that contain adult content. These arrangements appear to have been reasonably effective in restricting the range of apps that can be downloaded.

While the apps environment creates a number of challenges for the application of national content regulation measures, it also provides protective measures that are not available, or are less accessible, on fixed/desktop platforms. For example, devices which use Apple’s iOS operating system are able to be configured so that access to certain apps, as well as the ability to install and delete apps, is restricted and a passcode is required to bypass these settings. Technical tools are also available to assist in managing children’s interactions with apps, such as parental control apps, which can be installed on devices. For example, the Playrific app provides child-friendly content and the Kytime Android app allows parents to monitor and control smartphone usage by reporting on time spent using apps and on websites, as well as control when particular apps can be used.

\(^{39}\) http://thenextweb.com/insider/2013/02/03/android-malware-emerges-on-google-play-which-installs-a-trojan-on-your-pc-uses-your-microphone-to-record-you/
Apps are changing citizens’ expectations of how public protections such as access to emergency services are delivered

Citizens having access to reliable communications in an emergency has been a fundamental concept in media and communications policy. Online services, including those which use apps, are increasingly complementing traditional broadcasting and telecommunications services to facilitate management of emergency and public safety situations. The primary focus of the consideration to date has been in using apps to provide information to citizens, for example, location-based mobile telephone emergency warning capability is being developed and rolled out. This service sends out emergency warnings via text message to recipients based on the location of the device at the time of the emergency.

As apps become mainstream communication tools, particularly social media apps, citizens may increasingly rely on them for health and personal safety purposes. For example, the ability of GPS-enabled smartphones to track a user’s location has created expectations that a user with such a device can be easily located by emergency services.

Governments and emergency management organisations are considering how these new media tools may be used to engage with Australian community in a disaster or an emergency. The New South Wales Government has launched a domestic violence app, which contains information about access to services to assist with domestic violence situations. The app also includes a button, which links to Triple Zero, and a button which will send an SMS to a contact (such as a friend or family member). The SMS has three in-built messages and functionality which will utilise the device’s GPS to determine the location of the sender and send this information to the contact.

With the development of apps such as these, and the growing range of services that consumers can access through apps, the ability to contact emergency services through an app is likely to be an issue for consideration in the future.

Future management of the apps market will rely on a mix of regulatory and non-regulatory strategies

Consumers’ experience with the apps environment to date appears to be generally positive. Apps are being taken up at very high rates and there is limited evidence of consumers suffering serious detriment or having serious concerns about their experiences with these services. This is due, in part, to the apparent effectiveness of the combination of self-regulatory measures and technical tools put in place by app store providers, economy-wide safeguards and other sector-specific measures.

Nonetheless, the apps environment represents a significant transformation in the way citizens consume content, transact and share personal information. Existing regulatory safeguards do not anticipate the business models and consumer behaviour which characterise the apps environment. In this context it is appropriate to consider possible approaches for dealing with any consumer concerns or other risks that may emerge.

41 Further information about this application and the application itself can be found at https://itunes.apple.com/au/app/aurora/id611015460?mt=8.
A range of options is available for dealing with conduct that is harmful to consumers, and any intervention should be proportionate to the demonstrated level of harm. In the first instance, industry should be encouraged to develop self-regulatory arrangements that are tailored to specific problems. These arrangements should be developed through transparent consultative processes and be underpinned by effective compliance measures. Key considerations in assessing the need for additional measures for the apps environment, and their viability, are how to define the scope of such measures in a way that addresses a problem while also taking account of likely future developments in the apps market. Specific considerations would include:

- the growing range of mobile, desktop and other devices that use apps
- the desirability of developing regulation that is platform- and technology-neutral
- the relationships between apps-based activities and transactions, and other types of online activity
- the relationships and interactions between any sector-specific measures and whole-of-economy measures, such as Australian Consumer Law, the Privacy Act and the e-Payments Code.

**Regulatory or co-regulatory interventions may be appropriate for regulating some aspects of the apps supply chain**

The application of existing legislation to the apps market varies and, in some cases, the entities are not easily recognisable within the legislative framework. Communications and media regulation has traditionally been weighted towards industry participants rather than citizen-focused interventions. This model has worked effectively where regulation aligns with the activities of recognisable entities operating within a jurisdiction and the regulator’s role is clearly specified as monitoring or enforcing rights or obligations specified in legislation.

Relevant legislative safeguards are also provided on a whole-of-economy basis in Australian Consumer Law and the Privacy Act. These measures have extraterritorial application although their effectiveness may be undermined by difficulties in enforcing obligations on entities located outside Australia. The effectiveness of regulatory strategies is therefore likely to be improved where there are cooperative arrangements between jurisdictions for enforcement, or other cross-border regulatory measures.

**Facilitating industry self-regulatory responses**

With the need for intervention established, non-regulatory solutions may offer a more flexible response to the market dynamics and citizen ‘problems’ emerging in the dynamic digital environment. This is particularly so where the legislative framework remains unchanged or outdated. The ACMA’s framework for effective co- and self-regulatory arrangements identifies that a number of environmental conditions for effective self-regulatory measures are present in the apps market. This includes factors such as:

- a competitive market with few barriers to entry
- homogeneity of products
- degree of consumer detriment
- a rapidly changing environment.

Facilitation of strategies, such as industry self-regulation, are particularly useful in circumstances where the intended outcomes are improvements in service standards,

---

knowledge about obligations or to provide incentives for behaviour change by industry participants or individual citizens.
Many aspects of the apps market are currently subject to selected self-regulatory arrangements and these appear to be operating reasonably effectively. App stores governance arrangements, which apply to the relationships between the app store and apps developers, illustrate the self-regulatory measures being used. These governance arrangements cover matters such as the standards they require developers to meet. In addition, some user groups are developing standards as minimum governance arrangements, which they want to apply to the apps ecosystem. For example, a report by the Federal Trade Commission of the United States makes recommendations relating to governance of app developers, advertising networks and app trade associations. Similarly, the App Trust Project is intended to provide developers with easy-to-understand and use icons to communicate the privacy settings and features of apps. However, these governance arrangements are not ecosystem-wide and are not settled. Input from regulators may assist in facilitating and encouraging their adoption in the Australian market.

For the handling of personal information by apps, there have been attempts to foster citizen-friendly processes through industry self-regulatory initiatives. The GSMA Association (GSMA) has developed high-level principles for protection of privacy on mobile networks, devices and apps. These include:

> Data minimisation and retention—only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop apps and services should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.

> Children and adolescents—an application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information are appropriate in all given circumstances and compatible with national law.

GSMA has also published Privacy Design Guidelines for Mobile Application Development which provides more detailed guidance. While there is limited evidence of app providers implementing the principles or guidelines in full, they potentially provide a basis for future engagement with the industry on personal data management.

The Office of the Australian Information Commissioner has developed a consultation draft better practice guide for app developers. The draft guide suggests that developers be aware of privacy responsibilities, be open and transparent about privacy practices, only collect personal information that the apps need to function and securing that information. It also suggests ways to facilitate more meaningful user consent, such as short-form notices and privacy dashboards.

An analysis of many popular apps has shown that they do not comply with these principles and guidelines and that an effective compliance strategy is required to translate them into positive privacy outcomes for consumers. For example, adherence to the guidelines and principles could be required by contracts between app developers and app stores, with financial penalties for non-compliance. Compliance could also be achieved through industry self-regulatory measures. In the

---

45 www.apptrustproject.com. The project is an initiative of the Association for Competitive Technology which represents more than 5,000 small and mid-size developers and information technology firms. The association also has sponsor members including Apple, Microsoft and Facebook.
case of apps, there is scope for industry participants to develop codes providing a stronger set of privacy protections for the digital information exchanged in the use of apps.

The ACMA’s experience with the MPS market has shown that self-regulatory arrangements are most effective if there are strong financial incentives to comply with self-regulatory measures. Therefore, effective compliance monitoring arrangements, backed by effective penalties for non-compliance enforced by the regulator, would be critical to the success of any such strategy.

Communicating with consumers to manage the apps experience

The scale, scope and global nature of the online environment mean that direct regulation is unlikely to be feasible in all cases. Non-regulatory solutions, such as communication strategies, can help to address issues where improvement in knowledge or industry/citizen behaviour is the intended outcome. Communication strategies also offer a flexible response to addressing emerging issues in digital communications and content—such as digital identity management, managing digital reputation and digital literacy and participation—which were not areas of concern at the time existing legislative arrangements were developed.

The Cybersmart program developed by the ACMA is an example of a communication strategy which has been effective in educating children and parents about online safety and supporting participation in the digital economy. The program provides information, resources and activities to help build critical skills and encourage engagement with behavioural issues such as cyberbullying.

In the apps market, similar measures can be considered for educating consumers about the use of technical tools to manage their access to content, their sharing of personal information, in app purchases and usage costs.
Conclusion

The apps market is an important segment of a larger market for a range of software that runs on a wide and growing range of consumer and industrial devices. Computing capability is being incorporated into an increasing range of devices, which require apps to function.

The apps market has grown rapidly over the past five years. A significant proportion of Australians are now using apps which run on smartphones and tablets. The apps market—and the apps market generally—are likely to continue to grow as consumer take-up of smart devices increases.

Consumer satisfaction with the apps environment is generally high, as app developer guidelines, app store rules and technical tools, go part way to ensuring that apps meet consumers’ expectations. However, the level of protection afforded by these requirements varies from one device/operating system platform to another, and there are indications that consumers are concerned with particular aspects of apps personal information sharing practices.

Notwithstanding this overall positive picture of the apps environment, it poses a range of new challenges. The complexity of the emerging personal data ecosystem—driven in part by the way apps use personal information—is such that new approaches to protecting personal information in the online environment generally are likely to be required. The introduction of direct carrier billing for apps has created a regulatory gap in the consumer protection arrangements for app purchase payments.

A mix of regulatory and non-regulatory strategies is likely to be required in managing any issues, which may emerge as the use of apps, and the range of devices on which they run, continues to grow. Direct regulation is expected to continue to play an important role. However, the global nature of the supply chain is likely to give rise to increased reliance on self-regulatory measures and communicating with consumers directly to equip them with knowledge and skills to manage their apps experience.

An overarching consideration in improving consumers’ ease of managing apps and reducing industry compliance costs, is ensuring that the development of any new responses to emerging apps practices occurs within a coherent, single regulatory framework. Such an approach would address one of the key impediments to further innovation in a sector, which is currently subject to a mix of industry and economy-wide regulation.