Emerging business models in the digital economy—The mobile applications market
Occasional paper

MAY 2011
Emerging business models in the digital economy—The mobile applications market
Occasional paper

MAY 2011
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Concepts used in this paper</td>
<td>3</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td>5</td>
</tr>
<tr>
<td>Applications markets</td>
<td>5</td>
</tr>
<tr>
<td>Business models</td>
<td>8</td>
</tr>
<tr>
<td>Third-party developers</td>
<td>11</td>
</tr>
<tr>
<td>Consumer access models</td>
<td>12</td>
</tr>
<tr>
<td><strong>Discussion</strong></td>
<td>15</td>
</tr>
<tr>
<td>Mobile applications and the current regulatory environment</td>
<td>15</td>
</tr>
<tr>
<td>Overall regulatory environment</td>
<td>15</td>
</tr>
<tr>
<td>Regulation of similar markets—mobile premium services</td>
<td>16</td>
</tr>
<tr>
<td>Consumer policy outcomes</td>
<td>18</td>
</tr>
<tr>
<td>Standard consumer safeguards</td>
<td>18</td>
</tr>
<tr>
<td>Content safeguards</td>
<td>20</td>
</tr>
<tr>
<td>Personal information</td>
<td>22</td>
</tr>
<tr>
<td>Data portability</td>
<td>26</td>
</tr>
<tr>
<td>Data use</td>
<td>27</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>30</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td>32</td>
</tr>
</tbody>
</table>
Executive summary

The mobile applications market is one of a range of developments reshaping communications markets through changes in technology and use.

Mobile applications (‘apps’) are software programs that may be installed on smartphones and a growing selection of other devices. Due principally to the increased availability of smartphones—and faster broadband on 3G mobile telecommunications networks—mobile applications are a major growth sector in the digital economy.

This paper provides an analysis of the mobile applications market through an examination of three of the largest app stores. The analysis is designed to identify emerging issues for consumers. It examines the value chain and business models of applications development and use over the web, mobile platforms and managed services, in order to identify potential regulatory issues in the mobile applications market and consider a range of issues faced by consumers.

In 2008–09, rapidly escalating consumer detriment in the Australian mobile premium content space highlighted issues such as changing content delivery methods and business models, mobility and extended value chains. In response to that particular environment, the ACMA determined that sometimes it can be better to respond rapidly and firmly to developments that threaten consumer detriment, particularly where market conditions and product characteristics are not ideal for a co-regulatory approach. For example, there are poor incentives for industry to participate and many small players and/or complex products, especially from a consumer perspective.

Like the mobile premium services market, the mobile applications market is characterised by extended value chains and multiple players. This complexity has the potential to create issues for consumers such as lack of control over transparency and ease of transferring personal information between platforms, measuring data use via mobile applications and the clarity of charging arrangements for data.

Unlike other digital purchases that have one-off data costs, such as music and movies, mobile applications may incur additional ongoing and updating costs. The data use information provided to consumers also varies. Consumers in this market invest both financially and personally in the apps they purchase. This investment may create barriers for consumers to move between services. Some efforts have been made to establish general standards and protocols to promote data portability but this is an area of ongoing development.

The extended value chains and multiple players present in the mobile applications market can make the provision of standard consumer safeguards such as statutory conditions and warranties more complicated. Consumers may have difficulty identifying the responsible party, depending on which aspect of the mobile application purchase is at issue. Further, there are a variety of mechanisms available to apply

---

1 There is no industry-standard definition of a smartphone. However, most commentators agree that a smartphone is a mobile phone offering advanced capabilities, often with PC-like functionality (PC–mobile–handset convergence).

2 A retail component of platforms. Their primary business activity is the sale of apps, in contrast to platforms with other functions such as social networking sites.
content controls, such as restricting access by children, but an examination of three of
the largest apps stores highlights that the application of content controls varies.

Privacy issues in the mobile applications market reflect the ongoing societal debate
about the line between public and private information, and the control of personal
information. Security of personal information in this market also has a number of
layers, as consumers interact with several separate groups to whom they provide
personal information. Augmented reality and location-based services (LBS), which are
already present in the mobile applications market, also pose challenges for privacy, as
the distinction between personal and public information is blurred.

Education of both consumers and market participants on their current rights and
responsibilities is an important issue. In an innovative market such as mobile
applications, there is an evident need for regulators to continuously monitor market
operations and assess the potential for consumer detriment and regulatory concerns.
Introduction

The mobile applications market offers a useful illustration of the issues being raised by platform, device and service convergence occurring in the communications sector, with implications for the overall regulatory environment.

This paper examines issues consumers face in the market—in particular, content, privacy, and personal data security and portability issues—and the challenges of regulating markets with extended value chains and multiple international players.

Concepts used in this paper

This section outlines the main concepts discussed in the paper. For further definitions of specialised terms please refer to the Glossary.

**App stores**—retail components of platforms. Their primary business activity is the sale of apps, in contrast to platforms with other functions such as social networking sites. App stores are managed by a number of different types of operator. They provide simple payment mechanisms and easy-to-use environments, often linked to a device brand. For mobile applications sellers, app stores provide direct access to consumers and a reliable payment mechanism.

**Mobile applications**—commonly known as apps and applications, mobile applications are software programs that may be installed on smartphones and a growing selection of other devices (tablets, some digital set-top boxes, laptops, desktop computers). Mobile applications are not limited to mobile devices only—they are available, and can be used, with both fixed-line and mobile services.

Application software differs from system software (that is, operating systems) in that it is usually designed to fulfil one particular task or function. Mobile applications enhance the basic features of a device by providing additional functions and features that increase its usefulness and improve the user experience. Generally, mobile applications have the following characteristics:

> they are available via online download
> they enhance a device’s practical and entertainment functions
> they are designed to perform a specific function or related functions
> they operate on, but do not alter, the operating system software
> they may be free of charge (excepting data use costs) or paid
> they are generally 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.

**Mobile applications market**—one in which the buyers (consumers/users) and sellers (app developers) of mobile applications come together. This occurs online through dedicated retail platforms (app stores), accessible through the consumer’s device. As mobile applications are initially sourced online via an app store, a data connection and accessing device are required. As a result, the supply of data and devices is closely associated with the mobile applications market.

**Consumer policy outcomes**—consumer policy goods are programs or standards that are implemented to seek social policy outcomes. This can be done via a number of

---

3 Refer to the section ‘Consumer access models’ on p. 12 for a full description of the methods for accessing mobile applications and app stores.
mechanisms including legislation, self-regulatory bodies, or codes of conduct and industry or consumer education programs. The main consumer policy goods sought in the communications market may be categorised as:

> **Content safeguards**—aim to promote the availability of a diverse range of content, respecting community standards and empowering consumers to make informed choices. This includes provision for:
>  > classification of content/adult content/illegal content
>  > protection of children from harmful content.

> **Standard consumer safeguards**—aim to promote the provision of safeguards for consumers including individuals and vulnerable groups, and empowering users. This includes provision for:
>  > billing arrangements—itemised accounts, secure payment, accurate charging
>  > warranty/guarantees/refund arrangements
>  > quality of service issues—statutory conditions and warranties
>  > protection from false and misleading representation.

> **Personal information safeguards**—aim to promote the protection of personal information including:
>  > privacy of personal communications
>  > holding and portability of personal information, including provision of information to third parties
>  > personal information security.
Background

This section provides a summary of the structure of, and participants in, the mobile applications market.

Applications markets

Mobile applications are commonly made available through aggregators with online stores. Mobile applications aggregators are not new to the communications industry. Online stores offering mobile phone ringtones, themes and other applications have existed since the late 1990s. However, due principally to the increased availability of smartphones and faster broadband on 3G mobile telecommunications networks, mobile applications are a major growth sector of the information and communications economy.

App stores may be categorised as:

- **Device manufacturers**—including Apple’s App Store, Nokia’s Ovi, and Blackberry’s App World. These stores can be used only by consumers with the appropriate manufacturer’s device and proprietary software.
- **Operating system developer**—including Android Market and Microsoft Windows Mobile. These stores can be accessed by consumers with devices from multiple handset manufacturers via the proprietary operating system software (OS). For example, Android mobile applications can be used on Motorola, HTC and Samsung devices.
- **Mobile network operator**—including Telstra, Verizon and Optus. These stores can only be accessed by consumers with service contracts with the network operator. Consumers can use multiple handset brands to access these stores.
- **Independent**—including app stores operated as independent commercial concerns, or by developers such as GetJar and Mobango. Access to these stores is not dependent on the brand of device used, service provider or proprietary software.

The mobile applications market exhibits a number of common characteristics across all app stores, including:

- **Low barriers to entry**—Apple, Android and Blackberry all have development registration schemes with software development kits (SDK) offered free or at low prices with additional support mechanisms (for example, registration for individuals to develop iPhone apps costs $99). Mobile applications can be developed with SDK for low fixed costs.
- **Strong competition**—there are a large number of sellers and mobile applications available to consumers (more than 300,000).
- **Low barriers to exit**—with few sunk costs, developers may enter and leave the market quickly.
- **Extended value chains with multiple players**—mobile applications delivered through various platforms complicate the supply chain to the end-user. The responsibility for aspects of customer service can consequently fall across several different organisations or individuals. This increases the complexity of the relationship between service providers and end-users. For example, a mobile application is provided by the app developer, distributed by an app store via bandwidth provided by a network operator. All these parties will then have a role in service delivery to the end-user.
- **Global nature**—app stores are accessible from smartphones and other devices globally, and have a global consumer base, although most of the major market players have managing companies based in North America (Apple, Google,
Blackberry, Microsoft Windows and Palm). As a result, there are associated cross-border and trans-jurisdictional market implications. For example, distribution of content is often governed by geographical distribution and copyright agreements, which app stores need to comply with. There may also be issues associated with regulating individuals and entities located in international jurisdictions.

> **Unpredictable revenue**—the financial viability of mobile applications is variable. The top 10 per cent achieve about 75,000 downloads and there are huge successes, such as Tap Tap Revenge’s reported revenue of $1 million per month. However, 50 per cent of mobile applications achieve about 1,000 downloads and, after the app store has taken its cut, developers may expect to earn up to $2,500 on average.

Since 2001, when the first online app store retailing mobile applications was established (by Qualcomm BREW), the market has grown steadily. However, with the release of the Apple iPhone 3G in July 2007 and the opening of the Apple App Store in 2008, growth of the mobile applications market has been exponential. Most commentators agree that Apple’s opening of iPhone to third-party developers via the App Store in July 2008 was a key turning point in the adoption of smartphones and the use of mobile applications. By 2009, combined platform revenues were $4.2 billion, with some analysts expecting revenues to reach $29.5 billion by the end of 2013.

Smartphone market share (in terms of number of handsets sold) of the overall mobile market is growing rapidly. As of November 2010, smartphones comprised 23 per cent of the handsets sold in the US mobile market, in comparison to 16 per cent in quarter two, 2009. This pattern is also reflected in the Australian market, where Telstra data indicates that 73 per cent of mobile phones sales in Australia in the period September 2010 to February 2011 were smartphones. Currently, device manufacturer and operating system developer app stores have greater prominence in the mobile applications market than either network operator or independent app stores.

---

3. Bright, op. cit.
5. Third-party developers are those who write software for devices but are not directly affiliated with the device or operating system manufacturers.
The ACMA collected consumer data about mobile network broadband usage in April 2009 and April 2010. In April 2010, of those Australian household consumers 18 years and over with a mobile handset, 64 per cent had a 3G mobile handset—a nine percentage point increase since April 2009.

In the first quarter of 2009, shipments of smartphones exceeded those of voice-centric mobile handsets. The Apple iPhone accounted for 21 per cent of Australian smartphone sales during this period. Increasing take-up of 3G mobile handsets in Australia highlights the growing penetration of smartphones into the Australian market and the associated availability of mobile applications.

Figure 2 shows the range of functions now available on mobile handsets and the use of these functions by consumers aged 16 years and over. The already significant use of mobile applications by Australian users (47 per cent of 3G users access mobile applications), combined with the rising number of smartphones, illustrates the potential for future growth of the mobile application market in Australia.

---


Business models

Prior to the introduction of smartphones, telecommunications network operators were the main suppliers of mobile services (and fixed-line services). End-users’ choices were influenced predominantly by network coverage, pricing, provision of handsets and value-adding services (such as voicemail, text, email and limited 2G web access via GPRS). Hardware and software component suppliers had only an indirect relationship with end-users, and third-party suppliers provided complementary goods and services.

While not all consumers directly obtained their handsets through their network operator, operators still controlled service subscriptions. Further, with the initial introduction of web browsing and email capabilities, network operators launched ‘walled garden’ application platforms to maintain their centrality in the value chain. The key relationships in the market model are shown in Figure 3.

Figure 2 Mobile device functions and use in Australia

![Chart showing mobile device functions and use in Australia]

% of persons 16 years and over with a mobile phone

Source: Nielsen, The Australian Internet & Technology Report, February 2010. Note: question did not include the use of voice services.

---

The introduction of smartphones and the availability of 3G technologies (offering increased bandwidth) have driven changes in the mobile service business model in recent years. In particular, the role of handset and OS providers has become more prominent, and the reliance of third-party developers (developers of mobile applications) on network operators for delivery of revenue streams has decreased (see figures 4 and 5 below).

In addition, Apple’s revenue-sharing arrangements with developers has led to other changes. Apple reshaped the revenue model with its 70/30 revenue split in favour of developers and the exclusion of network operators from revenue-sharing arrangements for mobile applications, attracting large numbers of new developers to its app store.\textsuperscript{16} This revenue model has become the de facto revenue-sharing standard in the mobile applications business.\textsuperscript{17}

It has also driven the proliferation of non-network operator app stores as handset manufacturers and OS providers seeking to capitalise on alternative revenue streams. Network operators are no longer the primary source of revenue for app developers, and consumers of mobile applications are not reliant on the walled gardens of their network operator to access mobile applications.

The growing popularity of smartphones and tablet devices has continued to fuel this shift in the market, and access to third-party applications via a variety of devices is now being dominated by device and operating system manufacturers (through their app stores), as shown in figures 4 and 5.


\textsuperscript{17} Ibid.
The Wholesale Applications Community (WAC), an alliance of 48 telecommunications providers, device manufacturers and sponsoring businesses (for example, Alcatel-Lucent) has launched a wholesale app store.\(^{18}\) In response to the current success of non-operator app stores, the WAC model allows network operators to sell mobile applications to their subscribers independent of the device being used via an open platform, and charging them via their phone bill.\(^{19}\) Network operators capture a percentage of the mobile application purchase price as well as the revenue raised from data use. At present, many network operators are only receiving revenue from data use for mobile applications or are reliant on partnerships with device manufacturers to obtain a share of mobile applications sales revenue.

The current contest for market share in the application market is now primarily between the opposing business models of operating system and device manufacturer app stores. Operating system business models offer an open source system, with consumers able to access mobile applications from multiple sources. Device manufacturer models are closed proprietary environments limiting distribution of mobile applications to consumers via a single source—their app store.

---

\(^{18}\) [www.wacapps.net/web/portal/faq](http://www.wacapps.net/web/portal/faq), viewed 17 November 2010.

\(^{19}\) Ibid.
Third-party developers

Third-party developers are creators of mobile applications programs who do not work directly for the app store, device manufacturer or network service operator. There are several kinds of third-party developer:

> *hobbyists*—those developing mobile applications in their spare time for recreation and profit

> *professionals*—those developing mobile applications as a main source of income, either alone or as part of a business centred on mobile application development

> *contractors*—those developing mobile applications on behalf of another entity or individual.

The number of third-party developers has increased significantly as the improved revenue arrangements and increasing client base attract more developers to app stores.

The majority of app stores provide programs and support to encourage third-party development in their platform. There are a number of components to this support:

> distribution of revenue is weighted to favour developers—the revenue split in the largest app stores is 70 per cent to the developer and 30 per cent to the store\(^{20}\)

> there are no access restrictions or qualifications in place

> developer support includes access to SDK in the native code (software language) of their app store, developer forums, developer guidelines and other support mechanisms

> start-up costs are low—three of the largest app stores provide developer support programs for $200 and under\(^{21}\)

> marketing information and user analytics are also available

> secure payment mechanisms are provided

> access is provided to a ready-made customer base

> advertising of the app stores to consumers is provided by device manufacturers and, in some instances, network service providers

> advertising of individual mobile applications in an app store is also available—for example, developers can pay a premium to have a mobile application placed in the featured section in the Apple App Store.

Third-party developers may also operate across more than one app store. This means that the mobile applications can either be written in the native code of each platform or written in a higher level software language, which can run on all platforms the developer is selling on.\(^{22}\) The choice of developing language is complicated by restrictions proprietary platforms may place on using programming tools or controlling certain device features and by fragmentation across device platforms. For example, both Android and Blackberry run different versions of their OS on different handsets. Different versions of an OS may have varying levels of support for functions and actions in a mobile application, which impacts on the choices an app designer makes when creating a mobile application.

However, third-party developers are not entirely reliant on app stores to sell their product. Developers may offer product independently, such as on their own website. Developers involved in contracting may work exclusively outside of the app stores, selling individually designed products to enterprise clients. Such products may or may

\(^{20}\) Apple App Store, Android Market and Blackberry App World offer the 70/30 split in favour of developers.

\(^{21}\) Apple—$99, Blackberry—$200, Android—free.

\(^{22}\) Flash, HTML 5 and Java ME are examples of codes that can operate across different platforms.
not be sold in an app store. For example, a university may commission the
development of a mobile application for internal use by staff and students, while
Hershey has commissioned a mobile application, which is available free to consumers,
to promote their product range through app stores.

Third-party developers create revenue from mobile applications in several ways:
> purchase of the mobile application by a consumer
> in-app purchases (game money, for example)\(^{23}\)
> in-app advertising
> subscription services (a limited number of mobile applications are available via
subscription)
> sale of the mobile application as a product.

As there are no formal qualifications required to become a third-party developer and
the associated sunk costs are low, developing is open to a broad range of individuals
and other entities.

**Consumer access models**

The concept of online stores for consumers to download software applications is
continuing to expand, with Dell opening its Dell Download store, Google creating a
Chrome download store and Apple expanding its concept to include the MAC App
Store (a distribution platform for MAC OS X applications).\(^{24}\) Mozilla Firefox is currently
developing an open-source store and Amazon has opened an Android App Store to
complement its other online businesses.

The devices used to access app stores vary, and the numbers and types of device
used are increasing. App stores and other platforms can be considered access points
that allow consumers to obtain and use mobile applications, distributed by multiple app
developers. Figure 6 illustrates the multiple paths consumers can use to access
mobile applications from these points.

---

\(^{23}\) Not all platforms have enabled in-app purchase functionality.

\(^{24}\) GetJar has suggested that in 2009 there were 38 mobile applications stores in operation. See Pascal-
Emmanuel Gobry, ‘Number of “App Stores” grew from 9 to 38 in 2009’, Business Insider, 17 March 2010,
www.businessinsider.com/mobile-mobile applications-are-hot-hot-even-more-so-than-you-thought-
2010-3, viewed 25 November 2010.
Mobile applications may be obtained by end-users in two main forms—as pre-installed applications or downloaded applications. Pre-installed mobile applications are selected by device manufacturers and usually include:

- utilities (for example, calendars, alarm clocks, camera/photo apps)
- services (for example, weather mobile applications, Google maps, a compass, a world clock)
- entertainment (for example, music, video, games)
- communications applications (for example, web browsers, texting and voice applications).

Pre-installed mobile applications can increase the commercial viability of devices. The pre-installation of mobile applications from other commercial entities on devices is a method for device manufacturers to defray production cost, and increase the attractiveness of their device to consumers. It is also a useful method of creating additional revenue streams for carriers who pre-install their own apps prior to sale of the device to consumers—for example, Telstra Bigpond apps, Optus Zoo apps. Apple includes iTunes and Safari (web browser) as standard mobile applications on the iPhone, which develops and supports audiences for its current products. YouTube is also pre-installed on the iPhone 4, reflecting a commercial arrangement between Apple and YouTube. Similarly, Google Maps comes pre-installed on most smartphones.

Mobile applications may be downloaded and installed by consumers in several ways:

- Via the device—consumers can directly access the device manufacturer’s app store through a menu on the device, and download and install a mobile application. Access may be enabled through 3G or Wifi networks (in Wifi-enabled devices).
- Via the internet—consumers can access the device manufacturer’s app store (or, if applicable, the network provider’s app store) via the web browser on their device, and then download and install mobile applications. Access to the internet may be enabled through 3G networks or Wifi networks (in Wifi-enabled devices).
Via personal computers—consumers can download mobile applications via the internet to a personal computer (using proprietary software that provides access to the app store) and then load these onto devices through USB or Bluetooth connections.

Mobile applications range in price, from free (excepting data download costs) to $999. The average cost is under $10, with over 50 per cent of all mobile applications across all the app stores priced at $2 or less. Payment for paid mobile applications is made through one-off transactions or ongoing subscriptions in the following ways:

- **Credit card**—this is the most prevalent method in Australia. The interface is established through a consumer account (for example, an iTunes account for Apple or a Google account for Android).

- **Carrier billing**—this method is common for mobile commerce transactions, but is currently not common in app store arrangements in Australia. This is the payment method that the WAC proposes to use for its app store. Payment appears on a consumer’s bill or in the form of a call-credit deduction or charge. This is similar to current payment arrangements for mobile premium services. The revenue split in this situation may incorporate a percentage to the carrier. For example, Nokia’s Ovi store provides for a revenue split of between 40 and 50 per cent of the end-user purchase price to the carrier (depending on the cost of the mobile application), with the remainder divided between the developer and Nokia on a 70/30 basis. For a mobile application costing $1.19, this would result in a distribution of approximately $0.59 to the carrier, $0.42 to the developer and $0.18 to Nokia.

- **Voucher redemption**—app store-specific vouchers are available at multiple commercial outlets. These may be redeemed for credit via a user account. Credit card companies also provide gift vouchers that may be used for the same purpose.

Closed proprietary app store business models offer systems integration for consumers and a seamless user experience. App store business models that use an open source operating system may not be able to offer as efficient systems integration due to the fact that multiple players may be involved in the provision of devices to access the App store. However, the open source operating system business model allows consumers more choice in terms of sourcing mobile applications and greater transferability of information between platforms. Both business models have inherent advantages and disadvantages for consumers, who will ultimately choose which is more significant to them.

Meanwhile, network operators are seeking to offset the costs of increasing demands on their networks in terms of speed and resources from mobile applications. The WAC's commercial app store is one method of doing so, as it allows network operators to once more access the mobile application revenue stream. The success of this business model is dependent on the experience it can provide for the user.

The different app store business models highlight the inherent differences in approach to access and control on different platforms. In the longer term, the success of each business model may depend on consumer attitudes to these differences.

---

Discussion

This section provides an analysis of the mobile applications market through an examination of three of the largest app stores. These three were selected as they:

> are representative of the main models of app store currently available
> are stores with a high population of mobile applications and large developer communities
> are associated with several of the most popular brands of smartphones
> represent the majority of market share in terms of smartphone operating systems.

The market is assessed against the current regulatory arrangements that relate to mobile applications, with particular reference to consumer policy outcomes.

Mobile applications and the current regulatory environment

Overall regulatory environment

Mobile applications and app stores are subject to multiple regulatory schemas, (see Figure 7). In part, this reflects the capacity for mobile applications to be used with both fixed and mobile services. For example, eBooks purchased using one of the many eBook reader applications can be bought on mobile devices such as smartphones (either using 3G or Wifi) or through home computers (fixed broadband). The eBook can also be read from both devices, and the reader’s notes and bookmarks synced between the two.

The distinction between content and software also holds less meaning in the mobile applications market. The distinctions currently made between delivery platforms for regulatory purposes are based on technological differences in these platforms and are designed to support legislative objects. However, the same content is now accessible to consumers across a number of different platforms and the delivery mechanism is incidental to the purchase and use from the consumer’s perspective.

For example, the Australian Broadcasting Corporation (ABC) has audiovisual content that is accessible on its digital broadcasting channels. The ABC makes the same content accessible via the ABC iView mobile application, which is a software application. From a regulatory perspective, the two delivery mechanisms are subject to differing aspects of regulation. With entities now providing content and services across multiple delivery platforms, the regulation they are subject to may be inconsistent in its application to the same content. Technological developments such as the smartphone and mobile applications are also blurring the traditional divide between content and carriage services. Both types of service can now be accessible from the one device. Using a smartphone, it is possible to watch the ABC news report and, with the same device, make and receive a voice call, or send a text or email.

The mobile applications market functions on both a national and global scale, and this has implications for regulation in Australia. The app stores analysed for this paper are all based overseas, which is representative of the market as a whole at this time. App developers are also based in multiple international jurisdictions. For example, one of the most successful paid mobile application games in recent years, Angry Birds, was created by a company in Finland and is distributed across multiple platforms by a company based in the US. The game is played by people in over 30 countries worldwide.
Mobile applications have emerged from the convergence of content and telecommunications services. As a result, the market functions in a complex regulatory environment involving aspects of multiple regulatory schemas, as Figure 7 shows. This complexity is illustrative of the issues that new technology and services in the digital environment are presenting to regulatory agencies.

Figure 7 Regulatory aspects of the mobile applications market

---

**Regulation of similar markets—mobile premium services**

The ACMA has primary responsibility for compliance and enforcement activities under the *Telecommunications Act 1997*. The Telecommunications Industry Ombudsmen (TIO) also plays a role in the resolution of consumer complaints for telecommunications services, including billing disputes. Regulatory measures for mobile premium services put in place by the ACMA under the Telecommunications Act may also have relevance to the mobile applications market.

Mobile premium services have some similarities with mobile applications in relation to the devices employed to access and use them, although mobile application providers do not fall within the provisions of this code. Notwithstanding significant differences between mobile premium services and mobile applications in terms of their respective business models and value chains, consumers may have expectations that the
protections and values present in the mobile premium services environment are also represented in the mobile applications market.

The Mobile Premium Services Code C637:2009\(^{26}\) (MPS code) and related service provider rules were introduced as a result of growing consumer complaints about charges for mobile premium services. The objective of the MPS code is to establish and support appropriate community safeguards and customer service requirements for mobile premium services. The code is designed to ensure that consumers are:

- informed at sign-up
- understand the costs of the service
- have the ability to remove or stop the service.

The ACMA has articulated five core principles about consumer experience in the communications sphere, which have informed its recent review of the MPS code. These principles are:

1. The clear and accurate advertising of a product or service.
2. Products and services will be provided under clear and fair terms set out succinctly.
3. Costs associated with a product or service will be clear and unambiguous.
4. Assistance for the consumer will be readily accessible and provided in a timely manner should a problem be encountered.
5. Avenues for redress will be clearly identified for the consumer in the event that problems are unable to be rectified satisfactorily.\(^{27}\)

Although the MPS code is not applicable in the mobile applications market, the principles it seeks to implement are those which the ACMA believes may promote effective standard consumer safeguards. As a result, the MPS code provides a reference point for assessing the effectiveness of the consumer protections in the mobile applications market. The mobile applications market support of consumer protections is analysed against the requirements of the MPS code below.

**Customer information about prices, terms and conditions before/at time of purchase**

- Users are required to create a user account or ID and are provided with a copy of the terms and conditions of use on registration.
- Users are required to read and consent to the terms and conditions before being able to access any of the three platforms. The length and complexity of the terms and conditions varies significantly between platforms.
- Prior to purchasing a mobile application, users are able to access a profile on the app store that provides a brief outline of the application's functions, its download size, a classification rating (where the store has a ratings system), a user rating, the language and technical requirements, a link to the developer's website and its purchase price.

**Customer consents to provision of service based on accurate information about price, terms and conditions**

- The initial cost of purchasing a mobile application is clearly stated.
- Consumers are provided with the download size of the mobile application so they can calculate the data use cost. However, there is no indication of the ongoing data use of the mobile application and so no way of calculating ongoing data costs. Only


one app store requires all mobile applications to inform users when they are accessing data within a mobile application.

> There is no indication of the amount of ongoing data use by the mobile application and so no way of calculating ongoing data costs.

**Ability to remove or stop service**

> Mobile applications can be simply and easily deleted from a consumer's device and computers with the press of a button.

> Current subscription services are periodical, with consumers required to resubscribe. Failure to resubscribe will discontinue the service.

**Consumer policy outcomes**

**Standard consumer safeguards**

Users of mobile applications may expect to benefit from standard consumer safeguards—such as product warranties and guarantees, refund arrangements, quality of service conditions such as fitness for purpose, and prohibitions on false and misleading representation—that apply to the sale of computer software and other types of digital content. The Australian Competition and Consumer Commission is primarily responsible for compliance and enforcement of the regulatory requirements of the *Competition and Consumer Act 2010* (CCA), which regulate consumer policy safeguards such as those described. Federal, and state- and territory-based consumer protections and fair trading requirements are standardised under the *Australian Consumer Law 2011*.

Standard consumer safeguards are a key feature of consumer policy and the different approaches adopted for distinct delivery platforms illustrate one of the challenges for consumers arising from service convergence in the communications market. An assessment of the mobile applications market's approach to standard consumer safeguards is outlined below.

**Billing arrangements—including itemised accounts, secure payment and accurate charging**

> Purchase history is available online or via the payment facility.

> Purchases can be made by credit card, redemption of voucher or carrier billing in all stores.

> Secure payment facilities are available either directly from stores or via outsourced payment facility providers.

**Warranty/guarantees/refund arrangements**

> Refunds are available across all stores. Specifics in terms of time frames and methods of applying for refunds vary across the mobile applications market. One store offers an unconditional refund within 24 hours of the purchase of the mobile application.

> The mobile applications market in general supports legislated guarantee and warranty provisions.

**Quality of service issues—statutory goods and warranties**

> App developers are the final responsible party for quality of service issues for their products and services. Contact information for developers is available from the advertisement featured in the app stores, and sometimes within the mobile application itself.

---


29 Carrier billing is only available from those carriers who support this function.
Some technical and product support information is available via the different platforms to further support consumers.

False and misleading information

Consumers can seek redress through either the platform or the developer, although app developers are the final responsible party.

The preceding analysis highlights one of the main issues faced by mobile applications users in obtaining standard consumer safeguards—complexity in the supply chain. Consumers may have difficulty identifying who the responsible party is, and this may vary according to which aspect of the mobile application purchase or use is problematic. For example, the provision of billing and service arrangements is fragmented in the mobile applications market as responsibility for different aspects of the service is divided between app platforms, app developers, network service providers and financial institutions.  

However, unlike the early problems in the delivery of consumer safeguards and customer service experienced in the MPS environment, there is in mid 2011 little evidence of high levels of consumer dissatisfaction, detriment or complaints in the mobile applications market.

In general, app stores provide mechanisms to report problems, forums for resolution and user rating systems. However, primary responsibility for product and service issues remains with the app developer, financial institution or network provider. As the central contact point and distributor, app stores may have a greater role to play in consumer protection than is currently advocated by the stores themselves. Anecdotal evidence suggests that the bulk of consumer complaints are about inappropriate content, data use, intellectual property infringements and proprietary restrictions on devices.

The apparent low level of consumer dissatisfaction with mobile application services and products may in part be due to the fact that the market exhibits a high level of consumer control. To incur a cost, consumers must first authorise each purchase and download the initial product. In addition, a high percentage of mobile applications are free, with consumers only incurring related data use costs, while many popular paid mobile applications offer a free ‘lite’ version for consumers to trial. This means early issues experienced by consumers in the MPS environment, such as non-consensual charging and issues of informed consent, are not as relevant in the mobile applications market.

Consumers are also able to more easily opt out of services in the mobile applications market than in the MPS environment. For example, to stop a MPS subscription service, consumers must opt out of the service by contacting either the mobile premium service provider or their carrier. Charging in the MPS environment was also an issue due to the post-paid nature of carrier billing. In contrast, current subscription

---

30 Apple advised consumers whose iTunes accounts had been fraudulently charged for mobile applications by a third-party developer to contact their credit card issuer. See www.theaustralian.com.au/australian-it/mobile-applications/-bans-developer-for-itunes-scam/story-e6frgakx-1225868818248.


32 Authorisation involves security measures to access the consumer’s account. For example, authorisation in the Apple App Store to purchase a mobile application requires a three-step process before the purchase is authorised:

1. Select app
2. Press download
3. Enter username and password for consumer iTunes account.
services in the mobile application market are opt in. Consumers are required to pay for each subscription period up-front and resubscribe on a periodic basis, giving consumers more individual control.

Another significant difference between the MPS environment and the mobile application market is the presence of the app platforms. The main source of mobile applications for a consumer is their proprietary app store, which has a set format for advertising mobile applications. Consumer ratings and reviews form part of this format, providing further guidance for prospective purchasers. Each platform controls and manages its related app store and the mobile application market is currently characterised by large, high-profile corporations with significant investments in the associated proprietary technology and reputation. It is in the direct commercial interest of these operations to provide quality customer service and protect the interests of their users. Current agreements between the major platforms and developers all stipulate codes of practice for developers, although the nature and extent of safeguards provided to consumers varies between platforms.

Mobile applications have low up-front fees. This may mean that consumers are not motivated to complain when a product does not meet their expectations or is faulty, choosing instead to delete the product, provide a negative user rating, or find a more reliable or successful one.

Monitoring of the mobile applications market will need to continue as it is still immature. Levels of consumer risk and detriment in relation to the standard consumer safeguards may change.

**Content safeguards**

Content classification in the mobile applications market is similar to that in other online environments, and comes under the online content scheme in schedule 7 of the *Broadcasting Services Act 1992* (the BSA). The online content scheme is a complaints-based system with provision for the reporting and removal of prohibited content, and the provision of access restrictions for material rated MA 15+ and above. Complaints for non-game mobile applications are made to the ACMA, which may then seek advice on the classification of material from the Classification Board. Schedule 7 of the BSA gives the ACMA the power to order the take-down and removal of material considered to be prohibited content that has been refused classification or for material rated MA 15+ that does not have access restrictions.

Concerns about content classification have been raised previously in both the internet and MPS environments, which have similarities to the mobile applications market. As well as supporting community standards, content classification is a primary mechanism for protecting children by providing a tool to limit their access to inappropriate material. The protection of children is an object of the BSA, which achieves that object via legislative mechanisms such as content classification and access restrictions.

The use of the online content scheme to classify and regulate content in the mobile application market is not necessarily intuitive for consumers. Given that mobile applications are primarily accessed and used through a mobile phone (telecommunications) at present, the link with the online content scheme (broadcasting) is not obvious. This may require education of consumers and market participants about the appropriate avenues for complaints and resolution of consumer issues with mobile applications content.

---

33 For example, the subscription to *The Age* iPad app must be renewed by the consumer monthly, with each month’s subscription fee paid up-front.
An assessment of the mobile applications market's support of content safeguards is outlined below.

**Classification of content, including illegal and adult content**

> The majority of the app stores analysed have instigated an approval process, which developers must complete for each app prior to publication on the app store. One app store only requires developers to register and agree to the developer’s terms and conditions, without any further review processes before publication on the app store.

> Self-regulatory action is being demonstrated by app stores through their removal of mobile applications deemed inappropriate.34

> Formalised classification systems are present in some app stores in the mobile applications market. Those stores are using self-developed systems, not aligned with Australian classification standards. All the app stores have prohibitions against sexually explicit material, harassment and bullying behaviours, racism, abusive language and hate material in their developer terms and conditions.

> All the app stores have a user rating system and the ability to flag an issue with the mobile application to the store distributing it, as well as the responsible developer.

**Protection of children**

> The majority of the app stores surveyed indicated in their terms and conditions that the service was for users aged 13+.

> Provision of parental and content restriction settings is variable across the app stores. One has content restrictions available via user’s accounts, but restrictions settings on devices vary between device models and manufacturers. One store has content and parental restriction settings that could function via proprietary access software, for all devices using that software or settings that could be enabled on individual devices. Another store has restrictions available for enterprise clients that can be implemented and a setting for disabling data access that private users can enable. However, the private data access restriction is able to be easily reset from the device.

> There are also mobile applications that can be purchased to perform content restriction and monitoring functions.

App stores in the mobile applications market have shown evidence35 of a willingness to undertake self-regulatory activities for content classification, but levels are not consistent across the industry or even within the various platforms. Not all of the app stores reviewed had a formalised content classification system, and those that did were platform-specific systems and not aligned with the Australian classification system. Consumers may find the disparities between the systems confusing, hindering their effectiveness. As one store allows app developers to nominate classification ratings for their products, the objectiveness of the system is also questionable. There is anecdotal evidence mobile applications being used and purchased from platforms by children as young as three years36, which also places doubt on statements by app stores about age restrictions for these services.

---


35. Both Apple’s Appstore and Android have in recent months removed content that was deemed inappropriate or sexually explicit, or that may have breached copyright patents. See Matt Hamblen, 'Apple targets “objectionable” apps, leaves Playboy, S.I. in app Store', Computerworld, 24 February 2010, www.reuters.com/article/idUS24328901720100224.

Access controls vary across the app platforms and, as more consumers adopt the necessary technology, the protection of children is likely to be of increasing concern, including:

- access to inappropriate content
- inadvertent loss of privacy/personal information
- inadvertent expenditure (purchases and data use)
- exposure to online predatory behaviours.

App platforms that support devices from multiple manufacturers are less likely to be able to standardise access controls than those relying on a single proprietary device brand. The ACMA has the power under clause 14, schedule 7 of the BSA to legislate for the provision of a restricted access system—it recently legislated for the provision of a parental lock feature for specified domestic reception equipment. Currently, the largest app stores are promoting a 'family-friendly' environment and have taken strong stances on the provision of pornography, violence, and otherwise inappropriate material. However, if MA15+ and R18+ material becomes commonplace, as it has in the online and MPS environments, further analysis of access restrictions may be required.

Access controls and content restrictions are only some of the mechanisms that may be used to protect children, but they are commonly represented in a number of content markets. Other commonly used mechanisms include self-verification (users are asked to provide their date of birth), and requesting credit card or banking details. For example, the MPS environment limits the provision of MA15+ and R18+ content to restricted number ranges commencing with the digits 195 and 196. Access can only be provided to these number ranges after the carrier verifies that the customer is the account holder. It is important to note that currently in Australia, an efficient and reliable means of verifying age online is not available. Indeed, even ‘offline’ mechanisms for proof of age are subject to a level of abuse.

The effectiveness of the current Australian content legislation in the mobile applications market is currently under review. The Standing Committee of Attorneys-General (SCAG) in its first meeting for 2011 announced an interim approach for the classification of mobile applications and online games while a review of the National Classification Scheme is undertaken by the Australian Law Reform Commission. The review will investigate methods to accommodate and better anticipate technological and other developments and is expected to be completed in two years. The responsible minister, the Hon. Brendan O’Connor MP, Minister for Home Affairs and Minister for Privacy and Freedom of Information, outlined the proposed interim measures that will seek to move the classification of mobile application games to a complaints-based system in a manner consistent with other online content.

**Personal information**

The protection and control of personal information has become increasingly complex in the digital environment, with security of personal information and privacy big issues.

---

In Australia, privacy is overseen by the Office of the Australian Information Commissioner, which administers the *Privacy Act 1988*. State- and territory-based legislation provides similar safeguards. Privacy within telecommunications networks is subject to the Telecommunications Act and arrangements currently centre on voluntary codes, for which the ACMA has monitoring and enforcement responsibility. Privacy is an issue of some public concern and continues to be raised in relation to a broad spectrum of technological developments.

An analysis of the approach to personal information privacy within the mobile applications market is outlined below.

**Privacy of personal communications**

> All the app stores reviewed had privacy policies stating that all personal information collected will be protected and not sold to third parties. However, this was only relevant to the platform’s products and services, and did not cover information collected by third parties such as app developers. One app store reviewed also specified in its developer terms and conditions that mobile applications will not collect or sell information unless provided with written consent. App stores specified that these conditions did not cover information the users willingly contributed to forums, blogs or chat rooms, for example.

> All app stores offered support contact details for concerns about privacy.

**Holding and portability of personal information, including provision of information to third parties**

> All the app stores reviewed had privacy policies stating that all personal information collected will be protected and not sold to third parties. However, this was only relevant to the platform’s products and services, and did not cover information collected by third parties such as app developers.

> The majority of app stores analysed also had optional mechanisms to prevent tracking of an individual’s use patterns. However, these were only relevant to the platform’s products and services. The other app store specified that its developers would not collect and sell information to third parties without written consent.

> For all the app stores, information from user accounts was transferable across multiple devices, but for some of them, this was only between devices proprietary to the specific platform.

> One app store allowed for the transfer of user information to some other platforms such as social networking sites.

**Personal information security**

> App stores allow for consumers to purchase products using their account username and password. This means that payment details do not need to be re-entered when purchases are being made via smartphone and other mobile devices, which are less secure than desktop environments.

> All app stores reviewed claim that user information is secure and encrypted.

Ongoing public concern about privacy and personal information security on social networking sites highlights their importance. Security in the mobile applications market also has a number of layers, as consumers are potentially interacting with several separate entities to whom they provide personal information. This is illustrated in Figure 8 below.
Currently, smartphones do not have virus protection at the levels consumers are accustomed to on desktop and laptop computers, and there have already been reported instances of malware and data-mining viruses being present in various app stores.\footnote{www.theage.com.au/digital-life/smartphone-apps/cybercrims-turn-to-smartphones-20100809-11tm4.html} Consumers are accustomed to security software providing protection from phishing, malware, bad cookies and changes to basic operations. The lack of this level of protection on smartphones may be an issue. Targets for a virus or other malware require a population density to make the infection worthwhile. With the growth in the population of smartphones and the ability of handsets to log on to cellular or Wi-Fi networks and to be brought into otherwise secure locations, smartphones are increasingly attractive targets.

Security encryption on the devices accessing and using mobile applications is of concern, as consumers’ personal information can be obtained directly from the device.\footnote{Asher Moses, ‘iPhone encryption proven to be “useless”’, The Sydney Morning Herald, 27 July 2009, www.smh.com.au/digital-life/mobiles/iphone-encryption-proven-to-be-useless-20090727-dyfv.html.} So device security is an important consideration in the overall protection of personal information within the mobile applications market. Consumers may be unaware of or uninformed about needing to protect personal information on their devices.

At the app store or platform level, the level of security of personal information is being addressed, as shown in the above overview of the app stores’ approach. When information is collected at this level, it may be shared with consumer consent, either implied (purchase of a mobile application) or explicit (consumer is asked to permit sharing), and personal information encrypted. Consumer awareness of what type of information is collected and the manner in which it is used may need to be addressed in the future. As the central agency in the consumer relationship, app stores may need to take a more active role in ensuring that consumers are informed about their personal information being shared through the mobile applications market.
The platforms have varying levels of innate security and privacy that relate to the nature of the products themselves. For example, whether the operating system is based on open source software or designed for enterprise security changes the base level of security the device is able to provide. Open source software is able to be more easily compromised. The degree to which consumers are informed about the different levels of security afforded by the various platforms is also problematic.

The area of most concern is security of personal information at the mobile application level. TaintDroid, a mobile application created by programmers at Pennsylvania State University, recently demonstrated that across 30 popular mobile applications tested, 50 per cent were stripping geographic location data from users and sending it to remote ad servers without the user’s knowledge or permission.\(^{42}\) Also of concern is that the team identified 20 mobile applications that were misusing personal data in 68 clearly identified infringements of US privacy legislation.\(^{43}\) In most of these cases, the user would have been unaware of this activity. While this is a small study, it does highlight some of the problems with security of personal information at the mobile application level.

Within the mobile applications market, there are opt-in and opt-out models of information collection for advertising, and all of the platforms have privacy policies and guidelines in place. However, consumer awareness of these activities and their implications is questionable. There are obvious individual and commercial benefits to behavioural advertising (advertising based on personal preference information); however, these need to be balanced against users’ rights to privacy and security.

In an effort to combat concerns about the collection of personal information, such as the mining of personal information by mobile applications for marketing purposes, the US Federal Trade Commission (FTC) has proposed the implementation of a ‘Do not track’ register. Similar to current ‘Do not call’ registers here and overseas, the register would address issues of privacy in the collection of personal information. Registered individuals would be exempt from the behaviour tracking analytical software used increasingly in advertising online and in the mobile applications market.\(^{44}\) The implementation of the proposed register across a globalised market is likely to create numerous problems, with multiple jurisdictions, international regulations and multiple entities involved.

At the mobile applications level, advertising can be a lucrative revenue stream for app developers—it is one of the main business models operating in this market. Developers are unlikely to support the implementation of schemes that restrict their access to this revenue. The nature of the participants in the mobile applications market may also be an issue—with an app developer able to be anyone from a multinational corporation to a 16-year-old student, making market participants aware of and compliant with the proposed legislation is likely to be another barrier to successful implementation.

Augmented reality and location-based services (LBS), which are already present in the mobile applications market, also pose challenges for privacy as the distinction between personal and public information is blurred. For example, GPS-enabled mobile applications such as Run Keeper log when someone leaves their home and where they run to within a few metres, while Foursquare is one of a new breed of LBS that combines social networking site features with location-based services. Foursquare enables users to track each other’s movements, and report on products and locations.

---


\(^{43}\) Ibid.

Another example is the Commonwealth Bank Property Guide iPhone app, which uses augmented reality technology to allow users to view property details, including past sales history, current property listings and recent sales. Users simply view the property through the phone's camera and the information is mapped onto the real-world view. The mobile application provides information on over 95 per cent of residential properties in Australia, and this includes both properties currently for sale and those previously advertised online.\footnote{www.commbank.com.au/about-us/news/media-releases/2010/iphone-property-app/default.aspx, viewed 1 December 2010.}

Mobile applications using augmented reality and LBS have obvious commercial benefits for businesses seeking innovative marketing strategies, while for users of social networking sites they offer a natural extension of their online interaction. However, much like social networking sites, the use of these technologies has potential pitfalls in terms of the exposure of further personal information. Education of both consumers and market participants about their current rights and responsibilities would seem to be desirable in the mobile applications market.

With future developments in technology and greater community adoption of smartphones and other devices that use mobile applications, privacy and the distinction between personal and public information will continue to be debated.

**Data portability**

The mobile applications market is currently led by app store models from device manufacturers and operating system providers, in terms of the size of the associated app stores and the revenue generated from mobile application sales.\footnote{Erick Schonfeld, 'Despite 861.5 Percent Growth, Android Market Revenues Remain Puny', TechCrunch, 21 February 2011, http://techcrunch.com/2011/02/21/861-5-percent-growth-android-puny/, viewed 28 March 2011.} These stores have the largest number of mobile applications and large developer communities. Consumers are attracted by the wider variety and diversity of products offered in these app stores due to their size, and app developers are attracted to a large marketplace with many active participants. These app platform providers offer a closed proprietary market for consumer mobile applications, in that the app products sold on the platform can only be used by devices that run the proprietary OS.

The initial purchase of an individual mobile application is relatively inexpensive. Over time, consumers may invest more value in it through personal information, such as photos, contact lists, calendars, diaries and personally designed news feeds. In addition, purchase of multiple mobile applications will increase a consumer’s investment in a platform. In the long term, this investment may increase switching costs between platforms, reducing the consumer’s ability to access a wide variety of services.

This issue of data portability is similar to that of users of social networking sites who develop material on the networking site, and essentially reflects the ongoing debate in the digital environment about personal property rights. Some social networking sites, like the platforms within the app market, operate closed systems that prevent users from transferring information from one site to another. This in part reflects the value of user’s information to these sites, in attracting other users and paid commercial interests through the subsequent increase in traffic.

Data portability ‘enables a borderless experience, where people can move easily between network services, reusing data they provide while controlling their privacy and...”
respecting the privacy of others.' Preventing data portability raises the issue of who owns the information. While as yet there are no widely accepted protocols, groups such as the independent Data Portability Project have been advocating for common guidelines. However, there are also associated security and privacy issues when information can be transferred and shared easily.

Essentially the issue remains one of rights—who has the right to control access to and the dissemination of an individual's information and data? This question is reflective of many of the issues in the digital environment about the rights and responsibilities of the citizen, and is one for wider society to debate.

Data use

App designers create and sell their products in markets that are independent of the networks on which they are used. Current telecommunications regulation focuses regulatory measures on network carriers, but they are not currently recipients of the revenue from the sale of mobile applications (see Figure 9).

---

An effect of the use of individual mobile applications is the consumption of data. A consumer’s mobile application-related data is subject to a separate service contract between them and their carriage service provider. Data used in accessing mobile applications may form part of the overall service contract that consumers have, such as voice, text, and data packages for smartphones using a digital mobile network. Alternatively, it may be through a separate service contract they have contracted for with a broadband data provider.

Unlike other digital purchases that have one-off data costs, such as music and movies, mobile applications may incur additional ongoing and updating costs. There is a potential lack of consumer transparency about the amount of data individual mobile applications can consume.

---

Data consumption by individual mobile applications can be incurred in three ways:
1. Initial download—installation uses data to download.
2. Ongoing—data is used in ongoing game play or other functionality.
3. Updating—data is used to download updated versions or fix bugs.
applications use\textsuperscript{50}, in particular where the billing arrangements used by service providers for smartphones, bundle data, voice and SMS services. This could possibly result in consumers experiencing bill shock through unintentionally excessive data use via mobile applications.

In its 2009–10 annual report, the TIO noted that there was an increase of financial over-commitment for mobile services and problems with calculation and/or imposition of charges. The Ombudsman stated in the TIO press release accompanying the annual report that: ‘Part of the reason for this is so-called “bill shock”, where consumers receiving [sic] unexpectedly high bills, often after large downloads to mobile devices such as smartphones …\textsuperscript{51}

However, network carriers currently provide data-monitoring services similar to those used for their other broadband products.\textsuperscript{52} The provision of a warning to consumers at 80 per cent of data consumption limits and an opt-out cut-off system are mandated consumer protections in the European Union (EU). The US Federal Communications Commission (FCC) has released a public consultation paper on how to protect consumers from bill shock, which includes a discussion about whether it should implement similar protections to those used in the EU.\textsuperscript{53} The provision of warnings and cut-off mechanism are a simple and effective solution to help limit consumer expenditure, although it does not directly address the underlying information asymmetry issue.

\textsuperscript{50} RIM, via its Blackberry Mobile applications world vendor guidelines, does require that mobile applications must alert users to any potential data use.
\textsuperscript{52} Data is provided in a lump sum or cap and consumers are shown an approximation of their current level of use. The majority of carriers also send consumers notices when they have reached a predetermined level (for example, 80 per cent) of their set allowance.
\textsuperscript{53} www.fcc.gov/cgb/billshock/
Conclusion

Within the ACMA, the term ‘convergence’ is used to refer to the merging of the previously distinct platforms by which information is communicated. Broadly, the historical distinctions between radiocommunications, telecommunications, broadcasting and the internet are blurring. In the past, separate and distinct industries supplied content and services that were accessed by separate specific devices. Our present regulatory system is based on this pre-convergent technological format, meaning that emerging technologies such as mobile applications can strain some elements of the regulatory framework.

Changes in communications and media technology are outpacing what was thought possible just five years ago, let alone what was required from legislative frameworks over ten years ago. This should not be seen as a criticism of the legislation—the very nature of convergence is that it often leads to unexpected developments, sometimes very rapidly. The mobile applications market is covered by a framework of communications and media legislation, most of which was enacted before the release of the first smartphone or the concept of an app store became a commercial reality. While the legislation is technology-neutral in concept, the implications of the technological advances in the mobile applications market were not necessarily envisioned when the legislation was written.

The mobile applications market provides a current illustration of converged markets in practice and the pressures on the relevant current regulatory mechanisms. Convergence in this market is characterised by:

> multiple legislative schemes
> multiple jurisdictions
> multiple technologies
> converged markets
> multi-player supply chains.

All of these characteristics can complicate the determination and operation of appropriate regulation.

The ACMA faces a range of such challenges from emerging technology and business trends that are clashing with legacy legislation, controls and expectations. Similar to the mobile premium services market, the mobile applications market is characterised by extended value chains and multiple players, which adds complexity to the service-related aspects of the market. This complexity has the potential to create problems with the delivery of policy outcomes like privacy and protecting children via mechanisms such as content classification and access restrictions. There are also potential issues with consumers’ ability to measure their data use via apps (to the extent that this impacts on charging), the clarity of charging arrangements for data and potential for consumer bill shock.

The ACMA’s attitude to these emerging technologies is a graduated use of regulatory measures using the minimum power or intervention necessary to achieve the desired result, which is compliance on a sustained base, usually from having encouraged behavioural change. Non-regulatory mechanisms such as education (for both consumers and market participants) may provide effective and timely methods of intervention in the mobile applications market.

However, the ACMA has also determined that where the behaviour of market participants or the shape of market structures is incompatible with the ‘softer’ options
of co-regulatory control, the regulator should and must take ‘harder’ regulatory actions involving directions, enforcement and prosecution as appropriate and required.

Rapidly escalating consumer detriment in the mobile premium content space in Australia was a pointer to issues such as changing content delivery methods and business models, mobility and extended value-chains. In response to this particular environment, the ACMA determined that sometimes it can be better to respond rapidly and firmly to developments that threaten consumer welfare, particularly where market conditions and product characteristics are not optimal for a co-regulatory approach. These can include poor incentives for industry to participate, many small players, and/or complex products, especially from consumers’ perspective).

In an innovative market such as mobile applications, there is an evident need for regulators to continuously monitor market operations and assess the potential for consumer detriment and regulatory concerns. This regulatory approach should balance the objectives of consumer protections and safeguards with the need to allow innovation in a competitive and efficient market.

Glossary

App developers—creators of apps. May be either independent or work for an
organisation. Operating system, device manufacturers and telecommunications
network providers all produce apps, as well as other commercial, government, non-
commercial and non-government organisations.

Augmented reality—in the app ecosystem, this generally refers to a display in which
simulated images, graphics or information is superimposed on a view of the
surrounding environment.

Bill shock—as yet there is no standard definition; however, the term is generally
accepted within the telecommunications industry as referring to the negative reaction
consumers experience if their mobile phone bill has unexpected charges.

Convergence—primarily framed to refer to the merging of the previously distinct
platforms by which information is communicated. The historical distinctions between
radiocommunications, telecommunications, broadcasting and the internet have been
blurred.55

Market—a place where buyers and sellers come together to exchange goods,
services and information. Market participants consist of all the buyers and sellers of a
good who influence its price. There are two roles in markets—buyers and sellers. The
market facilitates trade and enables the distribution and allocation of resources in a
society. Competition is essential in markets and separates market from trade. When
forces within a market distort competition, the allocation of resources in the market is
inefficient. Regulatory intervention may be warranted in a market where allocation of
resources is inefficient due to market failure. The other reason for government
regulatory intervention in a market may be to ensure the provision of social policy
goods to consumers in that market.

Location-based service (LBS)—an app that requires knowledge about where the
device using it is located. Information about where the user is located may also be
visible to other users of the app. Examples include Google Maps and Foursquare,
which allows users to see the location of nearby friends.

Operating system software (OS)—the system software responsible for the direct
control and management of hardware and basic system operations. Additionally, it
provides a foundation upon which to run application software such as word processing
programs and web browsers.56

Platforms—distribution gateways aggregating product from third-party developers (as
well as their own) and making it available for consumers. Platforms are generally
operating system-specific (selling only apps for use with devices that have a particular
operating system) or sell apps for multiple kinds of operating systems. At present, the
platforms generating the most sales are those that are operating system-centric.
Platforms may also be responsible for the delivery of other products and usually
represent a model involving an operating system, device and online presence.

Smartphones—there is no industry-standard definition of a smartphone. However,
most commentators agree that a smartphone is a mobile phone offering advanced
capabilities, often with PC-like functionality (PC–mobile–handset convergence).

55 Australian Communications and Media Authority, Corporate Plan 2010–13, p. 9,
56 www.brandywinecomm.com/resources/glossary
Because smartphones are essentially mobile computers, they can serve as delivery platforms for third-party apps.

**Software developer kits (SDK)**—typically a set of development tools; in the case of apps, for the creation of applications for operating system platforms.

**Third-party developers**—creators of app programs who do not work directly for the app store, device manufacturer or network service provider.

**Walled garden**—a term used in the telecommunications and media industries to refer to carrier/service provider control over applications and content/media available on mobile devices.