AUSTRALIA

Mobile Apps and the Risks to Australian Consumers

Confidential and Proprietary

January 2013

CONTENTS

EXECUTIVE SUMMARY

WMC Global welcomes the opportunity to contribute to the Commonwealth Consumer Affairs Advisory Council's (CCAAC) call for submissions regarding "app purchases by Australian consumers on mobile and handheld devices."

For the last six years, WMC Global has led the world in mobile compliance services and analysis. Our contributions include the following:

- Eighty-four percent drop in Australian consumer Telecommunications Industry Ombudsman complaints about mobile premium services (MPS) since 2010;
- End-to-end compliance management of the U.S. premium SMS marketplace;
- Launch and management of the cross-carrier premium SMS shortcode registry in Latin America;
- Launch and management of the direct carrier billing environment in the United Kingdom for O2;
- Ubiquitous support for premium SMS, direct carrier billing, and app store experience for AT&T Mobility; and
- Mobile app storefront risk assessments for CTIA-The Wireless Association®, O2, and T-Mobile USA.

We base the insights presented in this report on our global experience in the telecommunications and mobile app environments as well as on our specific knowledge of the app market in Australia. Our submission makes several observations regarding challenges in the mobile app environment, including in areas directly relevant to the CCAAC inquiry, such as 1) customer experience, 2) information disclosure, and 3) customer protection.

Many of the issues Australian consumers face in the app market mirror issues that WMC Global has resolved in cooperation with the Australian carriers, the Communications Alliance, and the Australian Communications and Media Authority in the Australian MPS market. We are pleased to offer our assistance to the CCAAC to discuss the merits of further industry self-regulation efforts in addition to evaluation of the most relevant pressure points for best practices standards development and the potential regulation of critical areas such as the impact of in-app purchases on minors.

Our submission to the CCAAC aims to identify several methods for improving the experience of Australian consumers when purchasing and using mobile apps. We look forward to the opportunity to discuss this report with the CCAAC as we seek to further safeguard Australian consumers.

Katya Yatsenko
General Manager
WMC Global Pty Ltd
Suite 7.05
100 Walker Street
North Sydney, NSW 2060

katya.yatsenko@wmcglobal.com
+61 2 9922 5569

INTRODUCTION

This report summarises current consumer experiences in the Australian app market, specifically experiences with Google Play and Apple's App Store. We believe an industry code of conduct, self-regulation, and compliance monitoring and enforcement are the only effective long-term means to mitigate detrimental effects on the Australian consumer.

An overview of WMC Global, Section I provides context to our submission. Section II outlines the inherent issues within the app store environment, such as deceptive customer experiences, inadequate or inconsistent information disclosure, and lack of consumer protections. Section III presents our recommendations to the Commonwealth Consumer Affairs Advisory Council (CCAAC).

SECTION I

ABOUT WMC GLOBAL

This section provides an overview of our company's worldwide presence.

1.1 WMC Global in the United States and the United Kingdom

Since 2006, WMC Global has provided fraud, security, and compliance monitoring, enforcement, technology development, research and reporting, and technical writing to the carriers as well as to regulatory and advocacy organisations in both the United States and the United Kingdom, including CTIA-The Wireless Association™ (the CTIA) and PhonepayPlus.

Coordinating with industry bodies and their associated carrier members, WMC Global has developed audit standards for mobile commerce in each marketplace and has helped bring unity to a fragmented approach to compliance in the marketplace. In the United States, for example, WMC Global authored the *CTIA Monitoring Compliance Handbook*, a set of industry-wide premium SMS audit standards that combine cross-carrier-developed rules, along with federal and state requirements, into a single user-friendly document that anyone can follow. Our industry expertise and in-market monitoring help decrease the noncompliance rate significantly for both premium and standard rate SMS campaigns under the CTIA compliance assurance program.

In addition, WMC Global has partnered with the CTIA to provide a technology platform and sales expertise to develop the first premium SMS common shortcode registry for Central America and South America. This Latin American registry is designed to unite all carriers in the region under a single registry process, allowing businesses to on-board and market unique shortcode campaigns more easily across multiple countries.

PhonepayPlus, the U.K. Office of Communication's designee to regulate the content, promotion, and overall operation of all premium rate services (PRS) through its Code of Practice, has turned to WMC Global, as well, for industry expertise. We have consulted with PhonepayPlus to develop customer experience audit standards that we employ to perform ongoing PRS monitoring and data analysis. Moreover, we deliver to this client thematic reports (e.g., *Malvertising Investigation Report*) and regular "state-of-the-market" reports detailing the latest trends in PRS compliance across the U.K. marketplace.

Finally, WMC Global works routinely with U.K. carriers, developing customer experience audit standards, providing in-market monitoring, and delivering PRS market compliance reports and thematic reports (e.g., *PSMS App Investigation Report*, *Google Play Risk Assessment Report*). In direct response to PRS programmes that demonstrate persistent noncompliance, we developed our REHAB (Rehabilitation Environment for Habitual Anomalous Behaviour) product, an enforcement strategy that has proven extremely successful in dealing with determined offenders.

O2 also engaged WMC Global to develop audit standards for and to monitor Payforit transactions on its network. Simultaneously a payment mechanism and a billing mechanism, Payforit allows consumers to purchase products and services via their mobile phone or computer while enabling merchants to charge the cost for those goods to the consumers' mobile account or to their prepaid balance. U.K. carriers O2, Orange, Three, T-Mobile, and Vodafone developed and launched Payforit with the aim of providing a safe micropayment option for one-off and subscription goods. In further support of the Payforit initiative, WMC Global wrote the *Payforit Handbook*, a substantial step-by-step user guide for all participants (i.e., accredited payment intermediaries [API], merchants, and consumers).

And, WMC Global built and operates O2's Premium Rate Services Compliance System (PRSCS), an online provisioning and workflow management portal that allows APIs to manage their Payforit accreditation status and merchant services. Trusted APIs that qualify are permitted self-certification status in the portal to approve and launch services with less carrier oversight, while we continue to monitor the PRS market and Payforit transactions at large.

1.2 WMC Global in Australia

In 2009, WMC Global entered the Australian market after the Australian Communications and Media Authority (ACMA) had introduced the Mobile Premium Services Industry Code (MPS Industry Code). Working with the carriers, the aggregators, and the content providers and employing ACMA guidelines, WMC Global continues to provide in-market monitoring and enforcement that level the playing field for all participants. Our efforts ensure third-party providers' compliance on carriers' networks; protect carriers' customers, brand, and business; and promote ethical marketing behaviour throughout the industry.

With the customer safeguards put in place by the MPS Industry Code, WMC Global helps ensure that content providers and service providers display basic disclosures regarding pricing, recurring nature of subscription services, unsubscribe information, data fees, and helpline availability and operate functioning sources of customer care. Our in-market monitoring and enforcement efforts have improved advertising, messaging, and helpline standards and have increased consumer confidence in Australia. Simultaneously, consumer complaints to the Telecommunications Industry Ombudsman (TIO) have decreased substantially. In 2008, the TIO received an average 7,000 consumer complaints per quarter. By April 2012, overall complaints to the TIO had decreased 84 percent, indicating the impact of WMC Global's compliance monitoring and enforcement activities.

SECTION II

CONSUMER APP EXPERIENCE OVERVIEW

Based on our global experience and expertise in app market analysis and app certification, this report outlines some of our observations from the two most popular app outlets in Australia: Google Play and Apple's App Store, each offering more than 700,000 apps for download.

As we identify below, inherent user experience issues exist within the app store environment. We believe the only effective way to minimise risk associated with these issues and to protect consumers as has been achieved with MPS is to create an industry-wide best practices code of conduct and to implement self-regulation, compliance monitoring, and enforcement.

2.1 Downloaded App - User Experience Issues

WMC Global's research has documented user experiences and analysed how these experiences impact consumers, developers, app stores, and carriers. For this report, we review the impact of in-app purchases, advertising, advertising networks, contact details, sources of assistance, and refund policies specifically. We conclude that the current user experience, in many ways, fails to safeguard consumers fully within the app environment.

2.1.1 In-App Purchase Paths Targeting Minors

Some apps prompt users frequently to make in-app purchases. Given that the audience of these apps is mixed, this practice could cause concern for parents and guardians of underage users. Many apps that target children specifically are financed primarily through multiple in-app microtransactions. Additionally, we have seen in-app purchase price points as high as AU $51.99, indicating the level of risk of a mistaken or unauthorised in-app purchase. This specific instance was encountered in My Little Pony: Friendship if Magic ™, a game that targets children directly.

2.1.2 Intrusive Advertising and Advertising Network Use

Although legitimate channels exist for developers to monetise their apps using advertisements, the connection between unregulated advertising networks and app developers is an area that we at WMC Global believe is significantly problematic for consumers. This mutually beneficial relationship between advertising networks and developers can prove detrimental to consumers, who encounter vague requests for user consent, unclear or missing information about the unsubscribe mechanism, intrusive advertising offers, untraceable push notification ads, and high incidences of accidental click-throughs. Exhibit 1 depicts a push notification. The image on the far left shows the notification, and the other two images show the Website to which users are taken by clicking on the notification, a premium SMS advertisement.

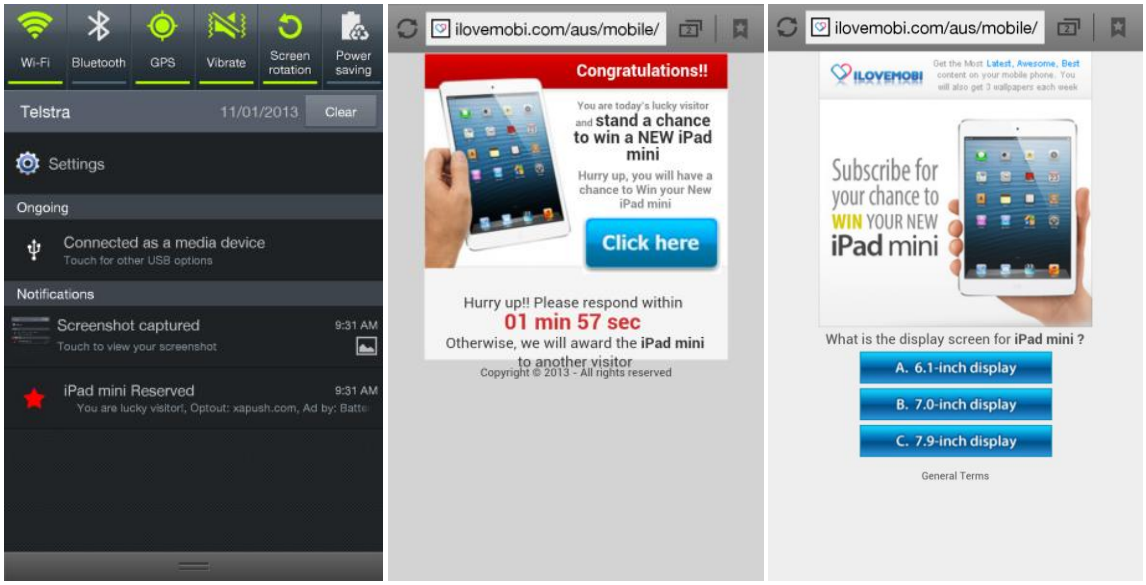

Exhibit 1: Push Advertisement from *Battery Booster* Android App

After downloading Battery Booster, we received a push advertisement that led us, via an affiliate marketer, to a Website for a competition that fails to indicate a charge is imposed for participation.

2.1.3 Lack of Accountability for Customer Support and Refunds

Google Play and Apple's App Store prefer to direct consumers to app developers as the first point-of-contact for all technical and support issues. Many apps lack sufficient, clearly labeled contact details and sources of assistance, such as a Website URL. Even when email addresses, company names, Website URLs, and other such details are provided, often they are vague, difficult to navigate, or untraceable.

App users who experience technical issues, discover faults, change their mind, or no longer require the item purchased usually seek a refund for the app or in-app purchase. But, in Google Play, for example, users are given only 15 minutes to request that refund. Moreover, refund policies vary among app stores, and users sometimes are not entitled to refunds in these situations. Neither Google Play nor Apple's App Store provides refunds for in-app purchases and subscriptions: the onus is on developers to deal with these issues.

Difficulties in actually reaching the developers hamper app users in their efforts to secure refunds. To exacerbate matters, no requirement exists for developers to honour such refund requests. The net result most likely is a call to the carrier customer care centre, to the TIO, or to both.

2.1.4 Malware

Mobile malware capable of tracking personal data that consumers often store (e.g., credit card number, bank account number) on their smartphones has become a growing concern. Recent estimates indicate that Android devices belonging to more than 1 million users in China are infected with trojans that turn the phones into a botnet, creating security threats such as remote hijacks and unauthorised purchases. Nearly 11,000 apps are infected with this one virus. Although Google offers a malware scanner, tests demonstrate that the scanner is only 15 percent effective against *known* malware.

Lacking an approval process, the Android ecosystem is particularly susceptible. And, in fact, despite Apple's reputation for imperviousness to attack, a mobile trojan made its way into iOS in 2012, secretly sending the contents of the phone's address book to spammers.

Some types of malicious apps attempt to impose additional fees using the premium SMS billing mechanism. As part of WMC Global efforts to enforce compliance with premium SMS audit standards, we identified and helped carrier clients shut down dozens of apps that initiated unauthorised premium SMS transactions.

2.2 App Browsing - Inadequate Information Disclosure by App Developers

Australian companies are generally well regulated in how they advertise and present information about their products. We encounter many examples where developers disclose information inadequately before the purchase. For example, frequently missing or unclear is information about associated pricing, data fees, and the nature of the app being purchased.

2.2.1 Lack of In-App Payment Disclosures

Google Play and Apple's App Store display the price of an app purchase clearly and prominently, yet few such disclosures are available for in-app purchases within the app store, where they are strictly voluntary. This omission is particularly concerning for parents who might purchase an app for an underage user without realising the potential for incurring additional charges.

2.2.2 Confusing or Misleading Product Claims

One of the main means by which inadequate disclosures exist is in intentional obfuscation regarding an app's *actual* functionality. Some developers advertise their apps in a potentially misleading way, claiming the apps perform functions that they simply cannot. Placebo apps, for example, fail to perform as advertised, existing merely to drive traffic to advertisements. Google Play describes placebo app *Battery Booster* (2x Battery): "Boost your battery life by 15-30% with just the press of a button! This battery booster/saver app will run in the background and automatically disable battery-sucking features of your phone when you aren't using them."[1] However, only consumers who expand the description, scrolling to the bottom, see the following disclaimer: "This app is a pure placebo. It does not actually boost your battery life. It is a prank app which you can use to trick your friends. Have fun!"[2]

2.2.3 No Data Use Disclosures

Users have a reasonable expectation that app developers and app stores disclose associated fees, other charges, and additional relevant information about an app, thereby enabling informed choices. However, most developers and app stores fail to disclose that using many apps requires data and that carriers might charge for this data use. Additionally, few descriptions disclose that data, an Internet connection, or a Wi-Fi connection is required to download the app, use the app, or both.

Although consumers are presented with a specific download size, we find no correlation between initial download size, or even the type of app, and the amount of data the app consumes when in use.

[1] Google. *Batter Booster (2x Battery),* https://play.google.com/store/apps/details?id=com.bb.battery.saver, accessed 4 January 2013

[2] Google. *Batter Booster (2x Battery),* https://play.google.com/store/apps/details?id=com.bb.battery.saver, accessed 4 January 2013

For example, My Little Pony: Friendship Is Magic™, a game geared specifically to children, typically consumes more than 17 times as much data compared with YouTube, a streaming video app.

2.3 Current App Consumer Protection Issues

Customer protection is an essential facet of any industry, including the app subset of the mobile data industry. But, with no specific code of conduct or regulation under which to operate, apps have become the focus of much scrutiny. We at WMC Global believe that privacy, third-party data collection, permissions, content classification, and the inadequacy of default settings are areas that must be addressed to ensure consumer protection.

2.3.1 Parental Control Implementation Issues

Each app store provides options for parents and other concerned users to limit the type of app content available to a specific account. Apple offers more comprehensive options than does Google in relation to such controls; however, both Google Play and Apple's App Store provide inadequate information on activating these controls when creating an account.

Apple includes Parental Controls in its iTunes software and Restrictions on its devices to allow users to control app content ratings. The default setting makes available all content and ratings. Users can "lock" the settings also to ensure further changes are impossible. To unlock the settings, an administrator password is required.

In Google Play, under Settings, users can employ content filtering to restrict access to apps containing inappropriate content. Similar to iTunes functionality, users can establish a PIN to ensure these settings cannot be altered. Even when content filtering is applied, apps containing objectionable content have found their way into Google Play, so underage users still are potentially at risk of exposure to this content.

2.3.2 Privacy and Permissions Policy Inconsistency

One of the primary concerns for app users, particularly for parents, remains privacy. Privacy relates to user data that apps collect, where this data is saved, whether this data is distributed, and why this data is collected in the first place. Increasingly, users are concerned about apps collecting personal data (e.g., contact phone numbers, account details, SMS messages) from their devices and transferring it to advertisers and other third parties. Developers must establish for their apps a clear privacy policy that details the data types being collected and how and where this data will be used. Exhibit 2 displays a poorly disclosed privacy statement.

Exhibit 2: *Grand Theft Auto III* Android App

This screenshot captures the user experience on opening Grand Theft Auto III. The screen scrolls automatically through disclosures relating to privacy, in-app purchases, and other issues, displaying the information across two screens and pausing for five seconds on each screen. The screen size of the test device and the tiny point size of the font render this information almost impossible to read.

Closely associated with privacy, permissions relate to app features that access system functions and data in a remote location; users must actively permit these features to operate on their device. Permissions are a controversial issue because many help access personal data on devices as well as help collect and store this data.

After downloading an app, Apple users can choose to prevent its accessing specific data types (e.g., their contacts, their location). Google users are shown *all* relevant permissions and must agree to them to download apps; they cannot choose to prohibit specific permissions. Consequently, app permissions in Google Play are a particularly contentious issue. Although Google automatically includes a list of all permissions an app requires, many users fail to review this list before installing the app, which on the extreme end can lead to risks such as trojans, malware, and MPS scams. Even when users do review all the app's permissions, they might fail to understand some or all. In our experience, many apps include unnecessary permissions, potentially to serve advertisements and collect personal data.

2.3.3 Content Classification and Age Verification Weaknesses

Currently, Australia lacks a clear industry or legal framework addressing apps specifically, causing confusion over whether apps should be treated as gaming or online services. Both Google Play and Apple's App Store have their own classification schemes for rating app content, which do not necessarily correlate with Australia's National Classification Code. During the app submission process, Apple assigns a rating based on set criteria. Android developers determine their own ratings, potentially leading to incorrectly rated apps.

Current age verification measures fail to prevent all underage accountholders from downloading age-restricted apps, such as the one displayed in Exhibit 3.

Exhibit 3: *Blendr* Android App

This screenshot captures a message we received via Blendr. Despite the app's stating that users must be older than age 18, we signed in via an underage Facebook account. The content of the messages we received from other users raises concerns about Google Play's insufficient content rating system and the threat to minors.

The only way to prohibit this access is through content filtering within the app stores and within device settings. Apple provides clear instructions in the iTunes Store; however, even when underage users are unable to download apps intended for mature users, they still can view all of the screenshots and the description, exposing them to potentially inappropriate content. In general, apps fail to provide sufficient information about the assignment of a particular content rating, which means parents and other users are unable to make informed choices about whether an app is suitable for their children or themselves.

2.3.4 No Protection under Existing Australian Laws and Regulation

Currently, no specific universal law, regulation, or code covers the app industry within Australia or overseas. Apps appear to fall under the National Australian Consumer Law (ACL) as well as under several acts, including the National Consumer Credit Protection Act 2009 (Cth), the Electronic Transactions Act 1999 (Cth), the Privacy Act 1988 (Cth), the Minors (Property and Contracts) Act 1970 (Cth), the Minors (Property and Contracts) Act 1970 (NSW), the Goods Act 1958 (Vic), and perhaps even the Telecommunications Act 1997 (Cth). Additionally, the Australian Guidelines for Electronic Commerce provide a relevant framework within which developers and app stores can operate. However, none of these acts was written with the express intention of protecting consumers purchasing and using apps. As a result, developers and app stores lack a definitive set of rules or guidelines within which to operate, and ultimately no standard exists for safeguarding users.

SECTION III

CONCLUSION AND RECOMMENDATIONS

Consumers are experiencing an ever-changing technological environment, marked by the explosion in smartphone popularity and the availability and uptake of apps and other new media products. Great potential risk comes for both companies operating within this emerging environment and consumers interacting with these companies and their products.

Based on our global compliance monitoring experience and our knowledge of international app markets, we believe material concerns surround the sale and distribution of apps to Australian consumers. Specifically, concerns abound regarding the inadequacy of information disclosed in app stores, with app developers appearing unable or unwilling to provide adequate disclosures when advertising apps.

Perhaps of greatest concern are issues that affect underage users directly, such as the following:

- Aggressive in-app purchase marketing (e.g., failure to limit transactions, misleading purchase paths, no pre-purchase disclosure);
- No disclosures regarding app data use;
- Limited protections from currently available payment and parental control settings; and
- Lack of regulation surrounding app classification and age verification.

To combat these issues and others, WMC Global has laid out a detailed plan for implementing several regulatory initiatives, including the following:

- Comprehensive disclosure policy covering data use, services offered, and pricing;
- Framework for developer accountability surrounding customer support and refunds; and
- Tighter user control of in-app purchases and age-restricted content.

We have implemented similar initiatives with MPS in Australia, and we are pleased to be able to offer our services to the CCAAC in the app store ecosystem. As a next step, we suggest a meeting between the CCAAC and WMC Global to discuss the most relevant pressure points for potential standards development and possible regulatory oversight in this growing market area.

Katya Yatsenko
General Manager
WMC Global Pty Ltd
Suite 7.05
100 Walker Street
North Sydney, NSW 2060

katya.yatsenko@wmcglobal.com
+61 2 9922 5569