Centre for Internet Safety

JANUARY 2013

CCAAC - enquiry into App purchases

SUBMISSION BY THE CENTRE FOR INTERNET SAFETY

Key Recommendations

- App developers avoid traditional legal language in their terms and conditions, and should instead use “plain English” clear terminology to precisely explain what the company will and will not do with a user’s contents and personally identifying information;
- Consumers should be able to turn off in-app advertising;
- Consumers should be encouraged to consider what they know about an app, who created it and what it does, before they download it;
- The organisations behind app stores and social network providers should be compelled to have an Australian presence for regulatory purposes;
- The ACCC should monitor app terms and conditions and publish a regular consolidated report;
- App stores and social networking sites should be required to have procedures for resolution of disputes between the app developer/owner/operator and consumers;
- The protection of mobile devices, the data they hold, their users, and the systems they interact should be enhanced by enabling device features such as file and network encryption, passcodes, and lost/stolen device locator capabilities;
- Where an app suffers a breach of personally identifying information, the app distributor should inform the relevant state, territory and Commonwealth privacy and consumer affairs agencies; and
- The Government should commission further research into how Australians use apps.

Introduction

The Internet traverses political, cultural and geographic boundaries within and between countries. It brings people and their views and behaviours closer together – and allows them to interact - in a speed and manner never seen before.

Internet access is now being conducted more and more via mobile devices, including smart phones and tablets. Such use grew in Australia by 21% between 2009 and 2010[1] with anecdotal evidence suggesting a much greater increase since then. Australia has the second highest penetration rate in the world for smartphones, at 37% of our population. Singapore is the highest at 62%.[2]

An "app" is a software program users download and access directly using their smart phone, tablet, and - increasingly - PCs and laptops. Apps offer the advantage of a customised user experience, with graphics and information presented in a manner designed for mobile and tablet devices.

For the purposes of this submission, the Centre will divide apps into two categories. One is the apps consumers download from app stores. These apps are often games, yet can also be product specific, ranging from maps through to accounting aids. The second category are social networking apps, including Facebook, Twitter and LinkedIn.

Apps are changing the mobile internet market. Rather than using traditional web search, users are spending more time going directly to an app that gives them the information they want. For example, mobile device users are spending 94

About the Authors

Alastair MacGibbon is an internationally-respected authority on cybercrime, including Internet fraud, consumer victimisation and a range of Internet security and safety issues. For almost 5 years Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. He was a Federal Agent with the Australian Federal Police for 15 years, his final assignment as the founding Director of the Australian High Tech CrimeCentre.

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achievedthe rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia's capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis

---

[1] http://www.acma.gov.au/WEB/STANDARD/pc=PC_410070

[2] http://blog.marginmedia.com.au/Our-Blog/bid/81865/Smartphone-Use-in-Australia-The-Advantage-for-Marketers

minutes per day using apps compared to 72 minutes on the web. Of these 94 minutes, 49% of this time is spent on games, 30% social networking and 6% on news.[3]

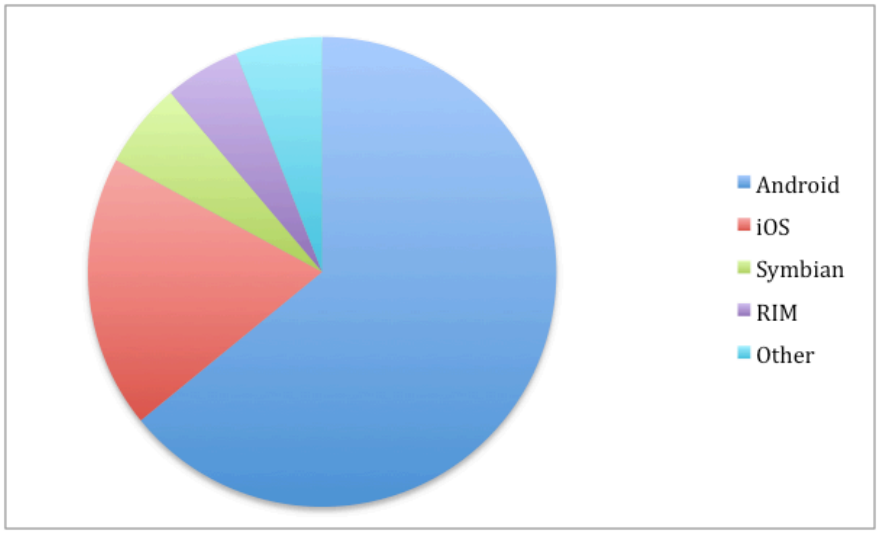
Downloading apps onto smart phones and tablet devices is now a significant business, with the two dominant players being Apple (Apple App Store) and Google (Google Play), who run app hosting sites.

While Apple makes money from selling its handsets, Google gives away its Android operating system to various device manufacturers in order to gain traction within mobile devices and, therefore, critical ubiquity to deliver ads.

There are now more mobile devices using the Android operating system (see figure below). While this logically means more people accessing Google Play to download such apps, there are roughly the same amount of apps for Apple as there are for Android.

Some apps are free, some are paid for, while others use a hybrid 'freemium' model with initial download free but added features paid for. The Android Market has 65-70% of all apps free compared to the Apple App Store which has 30% free.[4]

There are estimated to be over 43,000 Apple app developers against 10,000 Android developers.[5] This may be because every $1.00 generated on iOS by an app corresponds to $0.24 in revenue for the Android version.[6] The figure below [7] shows the dominant market share of the Android operating system in mobile handsets, however Apple has high brand loyalty with buyers often making numerous repeat purchases. Android with 2:1 market share over Apple makes its money from a variety of sources,



Worldwide Mobile Device Sales to End Users by Operating System in Q2 2012

[3] http://blog.flurry.com/bid/80241/Mobile-App-Usage-Further-Dominates-Web-Spurred-by-Facebook

[4] http://www.androidauthority.com/google-android-market-vs-apple-itunes-app-store-26281/

[5] http://www.androidauthority.com/google-play-vs-apple-app-store-2012-76566/

[6] http://appleinsider.com/articles/11/12/13/ios_apps_bring_in_300_more_revenue_than_android_counterparts.html

[7] http://www.gartner.com/it/page.jsp?id=2120015

including a push to improve and expand their content libraries, such as books and music; from Search conducted on apps; and from their growing advertising business on mobile.

As with internet search, advertising and cross-site promotion, advertising is where market dominance will be achieved. Where multiple app stores and social networks are available, it is important that all players have an equal chance to participate and succeed.

Enquiry question: *Do you usually read the terms and conditions, disclosures and other information to ensure you make an informed decision when downloading apps and making app and in-app purchases? If not, why?*

Do you consider the information provided prior to purchasing apps and when making in-app purchases clear and easy to understand? What other methods would you consider helpful in ensuring that there is adequate disclosure of information?

Downloading an app will always require the checking of a 'tick box' acknowledging the terms and conditions of use for the particular app. A terms and conditions agreement informs the user about the legal status of what they are using and may also include statements about copyright and disclaiming the operators of the app against any liability.

But before downloading an app, a user must first navigate the terms and conditions of the app store itself. The Apple App store (and its associated brands) terms and conditions statement is nearly 15,000 words long. For Google Play, the terms and conditions statement is nearly 7,000 words long. Facebook's Terms of Service is nearly 14,000 words. Smart phones have a small screen and reading voluminous information is both impractical and often impossible.

As off-putting as lengthy terms of service and condition statements are, they are a legal contract between the user and the respective app store. These can sometimes be more substantial than the average consumer might envisage.

App users are mostly unaware of the content within terms and condition statements, instead seeing the 'do you agree' statement which needs to be checked prior to download as an impediment to proceeding with the use of the chosen application.

The most popular apps are social networking sites. Such sites are applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles. User generated content is shared through personal profiles and can include any type of information, including photos, video, audio and blogs.

Publishing via many social networking apps, means users are usually forfeiting any sort of intellectual property rights they may have had to such content. Unbeknown to the majority of social networking app users, such as Facebook and Twitter, when agreeing to the terms of conditions (to which all members must agree) they are granting broad rights over their content. For example a photo posted on Twitter remains the intellectual property of the user but Twitter's terms give the company "a worldwide, non-exclusive, royalty-free license (with the right to sublicense)".[8]

There are many privacy concerns surrounding terms and condition statements. For example, when a user signs up with an app store and/

[8] http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html

or downloads an individual app, they may be asked for permission to let them access information certain on their device. This may include:

- The user's phone and email contacts
- Device call logs
- Device internet data
- Device calendar data
- Device location
- Device's unique IDs

A few apps may need to collect some or all of this data to enable the app to properly function. Others collect this data even though it is not related to the purpose of the app. This information could be used by the app developer, the app store, an advertiser, or an ad network. All of whom may share it with other companies. This information gathering and exchange is all about so-called 'monetisation', ie making money out of the consumer. In other words, the user or customer is no longer the consumer, but the product, and their personal information is very valuable. The problem is, the terms and conditions may allow this to occur, but the app user, whilst ticking the 'I agree' box has not given informed consent for this to occur.

App developers and app stores need to remove the traditional legal language contained within terms and condition statements, instead using clear terminology to precisely explain what the company will and will not do with its user generated content. Unfortunately for the majority of free apps, the clarity which would be provided in such 'plain english' statements would make it more obvious to device users the lengths to which many company's go in order to monetise the app.

While apps, such as games, are more likely to be downloaded from an official app store, there is a growing market, particularly for the Android platform of non-official apps. Apps that haven't been approved by an official app store are more likely to be invasive and may provide the application developers with access to a number of sensitive resources, for example the device's location, the user's contacts, unique device identifiers and even access to corporate information stored on the device. Privacy protection, control of corporate information and personal information management are of growing importance.[9]

By incorporating mobile ads into apps, developers can earn money from impressions and clicks. This option is especially beneficial for games and other apps which keep users attention over prolonged periods of time, such as social media sites. In some cases more money can be earned from advertising than if users were charged for the app. Implementation is a simple process whether its through Apple's iAd or Google's AdMob advertising platforms. Online advertising will continue to serve as the engine that drives not only app development but the broader online economy.

As mobile ad networks get smarter, location will enable context, interests, and a variety of other factors to be incorporated to help provide the right advertising at the right time. Obtaining location data is as easy as a permission request on both Android and iOS. Importantly, advertising companies pay up to four times more for geotagged advertising than advertising that is not location targeted. It is important for consumers to be able to turn off the advertising if they desire. This may be achieved by either providing an in-app purchase option to remove advertising or provide an upgrade to the full version of the app that does not include advertising.[10]

---

[9] Phair, N & MacGibbon, A. The Rise of Mobile Devices in the Enterprise – Security Risks & Considerations. Centre for Internet Safety.

[10] http://www.adobe.com/devnet/games/articles/maximizing-in-app-advertising.html

One of the strongest trends in IT is allowing - and in some cases encouraging - employees to bring their mobile devices to work (bring your own device - BYOD). Doing so has many ramifications, including security and privacy vulnerabilities introduced by free apps.

Smartphones, tablets, and the rise of BYOD in the workplace has put pressure on organisations to rethink their mobile and subsequently their enterprise security strategy. As more and more employees bring their own device into a corporate network, the confidentiality of the network could be at risk of compromise due to the various apps which may be running in parallel on the mobile device.

Enquiry question: *Are you aware of your rights when making purchases under the Australian Consumer Law the role of the ACCC and state and territory fair trading agencies?*

In the law, jurisdiction refers to a particular geographic area containing a defined legal authority. In Australia, Australian Consumer Law (ACL) covers the entirety of Australia, whilst each state and territory fair-trading organisation is limited by their respective jurisdictions. In effect, Australia has nine legal systems, the eight state and territory and one federal system. The ACL is a national law with multiple regulators. Each regulator is independent, has its own enabling legislation and exercises its powers and functions accordingly. This is confusing to consumers, often not knowing which entity to complain too. Added to this confusion is the borderless nature of e-commerce, meaning Australian consumers are downloading apps from all over the world.

Australia is a party to an extensive range of global treaties, which are formal instruments of international law. The ACCC, an independent statutory government authority, is Australia's peak consumer protection and competition agency. The ACCC enforces ACL within provisions of the Competition and Consumer Act 2010.

However, these provisions may not apply to overseas online transactions and, where they do apply, they are difficult to enforce in other jurisdictions.

Given these difficulties, cooperation with overseas regulators is required. There is limited jurisprudence arising from ACCC action against overseas entities. The organisations behind app stores, including Apple and Google, along with social network providers, particularly Facebook and LinkedIn should be compelled to have an Australian regulatory presence (not just a marketing and sales arm) to assist Australian consumer law regulatory agencies to educate and - where appropriate - prosecute those who infringe consumer law with respect to app download and use.

Further to a mandatory Australian regulatory presence, app stores and social networking sites should be required to have procedures for resolution of disputes between the app developer/owner/operator and consumers, as would be expected in offline commerce.

As the most appropriate agency, the ACCC should monitor app terms and conditions and publish a regular consolidated report which would help shed light on questionable industry practices, and assist consumers in making informed choices.

In the unfortunate circumstance where an app suffers a breach of personally identifying information - or when the app distributor becomes aware of a "rogue app" distributed via their app market- the app distributor should inform the relevant state, territory and Commonwealth privacy and consumer affairs agencies.

Lastly, given the dramatic rise of apps and the use of mobile devices, it is appropriate for the Government to commission further research into how Australians use apps.

Enquiry question: *What features of the app market, if any, concern you? What actions do you think could be taken to improve consumers' experiences when making app and in-app purchases?*

Apps found in the Apple App Store are more likely to be consumer-friendly and less invasive than those found in the Google Market because Apple spends more effort to check the functionality and coding of apps before it allows them to be visible to consumers, while the Google Market takes action to remove rogue apps after complaints.

We believe that Google Market, and other app marketplaces, should follow Apple's lead and more aggressively check apps against standard criteria of privacy and security features prior to apps being available for consumer download.