Privacy Implications of Behavioral Tracking in SmartPhone Applications

Michael Cueno

Abstract

This is to test a bilbio cite [1].

Contents

1 Introduction

Smartphone and tablet platforms in the US are currently caught in a privacy snafu with respect to behavioral tracking due to a lack of direct regulation [2] and very little consumer awareness [3]. As more users leave traditional consumption outlets such as TV, print and even web browser for mobile consumption [4], more research and development goes into procedures for tracking behaviors on these platforms.

We have seen a healthy debate for consumer protection in the realms of web browser privacy with the introduction of do not track mechanisms [5] and default settings which block third party tracking cookies [6]. The success of these developments can be argued, but the issues seem to be heading in the right direction. Unfortunately, it is less clear if the same thing can be said about the privacy issues surrounding the mobile ecosystem. This is increasing alarming as today′s smartphones have access to much more personal data sets than do your typical web browser, such as contact lists, text messages and location data.

The void of consumer awareness is begining to be filled with a growing number of publications that focus on current practices in mobile data collection.The Wall Street Journal, for example, has devoted an entire series to the issue [7]. As more

This paper illustrates the privacy implications that arise from the collection of personal, mobile data and suggests an approach to solving the issue from a policy standpoint.

2 Background

2.1 Evolution of Behavioral Tracking

The use of tracking software to model individual behaviors and actions on the internet came into its heyday with the proliferation of the third party cookie. This unique character string lives under the hood of your web browser and can be used for legitimate reasons such as keeping you logged into a session with your banks website, but the technology can also be used to collect data about you across many different sites. The use of cookies to perform behavioral tracking has exploded in recent years and shows no signs of slowing down [1]. (http://www.law.berkeley.edu/privacycensus.htm)

2.2 The migration to smart phones

As the use of mobile platforms continues to grow, we will continue to see the the same patterns in how media is consumed. A recent survey found that smartphone and tablet users watch, on average, 30 percent less TV and consume even less print media. (Source: ABI) This shift in consumption patterns along with the prospect of advertising to individuals instead of groups have pushed advertisers to invest heavily into mobile tracking technologies for the purposes of behavioral advertising.

2.3 Technical Discussion of Behavioral Tracking on SmartPhones

A majority of tracking on mobile platforms is done through the applications that the user downloads through the respective application vendors, most commonly, the Android Market and the App store from Apple. These applications often obtain access to permissioned data such as age, gender, location and the devices unique identifier. For smartphones running the Android OS, this is typically the International Mobile Equipment Identifier (IMEI) and for Apple products it is the UDID.

Application developers can access this identifier and send application usage statistics along with other permissioned data to advertising networks. When multiple applications send data to the same networks, all using the same identifier, a secret dossier can be established and maintained by that ad network for each device.

A troubling aspect to the use of these unique identifiers is that they cannot be cleared or reset on a device much like cookies on a web browser can. In fact, some countries have made it illegal to change, or spoof, these unique identifiers for anti-theft reasons. (SOURCE) This is in part, what makes smartphone tracking so appealing to advertisers. They are guaranteed a persistent way to identify an individual across multiple contexts.

At the moment the only technical protection that users have against this type tracking procedure is through permission awareness from the application vendors. The Android market for example, informs users what applications will access via a permissions screen prior to downloading the application. This is accomplished because Android makes developers request permission to all the data and resources that the application will require. The problem is that the average user is unaware of the security and privacy implications behind the permissions screen. Also, the permissions are commonly not read, and instead seen as a click through screen to installing an application. (SOURCE)

Thankfully, Apple has announced that it will be deprecating the use of the UDID in IOS6 due to the privacy concerns. MORE INFO NEEDED HERE

3 Analysis

4 prescription

5 Conclusion

References

[1] Thurm and Y. Kane. 'your apps are watching you'. *The Wall Street Journal*, Dec 2010. found at: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[2] 'privacy in the age of the smartphone'. *Privacy Rights Clearinghouse*, April 2013. found at: https://www.privacyrights.org/fs/fs2b-cellprivacy.htm#protections.

[3] Chris Jay Hoofnagle Jennifer M. Urban and Su Li. 'mobile phones and privacy'. *BCLT Research Paper*, July 2012.

[4] ABI Research. 'mobiles role in a consumers media day: Smartphones and tablets enable seamless digital lives'. July 2012. found at: http://www.iab.net/media/file/IAB-Mobile-Devices-Report-final.pdf.

[5] Erica Newland Heather West Justin Brookman, Sean Harvey. 'tracking compliance and scope'. *WC3*, Oct 2012. found at: http://www.w3.org/TR/tracking-compliance.

[6] Alex Fowler. 'firefox getting smarter about third-party cookies'. *Mozilla*, Feb 2013. found at: https://blog.mozilla.org/privacy/2013/02/25/firefox-getting-smarter-about-third-party-cookies.

[7] Wall Street Journal. 'what they know'. found at: http://online.wsj.com/public/page/what-they-know-digital-privacy.html, On-Going.