Privacy Implications of Behavioral Tracking in SmartPhone Applications

Michael Cueno

Abstract

Contents

1 Introduction

Smartphone and tablet platforms in the US have been caught in a privacy snafu with respect to behavioral tracking due to a lack of direct regulation [1] and very little consumer awareness [2]. As more users leave traditional consumption outlets such as TV, print and even web browser for mobile consumption [3], 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 [4] and default settings which block third party tracking cookies [5]. 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 in the mobile arena. Attribution for this can go, in part, to a lack of consumer awareness of the tracking practices that are carried out on mobile devices [**?**]. 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 to name a few.

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 [6]. I argue that as consumer awareness increases, so too will the demand for privacy on mobile platforms. This relationship is supported by a recent study [7], showing that over the past year, 72 percent of smartphone users are more concerned about privacy and 81 percent choose to avoid applications that they think will not protect their privacy.

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.

1.1 Why should we care?

Could talk about other countries policy laws here

2 Background

2.1 Evolution of Behavioral Tracking

Over the years, advertising networks have competed to increase the granularity on their target groups to what is now, in certain cases, an individual bias. A market has sprung up with devilish speed to compete for access to personal information which can be sold as profiles to the highest bidders, typically advertising networks SOURCE. This practice is known as behavioral data tracking and it got its start from the third party cookie used in web browsers.

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 [8].

The migration to smart phones As the use of mobile platforms increase, so too will the market for personal data on mobile devices. A recent survey found that smartphone and tablet users watch, on average, 30 percent less TV and consume even less print media [3]. This shift in consumption patterns along with the tantalizing personal data sets that mobile devices offer have pushed advertisers to invest heavily into mobile tracking technologies for the purposes of behavioral advertising SOURCE.

2.2 Technical Discussion of Behavioral Tracking on SmartPhones

A majority of tracking on mobile platforms is done through the applications that users download through their 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 devices 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 SOURCE .

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 source . Also, the permissions are commonly not read, and instead seen as a click through screen to installing an application. SOURCE

Web Browsing vs. Application Data. An important distiction must be made between the two ways that personal data can be collected on mobile devices. In particular, data can be gathered through mobile web browsing or through the various applications that a user may install on their device. Although IOS blocks third party cookies, most android browsers along with Firefox′s mobile browser do not [9]. Even in the case where thrid party cookies are disabled, there are various ways in which profilers can track a user through the mobile web browser. These techniques include 'device fingerprinting' [10] and leveraging a loophole in the Safari browser [11] among a few other methods [9].

These two seperate domains cause problems for advertising networks and consumers alike. Since they are indeed disjoint domains, a single device can appear to be two different users, one profile for mobile web and one for appli-

cation use. So far the only documented way of connecting these two profiles is by having a user click through an in-app-advertisement which loads in that user′s browser, thus tying the two profiles together [9]. However, the majority of data gathered in the mobile realm is through application use and not through browsing source. For this reason along with the fact that behavioral tracking through mobile web browsing is not a novel issue that is brought up through analysing privacy in the mobile ecosystem, for the remainder of this paper, we will only concern ourselves with the application tracking domain. there's a better way to phrase this..

The Future of SmartPhone Tracking (Real time location data)
The future in smartphone tracking holds some concerning characteristics for consumer privacy. Emerging technologies are commonly using location based information to provide services. SquareSpace, a payment system and competitor to Google wallet, uses location data to identify when a customer has entered a store and sends that information to the merchant along with previous shopping history so that merchant can better prepare for their transaction Source. This type of innovation has great implications for efficiency and customer satisfaction, but it also drags along horrendously private data sets that have a very high appeal to advertising networks.

Location data is the fourth most important aspect to whether a consumer will interact with an advertisement, falling underneath coupons, previous shopping history and favorite brands [3]. A company called AdNext has already begun to capitalize on the insight that location data can provide. Using location data gathered by wireless access points in one of South Koreas largest malls, COEX Mall, to build prediction models for the patrons, AdNext was able to deliver an ad based on the perceived next location of that patron [**?**]. The benefits of this approach are lucratively appealing to advertising companies and thus with the current legal climate and growth of location based services, a large market force is created around aggregating personal location data for the use of direct advertising.

This is the kind of data collection that keeps privacy advocates awake at night.

Differences between Web Browser Tracking and Smartphone tracking

The difference between traditional behavioral tracking through the use of third party cookies and the way that it is done via smartphones and tablets through applications is an important technical point that has implications on policy and privacy. In the case of cookies, the user has the ability to delete them and thus clear out the data that tracks them. NOT REALLY

In some cases, companies have used the unorthodoxed flash cookie, also known as a super cookie, which is able to respawn regular cookies after they have been deleted

2.3 Novel Issues to the Smartphone Case

Small screen size

Very personal o Make the point that smart phones are typically used by only one individual, always on and with the user. (FTC Report)

3 Evaluation

3.1 Something Needs To Be Done

Users are weary of tracking One of the most troubling aspects to the issue of privacy on mobile devices is the gaping distance between consumers' expectations of privacy and the actual reality of privacy on smartphones. In a survey taken last year, 78 percent of cell phone users think that their personal data such as contact lists, location data, name, address, etc, is at least as private as the data on their home computers [2]. This finding has a small caveat in that it assumes the survey respondents consider their home computers to be private, but this hardly seems like a controversial claim. If that is the case, then it would follow that the majority of smartphone users regard their personal information as secure and private.

In reality, underneath the hood of the mobile ecosystem, many applications obtain and use personal information on a regular basis. A study done by The Wall Street Journal analyzed 101 popular apps and showed that 56 applications sent the phone's unique identifier to third parties without notice or consent [**?**].

Many of these applications also attached many other types of personal data to the unique identifiers such as contacts, age, and gender before sending them to various companies. Since then, however, many of the application developers outed by the publication have adopted privacy policies. While it is beneficial to have the privacy practices documented in this form, the very mechanism of notice and choice is failing the average consumer, a point discussed further on.

Growth patterns Despite the fact that consumer awareness is rising with respect to data collection on mobile platforms, the trends of collection and aggregation continues to rise [**?**]. This should not be taken as a suprise as advertising networks have largely been given the go ahead from a legal perspective. The commonly cited case bieng DoubleClick vs Bose determined difinitively that tracking a user's behavior amongst multiple contexts cannot be ciminalized as long as that collection is not tortious FACT CHECK. Certianly, the demand placed on targeted advertising via ad networks is not going to go away. Thus, we will continue to see data collection companies compete and innovate over ways to more efficiently and more preciscly pinpoint your interests and thus, your suceptibility to interact with an advertisement.

Privacy Dangers One of the more violating practices that is emerging is the use of location data to serve more relevant ads to consumers.

3.2 Current Policy is not Working

Overview of current protections The current legal landscape surrounding the privacy of mobile data collection is a generaly passive one except in certain circumstances. The Federal Trade Commission (FTC) is the agency responsible for bringing suits against companies that do not abide by privacy law. Of course their powers only go as far as current statutes allow. There are only a few statutes that can be applied to the issues of smartphone data collection as it occurs in the context of advertising purposes.

Initially, in an attempt to better understand the industry [**?**] and possibly to induce companies to publish privacy policies, the FTC carried out a criminal investigation on mobile app developers under the pretenses of the Computer

Fraud and Abuse Act (CFAA). In particular, the investigation centered around the question of weather the collection of a users personal information through smartphone applications without the user's notice or consent could be considered computer fraud. Ultimately the investigation did not lead to any suits, however it did prompt mobile app developers to take the issue of publishing privacy policies more seriously not sure .

One case where the FTC had success in bringing actions against mobile data collection, was in a case involving the Children's Online Privacy Protection Act (COPPA). The act requires parental consent before collecting or sharing any information about any child under the age of 13. The lawsuit identified a number of companies that clearly marketed their applications to children and then collected emails and allowed users, mainly children, to post to the internet in the form of blogs among other things [**?**]. The defendants quickly settled to the tune of $50,000.

Why notice and choice is pursued For the general case of tracking adults through application use however, the FTC does not seem to want to push its weight around. Although the FTC states five principals in regards to fair information practices, notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress, they have, in practice not pursued them equally with the same rigor. In part due to a recognition of the importance of the free flow of information in today's economy [**?**] they have fallen back almost entirely to upholding the principals of notice and choice. Also, the commission's concept of notice includes in it common themes of many other fair information privacy principals such as the APEC privacy framework's collection limitation and uses of personal information which limits the collection and use of personal data to only that which is relevant [**?**]. In other words, the FTC punts on the concepts of fair use and collection by allowing notices to waive them. Effectually, the commission's approach allows for contractual like notices, that can contain anything the drafting party desires, no matter how "unfair" the practices [**?**].

In practice, the FTC has encouraged companies and mobile app developers to publish privacy policies. This has been apparently for practical purposes because the main mode of enforcement that the commission has used is going

after companies that have violated their terms of service or privacy policies. What else can I say..

Failures of notice and choice The theory of notice and choice for protecting consumer privacy is a wonderful solution to a very real problem. However, when applied to the mobile application world, its practical implementation is truly horrendous. Notices are often full of legal jargon and verbose to the point that many consumers do not bother to read them [**?**]. They also frequently are not even seen by the consumer, instead implicitly agreed upon through using the application (NOT SURE). The concept of choice is also troubling. The only mechanism of choice that a user is given with regards to the useage of an application, is to not use that application. Assuming that the user chooses not to use that application based solely on its policies on personal information, there is nearly never an alternative to that application that differs only in this way. Thus, the privacy concerned user makes not only the choice to not use the app, but the choice to not use any application that offers a similar service get sloan's source .

If consumers were made aware of the privacy implications in a simple and transparent notice and then given a choice that did not bar them from participating in the mobile ecosystem, the theory of notice and choice would be more aligned with its use in practice. Whats more, the regulating bodies have already set up their infustructure around these concepts which would make for a smooth approach to enforcement. What are you talking about

4 prescription

4.1 Solutions section??

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

FTC should push vendors to regulate apps

5 Conclusion

References

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

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

[3] 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.

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

[5] 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.

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

[7] TRUSTe. 'truste privacy index'. found at: http://www.truste.com/us-consumer-confidence-index-2013/, Jan 2013.

[8] Berkeley Law. Web privacy cencus. found at: http://www.law.berkeley.edu/privacycensus.htm, 2012.

[9] Kevin Trilli. 'mobile tracking: How it works and why its different'. found at: http://www.truste.com/developer/?p=86, Feb 2013.

[10] Peter Eckersley. 'how unique is your web browser?'. *Electronic Frontier Foundation*, 2010.

[11] Johnathan Mayer. 'safari trackers'. found at: http://webpolicy.org/2012/02/17/safari-trackers/, Feb 2012.