Privacy Implications of Behavioral Tracking in SmartPhone Applications

Michael Cueno

Abstract

Contents

1 Introduction

Privacy issues on smartphone platforms in the United States have been likened to the Wild West 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 presence of a conversation and and beginnings of processes to deal with the privacy issues are encouraging. 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 [2]. 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 a two tiered approach to solving the issue. First, from a tecnhological, industry regulated perspective, and secondly, with some suggestions for leglislation to plug the holes that cannot be filled with the technological approach.

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 [8]. This practice is known as behavioral tracking and it got its start from the third party cookie used in web browsers.

This unique character string lives under the hood of modern web browsers and can be used for legitimate reasons such as keeping users logged into a session with their bankś website, but the technology can also be used to collect data about consumers across many different sites. The use of cookies to perform behavioral tracking has exploded in recent years and shows no signs of slowing down [9].

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 [10].

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, such as contact lists or location 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 [11]. These unique profiles that can reveal very personal things about a user such as political affiliation or even sexual preferences [12].

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. [13] 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 of tracking procedure is through permission awareness from the application vendors. The Android market for example, informs users what types of data 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 [14].

Web Browsing vs. Application Data. An important distinction 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 [15]. Even in the case where third 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' [16] and leveraging a loophole in the Safari browser [17] among a few other methods [15].

These two separate 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 application 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 while carrying along some metadata to link two profiles together [15]. However, the majority of data gathered in the mobile realm is through application use and not through browsing [18]. For this reason along with the fact that behavioral tracking through mobile web browsing is not a novel issue that is brought up through analyzing privacy in the mobile ecosystem, for the remainder of this paper, we will only concern ourselves with the application tracking domain.

2.3 Novel Issues to the Smartphone Case

Small screen size One significant problem that advertisers must combat when to catering smartphones, is the small form factor. Even while the norm for screen sizes seems to be falling into equilibrium around larger, more pixel dense screens [19], they are much smaller than other delivery systems such as laptops and tablets. This can make typical advertisements such as banners become overly obtrusive. Ads loose their effectiveness when they are perceived as a hindrance by the user [20]; a very easy line to cross given the small and precious real estate on a typical smartphone.

Advertisers have been struggling with how to make effective use of the small screen size ever since the consumers' adoption of the smartphone. In part, this issue explains the large gap between consumer usage and advertising dollars spent on mobile which was an estimated 'opportunity loss' (uncollected advertising revenue) of $20 billion dollars in May of 2012 [10]. But while banner adverts still frequent many apps, companies are starting to use less conventional methods for delivering ads. Some techniques include notifications through the phone's operating system, rich media advertising, and audio ads where they can be applied. As the mobile advertising ecosystem matures, the methods of ad delivery will depart from the obtrusive, scaled down versions of web page ads and become more intimately tied to the phone's platform.

Another characteristic of smartphones that distinguish them from other

devices, is that they are very commonly used by only one individual, always on and nearly always with that individual. This makes them very attractive to the advertising ecosystem in that each device can be regarded as one specific person.

Already, we can see some examples of companies leveraging the smartphone's novel characteristics to create a more seductive advertising impression on consumers. Some emerging startups, for example, are commonly using location based information to provide services. Square, 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 [21]. This type of innovation has great implications for efficiency and customer satisfaction, but it also creates the externalities of private data sets that have a very high appeal to advertising networks. In fact, Square's privacy policy states that it will collect location, transaction and other types of data from users and share that personally-identifiable information with third parties such as advertising networks [22].

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 [23]. 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.

Despite its small screen size, the smartphone is becoming more and more attractive to advertisers as a platform. One of the best metrics to measure the success and exposure of advertisements is through what is known in the industry as the CPI (Cost Per Impression). This is the cost that advertisers must pay each time that an ad is served. Often this statistic is reported per one thousand impressions, or cost per milli (CPM). The average CPM

across website banners is a rough statistic as it varies widely based on niche and exposure, however, for reference, in 2012 it was $2.66 [24]. For name brand sites such as yahoo.com, cars.com and others, the standard 300 X 250 advertisement is sold for $7.00. Interestingly, advertisers can tack on an extra $9.00 for behavioral targeted ads [25] Compare this to a recent report from Opera Software which states that the IPhone pulls in a $2.85 CPM while phones running the Android OS received an average of $2.10 CPM [26]. The report continues to extrapolate that rich media, screen resolution and better user interactivity drive the CPM rate. Certainly, as smartphone technology continues to grow, so too will these characteristics. Thus, the current trends suggest that even with its weaknesses, the smartphone will become a more dominant advertising delivery device in coming years.

3 Evaluation

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 [11]. 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.

3.1 Current Policy and Legislation

The current legal landscape surrounding the privacy of mobile data collection is a generally 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 [6] 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 whether the collection of a user's 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.

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 [27]. The defendants quickly settled to the tune of $50,000.

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 [28] 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 [29]. 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 [29].

In practice, the FTC has a limited arsenal of weaponry to combat the privacy issues raised on smartphones. The enforcement strategy that they have adopted has been to encouraged companies and mobile app developers to publish privacy policies and then to pursue those entities that violate their policies.

3.2 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 mobile applications, 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 [30]. They also frequently are not even seen by the consumer, instead implicitly agreed upon through using the application. Furthermore, applications are not required to post privacy policies and many applications simply do not [11]. This sums to a situation where the user of the app is unable to make an informed decision on whether to accept the trade-off of allowing access to personal information with the service of the app.

Even if notices are provided and clear, the implementation of choice is also troubling. The only mechanism of choice that a user is given when confronted with an application that does not align with their privacy preferences is to not use that application. Assuming that the user chooses not to use that application based solely on its privacy policies, there is rarely an alternative to that application that differs only in the way it handles privacy. For instance,

if a consumer wishes use Amazon as their mobile, online shopping outlet, but disagrees with it's terms of service or privacy policy, there are not likely to be any other online shopping applications that offer their services without burdening the user to agree to a similar privacy policy [31]. 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.

Ideally, notice and choice would allow consumers to make informed decisions about the services and third parties that they expose their data to. Consumers would be aware of the complex ways that their data would promulgate through the advertising ecosystem and could more readily make an informed decision to consent or deny those practices without being barred from the service in the case of the latter outcome. Unfortunately, the ideal is far from achieved in practice as noted earlier, and we are left with a void of consumer awareness and a lack of any meaningful choice and instead consumers use applications and allow them to collect their personal data through passive acquiescence [32].

4 Prescription

Care must be taken when approaching the mobile ecosystem through the legislative lens of privacy control. Certainly, draconian measures that would limit application developers from collecting any personal information would be devastating to the industry. Many applications must use this type of data for the legitimate purposes of creating accounts for users and providing other services. On the other hand, the current legal climate of notice and choice is not sufficient in protecting the privacy of consumers in the mobile realm. Furthermore, with the lack of consumer awareness, the demand placed on privacy is not a strong enough market force to cause change in the mobile application industry. Therefore, policy in conjunction with consumer advocates must step in to better protect consumer privacy on the smartphone.

4.1 Dangers of Explicit Statutes

One danger that must be mentioned when addressing any regulation regarding the gathering of smartphone data is the possible societal impacts of limiting the use of such data. Certainly, not all data uses are evil. Many important discoveries and innovations would not have been possible without the unrestricted access to personal data.

In one case, researchers at Harvard School of Public Health carried out a study in Kenya that consisted of analyzing the location data of nearly 15 million mobile phones to try and understand the infection patterns of malaria [33]. The study found that human travel carried the infection more so than travel by mosquitoes, and that the spread of the infection followed stable patterns every year. Ultimately, the study identified areas where malaria treatment centers would be most effective, and infection rates have gone down %25 since 2000 due targeted prevention.

Clearly, some uses of mobile data can benefit an entire population, and as such, any policy implemented should not block the legitimate uses of personal, mobile data when the user consents to its use. As a result, legislation should emphasize the prevention of harm in the use of personal data and not criminalize the mere ownership of personal data sets as long as they were acquired through legitimate processes.

4.2 Technological Solution

Any regulation that uses specific, technological requirements in its language would become anachronistic rather quickly as technology advances. Thus, any statute attempting to resolve privacy issues specific to smartphones should be avoided. Instead, the FTC can use its influence to push recommendations and best practices onto the mobile ecosystem in order to achieve an industry regulated atmosphere.

Possibly under threat of creating what is known as a Trade Rule, the FTC could push mobile phone platforms to create better privacy controls for the phones that they run on. Since data collection occurs through the operating system of the mobile phone via permissioned access to specific data sets, the operating system is in the best position to block the application of these data.

Apple's IOS 6 has made great progress in this direction, offering users a privacy control panel. The panel options start with the different types of data that may be collected, location and contacts for example, and upon tapping a specific data type, IOS 6 shows the user all the applications that request access to that data. The user can then, app by app, grant or revoke access to that application's use of the data. This kind of control is applauded by privacy advocates and models exactly the kind of innovative solutions that only the operating system creators can provide. The very existence of this kind of control would allow consumers to be more aware of the data collection practices of certain applications.

Currently, Android users are only made aware of the types of data that an application will collect when they initially download the application. As mentioned previously, the user typically does not pay attention to these notices nor have a choice other than to be excluded from using the service that the application provides if they disagree with the practices. With good privacy controls in place however, the mechanism of notice and choice becomes more effective because the user can choose to still use the application, but in a way that retains her privacy preferences.

As the consumer is more easily able to deny applications the data that they request, application will need to make more clear and concise arguments for the use of that data in order to persuade the consumer to grant access to personal data sets. This approach has the extra benefit of making notices more human readable since now the drafting party is creating the notice directly for the consumer and not for a lawyer. It follows then, that users will become more aware of the value that their data holds and thus will be able to make a more informed choice.

4.3 Regulatory Solution

While this type of technological approach works great to protect consumers against data leakage from specific data sets such as location data, it is inherently limited by the technology that implements it. For instance, any data that the user supplies to the application directly, username, email, date of birth or application usage statistics for example, cannot be blocked by the operating

system short of cutting off network usage from the application. However, if this type of limitation where implemented it would make it extremely difficult for application developers to create useful applications as many applications fundamentally require access to the network.

Another area that any technological approach could not influence is the process of what happens to personal data after the point of collection. If an application user decides to allow some app access to her location data in order to get directions home, she would be offered no protection against how that data is used in the future. These holes in the solution beg resolution through regulation.

Suggestions on Policy formation

The focus on notice and choice in the United States for dealing with privacy issues in the mobile realm have resulted in a legal climate that emphasizes bureaucratic legislation which places extra costs on consumers and business, instead of encouraging enhanced privacy protection [29]. What is required, is a shift in the enforcement strategy undertaken by the FTC to promote the fair use of collected personal information, rather than the current approach of promoting privacy policies and then bringing allegations against companies who offend their policies.

Spelling out the exact components required for effective legislation is beyond the scope of this paper. Fortunately, encouraging work is being done with respect to privacy legislation in what has become known as the Consumer Data Bill of Rights [34]. In this report, seven privacy principals are detailed pertaining to the commercial use of personal data. I will outline the suggestions in that report and try to extend them to cover any issues that may be novel to the smartphone.

Any legislation dealing with data collected through a smart phone should make the distinction between personally identifiable and anonymized data. Here, personally identifiable, would mean any data connected to a name, email address, device unique identifier or any other information that could link the data to a specific person or device. Furthermore, no legislation should be put forth that attempts to regulate the use of anonymous data due to the problematic externalities that would arise from such a practice. Anonymous

data is often used for research that is beneficial to society with no harm to the individuals that provide the data [33]. Also, by its nature, anonymous data could never be used to collect damages if a company was to violate any legislation surrounding the use of such data since it could not be proven to actually belong to a plaintiff. Therefore, any statute constructed should only deal with personally identifiable information.

Currently, applications do not need to publish a privacy policy, they are only encouraged by the FTC to do so. To improve transparency, policy should be put in place to require any application or service that uses personal data to create a privacy policy and obtain consent from the user before collecting data. To avoid any chilling effect that such regulation may have on startup companies, a clause could be added which excludes any application or service with less than 10,000 users from abiding.

To promote the enhancement of privacy protection within the commercial realm, the FTC should be given enforcement grounds to pursue companies who do not adequately secure the personal data that they collect. Statutes could be put in place that create liability for companies whose data sets are compromised in conjunction with appropriate negligence in securing that data.

Consumers should also be protected against the long term, and unintended uses of their personal data. Any privacy legislation should consider enacting a proper way of allowing consumers to dispose of personal data sets from applications upon the termination of their accounts or services. Given the complexities of the mobile and online advertising ecosystem, it would be incredibly difficult to ensure that all traces of personal data collected through a specific application are appropriately deleted. In light of this fact, the mechanism of notice will need to be sufficient in informing the consumer that any data shared with third parties would not fall under this regulation.

4.4 Notable Current Developments

Currently, there is some encouraging debates and conversations happening in the legislative sector with regards to mobile privacy. One such development is a bill introduced by representative Hank Johnson called the Application Privacy, Protection, and Security (or APPS) Act. This bill would make notices

of privacy procedures mandatory for mobile applications, provide opt-out and deletion measures to consumers, and put in place statutes for the security of any collected personal data [35].

Also, the Obama administration has put forth what it is referring to as the Consumer Data Bill of Rights. It contains legislative suggestions to congress which specify the core principals that are common to many other fair information privacy practices [36]. It will be interesting to see if any privacy legislation materializes out of that report.

5 Conclusion

If consumers are made aware of the privacy implications in a simple and transparent notice and then given a choice that does not bar them from participating in mobile services, the theory of notice and choice would be more aligned with its use in practice. The combination of a more privacy concerned mobile operating system market and appropriate personal data regulation will result in a much more private experience for the average smartphone user.

References

[1] 'privacy in the age of the smartphone'. *Privacy Rights Clearinghouse*, April 2013. available 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. available 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. available at: http://www.w3.org/TR/tracking-compliance.

[5] Alex Fowler. 'firefox getting smarter about third-party cookies'. *Mozilla*, Feb 2013. available at:

https://blog.mozilla.org/privacy/2013/02/25/firefox-getting-smarter-about-third-party-cookies.

[6] Wall Street Journal. 'what they know'. See ongoing series, available at: http://online.wsj.com/public/page/what-they-know-digital-privacy.html.

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

[8] Julia Angwin. The web's new gold mine: Your secrets. July 2010. available at: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

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

[10] Mary Meeker. 'internet trends'. May 2012. available at: http://www.kpcb.com/insights/2012-internet-trends.

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

[12] Herb Weisbaum. Who's watching you online? ftc pushes 'do not track' plan. 2012.

[13] Brain X. Chen. Cellphone thefts grow, but the industry looks the other way. May 2013. available at: http://www.cnbc.com/id/100700503.

[14] FTC Staff Report. Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. available at: www.ftc.gov/os/2012/03/120326privacyreport.pdf, Mar 2012.

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

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

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

[18] Natasha Lomas. The app economy is in rude health, says flurry, but mobile browsers are being squeezed by facebook. April 2013. available at: http://techcrunch.com/2013/04/03/apps-vs-mobile-web/.

[19] Darrell Etherington. Study: Average display size climbing on all devices except for mobile pcs. Oct 2012. available at: http://techcrunch.com/2012/10/16/study-average-display-size-climbing-on-all-devices-except-for-mobile-pcs/.

[20] David Murphy. Mobile advertising intrusive and largely ignored. 2011. available at: http://mobilemarketingmagazine.com/content/mobile-advertising-intrusive-and-largely-ignored.

[21] This is outlined in the future plans for the payment system, Square. See Jack Dorsey's talk (founder of Square) at: http://www.youtube.com/watch?v=2zoeiNBdPdo.

[22] See Sqaure's privacy policy page at https://squareup.com/legal/privacy.

[23] Byoungjip Kim, Jin-Young Ha, et al. Adnext: a visit-pattern-aware mobile advertising system for urban commercial complexes. 2011.

[24] Jason Del Ray. 'forrester reduces its forecast for online ad spending'. Oct 2012. available at: http://adage.com/article/digital/forrester-reduces-forecast-online-ad-spending/237647/.

[25] 'interactive media advertising rates, effective february 27, 2012'. Advertisment quotes from triangle online network. Available at: http://media2.newsobserver.com/advertising/pdf/InteractiveRatesQ12012.pdf, 2012.

[26] Opera Software. 'the state of mobile advertising, q2 2012'. available at: http://business.opera.com/sma/2012/q2/, 2012.

[27] Mamie Kresses or Michael Ostheimer. 'mobile apps developer settles ftc charges it violated children's privacy rule'. Aug 2011. available at: http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm.

[28] Fred H. Cate. The privacy problem: A broader view of information privacy and the costs and consequences of protecting it. 2003.

[29] Fred H. Cate. *Consumer Protection in the Age of the Information Economy*. Ashgate Pub Co, 2006. Chapter 13.

[30] Federal Trade Commission. Workshop on the information marketplace: Merging and exchanging consumer data. comments of Ted Wham, May 2002.

[31] Felicia Williams. Compliance to the fair information principles. 2006. avaliable at: http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf.

[32] Robert Sloan and Richard Warner. Beyond notice and choice: Privacy, norms, and consent. 2013.

[33] The Boston Consulting Group. 'unlocking the value of personal data: From collection to usage'. Feb 2013. Location data was gathered by analyising texts and calls intercepted by cell phone towers (not gps).

[34] The White House. 'consumer privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy'. Feb 2012. available at: www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[35] Application privacy, protection and security act. Introduced by Rep. Johnson. More information available at: http://hankjohnson.house.gov/press-release/rep-johnson-introduces-apps-act-privacy-bill.

[36] Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. available at: www.whitehouse.gov/sites/default/files/privacy-final.pdf, Feb 2012.