Mobile App Monetization

Sharon Lin and Kunal Shah
UC Berkeley Master of Information and Data Science
W231-2: Legal and Ethical Concerns

The Rise of Mobile Apps

Since the introduction of the first iPhone in 2007, the adoption of smartphones has dramatically increased across the world. Compared to laptop or desktop, smartphones provide more ease to users in accessing the internet and the contents they need, while being much more convenient to carry. Mobile Analytics by comScore have shown that mobile usage has been increasing faster than desktop usage ("The U.S. Mobile App Report"). And as of January 2014, mobile has officially overtaken desktop in terms of number of users. Even internet giants such as Facebook and Google, which together account for a large amount of internet usage across the world, have changed their launch strategies for their core products to be mobile-first (Ingram). According Pew Research Centers, there are currently two billion cell phone users around the world, of which approximately half of the users are smartphone users (Purcell).

As smartphones become commonplace in the world, mobile apps have become a quintessential aspect of the mobile sphere. Mobile apps are programs designed to run on the smartphone, distributed via application distribution platform such as Apple's App Store or Google's Google Play. In the report by Pew Research Centers, they found that more than 80% of the time a user spent on mobile is spent in apps (Purcell). On top of heavy usage, the report also found that users are frequently exploring new apps. Half of the users mentioned that they have downloaded an app in the past 30 days, and 10% have downloaded in the past week. Users will also pay money to have access to these apps. One in eight users had paid to download an app. This not only makes mobile apps a steadily growing market, but also a market that's prime for marketing and monetization.

The app market has become the core of the smartphone industry. But what is the implication of the growing economy of the app market, and how will this affect users? Dixon, a partner with a venture-capital firm, says that "the app economy creates an environment in which the rich get richer". Popular apps dominate the app ranking boards, which leads to have more downloads and more time on the ranking board for these apps. This subsequently leads to higher usage and revenue. This has shaped the mobile industry to become similar to the TV industry. In the TV industry,

popular shows get more users, thus get more revenue, both from DVD sales and ad revenue. The less popular shows receive less revenue and are eventually cancelled. In the mobile world, while apps usually will not get "cancelled", the most popular apps get more users, and will gross more revenue from a combination of app sale, in-app purchase, and advertising. The apps that do not make onto ranking boards are harder to get discovered, especially without marketing promotions. These apps often get less users and thus gross significantly less revenue.

However, unlike TV, where show producers have fewer data points and less specific information about their audiences, apps are able to collect much more data about their users due to the nature of smartphones. This opens up more avenues for privacy invasion, and leads to more unethical practices. In this report, we will explore the common strategies app developers utilize for monetization, the privacy and ethical issues such strategies entail, and the current state of public policies that are set in place for regulation.

Policies

Before we delve deeper into how app monetization poses privacy and ethical concerns, we want to outline the current state of policy framework that safeguard users against such issues.

The Belmont Report, published by U.S. Department of Health & Human Services, was the first step towards protecting users from potential harm from deception and unethical practices ("The Belmont Report"). The "Respect for Persons" principle holds the most relevance with respect to app monetization, because it requires a very clear line of consent from users about using their information. It ensures that researchers carry out research without deception, and truthfully inform the users about the usage of their private data. However, the Belmont Report was very vague about the privacy of users in an online/internet context. It focused more on consent about collecting and using information in experiments.

This oversight was addressed in the more recent Fair Information Practice Principles, FIPPs for short (*National Strategy For Trusted Identities In Cyberspace*). FIPPs looks to specifically safeguard the ways in which online entities collect and use PII (personally identifiable information). The safeguards offered by FIPPs are:

- **Awareness:** The user must be informed of the data that is being collected from him, the uses for that data, and any other potential recipients of that data.
- **Choice:** This is an extension of the Belmont Report principle, stating that the user must have an appropriate choice in the decision to share any information

they regard as private/personal information.The safeguards also cover any "secondary" uses of the shared information, including sharing it with third-parties.
- **Security:** The information collectors should also take necessary steps to ensure integrity and security of all collected information.

FIPPs as such covers a lot of ground in ensuring that when interacting with online portals, users don't fall prey to deception or trickery which can lead to potential harm. However, it falls short in many ways. Collectors often have tricky caveats in their policies like "third parties may have access to information you provide under certain conditions". Statements like these are often not accompanied by clarifications on such "conditions", and it leads to a slippery assurance.

In California, CalOPPA (California Online Privacy Protection Act) takes a slightly more detailed approach than FIPPs with respect to online privacy (*Consumer Federation of California*). CalOPPA necessitates websites that operate for California residents to specify a privacy policy on their site, that satisfies the following requirements:

- The policy should be easily **available.** For an app or website, there should be a direct link to it right on the front page.
- It should be **readable.** Technical or legal jargon should be avoided, and should be stated in simple English (and more languages if possible).
- **Data Collection** process should be specified in detail. It should list all PII collected by the site/service, and should also specify how the PII mentioned above is collected.
- It should provide information about information **sharing**, by explaining who the information would be shared with, and if possible, provide links to privacy policies of the third parties who can access the information.

The above frameworks tell us that the policy makers have taken some steps with regard to safeguarding the information users share from entities external to the data collecting entity. However, the framework is clearly in very poor shape from the perspective of how the entity itself can exploit the data it collects. An app/website could use all the information it collects to tailor experience of users on their services. And while customization for every user can be an excellent feature, it can also lead to a very subtle exploitation of a specific weakness or nature that the user might not be aware of.

Background on Mobile App Monetization

With the ubiquitous presence of smartphones and tablets, mobile app downloads have skyrocketed. In order to monetize these apps, app companies have sought out ways to monetize their apps, either through releasing paid apps, promoting in-app-purchase, or setting up advertisements.

Many apps are released as paid apps in order to generate revenue. However, app companies have been looking for additional ways to generate more profit. One of the limitation of paid mobile apps is that users pay a set amount up front for the app, but usually do not have to make additional payment after making the initial purchase. While companies sometimes release additional content behind a paywall in the app that requires additional payment for access, users are still able to access all the content for a set pricing. In this way, companies cannot generate additional revenue from these users past the maximum cost of the content. In order to continuously and indefinitely generate revenue from apps, companies started releasing their apps, especially mobile games, as freemium apps. For freemium apps, users can download and access the app for free. However, once a certain limit has been met for a user, such as spent all of his in-game virtual currency or used up all the actions one can do for the day, the user is compelled to start paying for in-app-purchase in order to continue interactions in the app. For example, in many mobile game apps, users cannot proceed past certain points because they don't have enough in-app currency. And in order to proceed, they're forced to purchase such currency through in-app-purchase. In this case, app companies can continue to generate revenue as long as users continue to pay in order to keep on playing.

In addition to in-app-purchase, companies can also monetize users via advertisement. As a user interacts with an app, ad content for another app or brand will sometimes be served. In such cases, revenue can be generated either by impression, click, or download. For pay-per-impression, the company purchasing the ad will pay the ad-delivering app for every ad content it shows the user, regardless of the user's action upon being served with the ad. For pay-per-click, the ad-purchasing company pays when a user clicks on the ad. For pay-per-install, the company pays when a user downloads the app. Advertising revenue can be lucrative for apps with huge install fanbase, especially social media apps, where users usually do not need to pay to access the app, and there is no in-app-purchase implementation. Social media apps, such as Facebook, Instagram, and Twitter, make most of their revenue through advertisement. Some freemium apps also utilize both advertising and in-app-purchase as sources of income, by offering in-app currency bonuses for installing another

advertised app, which in turn encourages users to purchase additional in-app currency to continue using the app.

Traditional Advertisement

In order to generate revenue, mobile companies have incorporated ads that are similar to online advertising units into their apps. Some of the most common mobile advertising units are banner and interstitial ads. Banner ads usually take up the top or bottom part of the screen when an app is launched, and most of the time users cannot dismiss them. Interstitial ads are ad placements that will pop up during various times when the user is interacting with the app. In order to maximize revenue from ad placements, companies will often utilize users' data in order to optimize the likelihood of users taking an action with the ad. App developers often integrate their apps with third party mobile platforms, such as Chartboost and Flurry, that will help companies analyze user data and optimize monetization through mobile ads. From the developers, these third party platforms receive users' in-app data, such as when a user logged in, how long they spent in the app, and what actions they took in the app. Using these data, platform companies can develop algorithms that determine what type of ad a user is most likely to interact with it, when is the best time to present the ad, and how much revenue the ad will generate.

While app companies do not disclose PII, such as the user's name or phone number, to the third party platform company, data about the device a user uses can be disclosed. For example, Apple adopted a system called IDFA (Identifier for Advertiser), which allows advertisers to track users without PII. IDFA is a randomly generated identifier that's associated with an Apple device. The identifier is cached within the device. And as long as the user does not initiate a regeneration of the identifier, advertiser can use the identifier to track the user's activities across different apps. Even though the identifier does not disclose the user's personal information, by utilizing the identifier to track user's in-app activities and how much the user spends, advertisers can place ads for apps that they believe the user will spend money in. As for the user, IDFA is not an identifier that they can just "turn off". Apple has offered the ability to turn off tracking. But what this really means is that the identifier is re-scrambled automatically after a period of time. This makes tracking extremely difficult, but it does not equate to no tracking due to lack of identifier. Furthermore, users are not informed of such ad tracking ability in an explicit way, and the IDFA tracking is turned on by default on Apple devices.

Aside from tracking, advertisers often utilize strategies that are not very ethical in order to maximize advertising revenue. For example, when an interstitial ad

pops up, the button to close the ad is often designed to be very small. And unless the user clicks precisely on the close button, the click would register as an ad click, and user will be redirected to the ad content. This is especially an issue with banner ads. Many developers will design their apps in ways to incorporate banner ads right next to buttons that users need to use to interact with the app. This will result in high volumes of accidental clicks, and users being forcibly redirected out of their apps. While banner ads on desktop have given way to native advertising, it is still prevalent on mobile apps due to the smaller screen. Because the publisher of the advertisement holds the control on the display of the ad, advertisers have to pay for the cost accrued by the accidental clicks. While the tactics may not seem as ethical, it is still legal. And similar to online advertising, while there isn't much discussion regarding ethical issues regarding mobile advertising, the FTC has started taking a look at the privacy issues regarding mobile advertising.

In 2012, FTC has put out a guideline to help mobile app developers observe truth-in-advertising and privacy principles ("Marketing Your Mobile App: Get It Right from the Start"). In the guideline, FTC discusses that app developers should "collect sensitive information only with consent", listing medical, financial, or precise geolocation as examples for sensitive information. While it is true that most app developers do not collect such information, many of these information can be deduced from users' app usage data. For example, developers can gauge a user's financial level by how much and how frequent a user spend money in the app. With that, advertisers can do segmentation on users' depending, and set up ad units accordingly. In such case, a user's PII is not even needed as advertisers can already collect what they need from user's usage data. Also, even though FTC has released this as a guideline, there's no enforcement on such guideline. It is well known that many app developers collect user's geolocation data as part of the app's functionality. For example, Uber strongly encourages users to have location service to be turned on, as it is one of the main functionality of the service. And as part of Uber's privacy policy, they can use user's personal or usage information, which includes name, geolocation, email, even credit card, for what they would deem as internal business purpose ("Uber's Users Terms"). And because there is no explicit statement of how long Uber will keep your data, it is assumed that the data is kept forever. And in the event that the user deletes his account, Uber will still hold onto the user's data unless the user explicitly writes in to have his data removed. With geolocation data stored, advertisers can use such data to determine what type of advertising works the best for specific geolocation, and serve specific advertising content based on such information. This becomes a privacy issue as developers and advertisers can potentially estimate specific location information about their users,

such as where they live and where they work. With approximated data about a user's location and spending pattern, developers can serve exploitive ads that are very targeted even without any PII.

In-App-Purchase

Nowadays, the most common way for app developers to monetize their users is through in-app purchase, IAP for short. IAP is a microtransaction that a user make in order to purchase virtual goods. Monetization through IAP is the integral aspect of freemium apps, which are mostly games. For freemium games, app developers will offer the app free of charge. However, users will have to pay money, the "premium" aspect of the app, in order to access functionality, features, or virtual goods. In order to maximize users' spendings within the app, developers will track users' IAP-related actions within the game. This can range from when a user clicks on the button which launches the in-app store, how often a user clicks on specific IAP item, how much the user spends in each transaction, and how a transaction is terminated, either successfully through a purchase or unsuccessfully through the user canceling the transaction. With these information, users are often segmented into different groups base on their IAP history - whales, dolphins, and minnows. While most of the users will never make an IAP transaction within the app, these three user segments, especially the whales, generate majority of the IAP revenue for an app. Minnows are users who spend very little within the game, usually around $1-$5 per month. Dolphins are users who spend around $5-$20 per month. Whale's definition differs depending on the app developer. Whales' average spend can range from $20 per month to hundreds of dollars a month within the game. Whales generate majority of the revenue for an app. According to a VentureBeat interview of 5th Planet's CEO Robert Winkler, in 2012, their game Clash of the Dragons has 90% of its revenue coming from users who have spent more than $100, and 40% of the revenue comes from users who have spent more than $1000, with their top whale having spent $6700 (Carmichael). With potential revenue from dolphins and whales being so lucrative, developers will track extensive information from such users, and highly guard the information of users they know are whales. However, users are mostly not informed by the app developers what type of information is being tracked, and to what extent these tracking goes.

One of the biggest complaints that arises in regard to in-app purchase is the unauthorized charges by kids on apps that are targeted at children. On many smartphone devices, authorization, often in the form of password, is required when making a purchase inside an app. However, once a purchase authorization is made, app distribution platforms, such as Apple's App Store, will allow a "grace period" of

certain time range before it'll prompt for authorization again. This means that after users input a password and make a purchase, they have a certain time period, such as 30 minutes in Google's case, within which they can make unlimited amount of purchases without being prompted an authorization request. This becomes a major issue within children apps, where children will make hundreds of dollars of in-app purchase without parents' consent and authorization. Furthermore, parents were never informed of this "grace period" functionality, and were often not aware of the charges until they receive the bills. Because of this "unfair" practice of billing parents charges that they did not authorized, FTC has filed complaints against device manufacturers such as Apple, Google, and Amazon, and at least Apple and Google have since settled these complaints by refunding parents charges from unauthorized in-app purchases made by their kids ("Google to Refund Consumers at Least $19 Million to Settle FTC Complaint..."). And to resolve the issue that parents are not informed about the "grace period" policy, Apple and Google now allow users to change authorization preference to prompt password each time a purchase is made. In Apple's case, when a user makes a purchase, the authorization screen shows that it will not prompt the user for password entry again for 15 minutes. A user can change the setting to prompt password every time a purchase is made. However, by default, the "grace period" option is turned on. While this now circumvent the complaint made by FTC that users are not "informed" about this authorization grace period practice, and that users cannot turn this "grace period" off, even with these new features and on-screen information, the default settings on the device remain the same. Because the default has not changed, parents who were not paying attention can still get charged for hundreds of dollars of unauthorized in-app purchase.

While the FTC has filed several complaints about unauthorized charges made by kids, they have not set up much guidelines regarding other in-app purchase practices. One of the biggest exploitive practice is the reliance on "virtual currency". Many apps, especially games, will have virtual currency that users can spend for features or functionality within the game. In order to obtain such virtual currency, users must spend real money and purchase these currencies through in-app purchase. This is a deceitful practice because, while a user may not spend real money directly to unlock a feature or turn on a functionality, they'll likely do so if they're spending virtual currency. And app developers can run sales to entice users to purchase virtual currency, which intrinsically has no long-term value and is ephemeral. Furthermore, if a user purchase such virtual currency but does not spend all of the currencies, they cannot get their money back. For example, a minimum in-app purchase of $0.99 can give a user 100 gold inside a game. To unlock a specific feature may require 50 gold. If the user does not spend the other 50 gold within the game, it remains within the

game with no real value. This is especially an issue in mobile casino games. In most casino games, users use real money to purchase virtual currency to gamble within the game. And in the case that the user wins “money”, the amount of virtual currency they have within the game increases. However, they cannot cash out such winnings, and they cannot get refund on any virtual currency they do not end up using. What further makes this practice even more unethical is that, app developers, often casino game developers, often utilize app usage data to determine what segments of users are more likely to give in to sales and more likely to be addicted to games. This makes such users especially vulnerable to app developers who can exploit their addictive behaviors. Developers can run promotions to get such users to purchase virtual currency. And once the users are addicted to the game, they will continue playing and continue to spend money within the app. This is an unethical practice that should be changed.

Native Advertising

As traditional advertising becomes less effective due to banner blindness and ease to dismiss interstitial ads, app developers have incorporated more native ads into their apps. Native ads are paid media in which the experience with the ad follows the natural form of user experience within the app ("A Guide To Mobile Native Ads"). For example, Tumblr has its ad units set up in a form that’s similar to the form of the contents users post in their app. In such case, a small indicator, usually in the form of a “Sponsored” text next to the ad, is presented to inform the users that these are ads. However, it is very easy to miss such indicators if users are not aware of them. With native advertising, advertisers can easily target users using social media data, and deliver the optimal content in a natural setting.

Since the emergency of native advertising, there have been many ethical issues relating to such practice. First of all, because ads are blended in with the contents, it is very easy for users to miss indicators differentiating ads from real contents. Furthermore, if users aren’t informed or educated in differentiating ads, they can be misled into thinking that ads are real app contents. This is especially an issue for apps that curate news articles or facts. For example, a user is browsing an app curating health-related articles, and there’s a native advertisement about a new fad diet. If the user cannot differentiate the ad from the rest of the content, he can easily believe the ad to be part of the app content. This will not only lead to accidental clicks, but potential mis-information on the user side.

Aside from potential issue caused by difficulty differentiating ads, there have been ethical and privacy problems arising from companies using user-generated

content as native advertising. This is especially an issue in social media apps. Previously, Facebook and Instagram rolled out the ability to allow advertisers to use user-generated content as sponsored posts, a common form of native advertising within social media apps. This became a huge controversy as the users were not informed that their post is being used for advertising purpose. Furthermore, this becomes a privacy issue as other users, mostly strangers, that are not in the user's immediate contacts were able to see the post or picture the user posted due to its "sponsored" status. When Facebook and Instagram first rolled out such policy change, most users were not aware of the change because app developers bury such change deep within their Terms of Service change notices. In Instagram's case, their Terms of Service change revealed that the company has the rights to use any photos users posted on the app without notification to the user, which pave the way for such photos to be used for advertising purpose. Many news outlet picked up on this change and reported extensively on this clause (Patel). The user base protested and Instagram immediately backtracked the change (Systrom). Since then, companies have shunned away from using user-generated content as advertising without consent due to bad press and user backlash. However, many companies have turned towards paid endorsement via user-generated contents as an avenue for native advertising.

Recently, many companies started paying users with high fanbase to post content curated specifically for their products. They then turn such post into a "sponsored" native advertising post, and rely both on advertising reach and the user's large fanbase to reach a wide range of audience. In such case, if a user sees the content via organic reach instead of sponsored content, there is no disclosure that the content was curated for advertising. Users, therefore, will have no ability to differentiate curated ad content from actual content. Combined with bulk data collection from users, advertisers can segment users and target them with native advertising contents that are very effective against users. This is an ethical issue as users can be mislead and misinformed by such contents. However, there is currently no policy regulating native advertising within apps, leaving users vulnerable to potential misinformation presented by advertisers.

Deep Dive into Current Privacy Policies

In reality, a lot ethical and moral violations exist despite of the frameworks set in place to protect users. The practices in reality highlight some major flaws in FTC's vision and the coverage of the policies they have put in place.

FTC focus on other problems

In the mobile space, FTC currently is more active in addressing issues caused by mobile carrier services ("Mobile Technology Issues"). These involve issues with carriers

using deceitful means to get money from users through overcharging on bills or having hidden “special conditions” on features like unlimited data. FTC further addresses carriers’ violations of truthful advertising. One of the major issue they try to tackle is carrier advertising “unlimited” data as a feature people can purchase, when in reality the data is not “unlimited”, as carriers will start throttling users’ data usage after a certain threshold. Another primary focus in this space for FTC is on potential COPPA violations.

Both these kinds of violations are really important to handle, and merit attention from the FTC. However, the concerns over exploitive use of data for app monetization is an equally important issue, and the FTC needs to focus on these issues too.

Data collection safeguards

There are few details missing in the safeguards with regard to data collection. The framework stresses in detail about policies specifying what PII is collected from the user, and how it is stored and used. However, it needs to do better job of defining limitations on data collection. There are no regulations on bulk data collection from a user. There are some broad guidelines, but there is no binding regulations on app developers.

Another aspect that most mobile developers’ Term of Services lack is that none of them grant the user himself any control of any form over his data. Developers are not obliged to delete the data once a user deletes an app, or no longer wishes to use it. There is no obligation on app developers to make an official process for people to request their data to be removed. In some cases, users can make such request through app moderator channels, or an explicit request via written letters or emails. But the process is never easy, and the app developers are not bounded by regulations to comply to the requests.

Users also lack any way to “opt-out” of data collection while using the app. If an app provides a useful service, but adds unavoidable intrusions that are ethically gray, users have no way around it. The policies do not give the users any power or say in data collections, even when some collections are blatant ethical violations.

Policies allow vagueness

CalOPPA requires apps to provide information about what data would be collected by the app in an “easily accessible” location for users. However, most apps don’t reveal this information during the install/download process. It is usually nested inside the developer’s website, which most users never look up at all. It is not even enforced that the app developers need to reveal the specifics of all the information

collected. Since the term accessible is open for subjective interpretation, that part of the policy has provided a very limited safeguard.

The Privacy Policies are also required to list out all the data that is collected that is personally identifiable, and explain how it would be used/distributed. However, there is no safeguard against policies using language such as “PII won’t be share with third parties except in special conditions”, or “we collect PII like email and phone number”.

A far more obvious hole with this part of the framework is that it provides minimal safeguards against Term of Service policies that collect and store data collected by the app for purposes that are vague and broad. Most apps mention that “user data will be collected only to improve user experience”. This provides no guarantee that the data will not be used in a way that would be objectionable if the user knew of the process. Furthermore, “improve user experience” is a very broad purpose, and the interpretation is decided by the developers and not the users. Therefore, users have no protection against data collection that they may view as unethical but the developers state that they need it for such purpose.

With these views, we can see that the policies we have in place right now provide a framework to build stronger versions of policies moving forward, but the coverage for now is quite inadequate in providing reasonable safeguards.

Conclusion

As noted in the previous section, the current public policies regarding the mobile app industry need to be revisited in terms of their adequacy to protect users against exploitation. However, changes need to be made beyond just modifying the current policies in place.

Ideally, we will not just revisit the policy framework, but rather update the policy development framework itself. In a world that is progressing with a heavy emphasis on big data, specially in the realm of apps that take up a lot of a user’s time, we need a more progressive development process for policies too. Our ideal solution would be:

- Develop a more accessible forum/avenue for voicing out ethical/privacy violations.
- Once verified, the holes in the policy that allowed those violations to happen should be addressed in a timely fashion.

An iterative process like this, though difficult, would be the only way to keep up pace with the development cycles of apps.

However, we realize that such a solution is extremely idealistic, and realistically, we need to settle for more concrete and immediate additions to the framework that are at least “absolutely required” in light of problems highlighted in this report. In our opinions, such additions are:

- There needs to be more explicit information given to the user about what data is tracked by which actions - including definition of such data and action, how long they’re stored, and easier access to user’s own data that’s collected by the app. App developers should also be required to provide ways that allow the user to easily request his data to be removed once he is no longer using the app. In such scenario, even if he can’t control what the app collects, the user will have a better understanding of what the app collects, and allow his data to be removed.
- There need to be more safeguards around data usage. App developers must reveal what data was used for which service improvements, general roadmaps for service improvements, and be more explicit in their Term of Services about what constitutes “user experience”.
- The information listed above should be more accessible at the time of install and download rather than located in a separate location outside the application distribution platform.

It is clear that we still have a long way to go before users can feel “protected” against data collection by app developers. But greater awareness will eventually lead to greater voice to such concerns. And this will lead to policy changes that will allow safer environment for app users.

Works Cited

"The Belmont Report." *The Belmont Report*. U.S. Department of Health & Human Services, n.d. Web. 03 May 2015. <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.

"The California Online Privacy Protection Act (CalOPPA)." *Consumer Federation of California*. Consumer Federation of California, n.d. Web. 03 May 2015. <http://consumercal.org/about-cfc/cfc-education-foundation/what-should-i-know-about-privacy-policies/california-online-privacy-protection-act-caloppa/>.

Carmichael, Stephanie. "What It Means to Be a 'whale' - and Why Social Gamers Are Just gamers." *VentureBeat*. VentureBeat, 14 Mar. 2013. Web. 04 May 2015. <http://venturebeat.com/2013/03/14/whales-and-why-social-gamers-are-just-gamers/>.

"Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges." *Federal Trade Commission*. Federal Trade Commission, n.d. Web. 04 May 2015. <https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it>.

"A Guide To Mobile Native Ads." *Mobyaffiliates*. Mobyaffiliates, 28 May 2014. Web. 04 May 2015. <http://www.mobyaffiliates.com/blog/mobile-native-ad-guide/>.

Ingram, Mathew. "The Rise of Mobile Apps and the Decline of the Open Web — a Threat or an Over-reaction?" *Gigaom*. Gigaom, 08 Apr. 2014. Web. 03 May 2015. <https://gigaom.com/2014/04/08/the-rise-of-mobile-apps-and-the-decline-of-the-open-web-a-threat-or-an-over-reaction/>.

"Marketing Your Mobile App: Get It Right from the Start." *Marketing Your Mobile App: Get It Right from the Start*. Federal Trade Commission, n.d. Web. 03 May 2015. <https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start>.

"Mobile Technology Issues." *Federal Trade Commission*. Federal Trade Commission, n.d. Web. <https://www.ftc.gov/news-events/media-resources/mobile-technology>.

National Strategy For Trusted Identities In Cyberspace. *Appendix A – Fair Information Practice* (n.d.): n. pag. *Fair Information Practice Principles (FIPPs)*. National Institute of Standards and Technology. Web. <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>.

Patel, Nilay. “No, Instagram can't sell your photos: what the new terms of service really mean.” *The Verge*. The Verge, 18 Dec. 2012. Web. 03 May 2015. <http://www.theverge.com/2012/12/18/3780158/instagrams-new-terms-of-service-what-they-really-mean>.

Purcell, Kristen, Roger Entner, and Nicole Henderson. "The Rise of Apps Culture." *Pew Research Centers Internet American Life Project RSS*. Pew Research Centers, 13 Sept. 2010. Web. 03 May 2015. <http://www.pewinternet.org/2010/09/14/the-rise-of-apps-culture/>.

Systrom, Kevin. “Thank you, and we’re listening.” *Instagram Blog*. Instagram, n.d. Web. 03 May 2015. <http://blog.instagram.com/post/38252135408/thank-you-and-were-listening>.

"Uber's Users Terms." *Uber - Legal*. Uber, n.d. Web. <https://www.uber.com/legal/ind/terms>.

"The U.S. Mobile App Report." *ComScore, Inc*. ComScore, n.d. Web. 03 May 2015. <http://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report>.