App Store: Am iSecure?

By Gagandeep Singh Kohli

CSC 300: Professional Responsibilities

Dr. Clark Turner

June 28, 2011

Abstract

In 2010, Apple was sending personal data of iPhone users such as birthdays, gender and postal codes to advertisement agencies [12]. This data was sent by applications installed on the iPhones that had been approved by Apple and published to the App Store. After acknowledging the presence of these features, Apple continued to allow applications to send out users' personal information without informing its consumers [15]. The Wall Street Journal claims that people were shocked after hearing that applications sold massive quantities of confidential information to advertisement networks [18] [30]. In addition, people claimed that actions of these applications intruded upon their personal privacy and thus gave companies insight to their private life [30]. Therefore, the following question arises: was it ethical for Apple to allow the continued transmission of user sensitive data to application vendors? Software Engineering Code of Ethics will be used to show that the actions of Apple and application developers are unethical in terms of privacy and business practices.

[1]Edited and revised by: Sean Glover - darkone238@gmail.com & Liz O'Neal - caldrama@sbcglobal.net

Contents

1 Facts

With growing demand for both mobile devices and personalization, software companies are focusing their software development toward the mobile platform. As a result, companies such as Apple, who originally started in the computer industry, have shifted their focus toward the mobile market [23].

In 2007, Apple entered the mobile market with the release of the iPhone [23]. Michelle Maisto, editor at eWeek, states that Apple is ranked as the fourth largest mobile device carrier in the world of mobile market. After selling 7 million iPhone units, Apple launched the iPad and an application market [11]. Refered to as the App Store, Apple's application market ranked number one among similar application market by out selling Microsoft's Windows Marketplace and Google's Market [25].

In April 2010, Alasdair Allan, a researcher at Exeter University, found a file named *consolidated.db* that Allen states exists on every iPad and iPhone [1]. The file contains information such as a user's name, gender, birthday, pinpoint location and Unique Device Identifier (UDID). Additionally, a UDID is a number given to each device and may be used to identify a particular user [27]. Given that the file is stored without any security protection, downloaded applications are given permission to access the file without the consent of the user [10].

In addition, Eric Smith from Bucknell University discovered that UDIDs of iPhone devices were being shared with various advertisement agencies by applications downloaded on the iPhone. The UDID may be used to track a mobile device users' online activity such as which application the client have download [16]. Along with the UDIDs, users' geographic locations were being transmitted as well [16].

In December 2010, Wall Street Journal issued an investigative article, reporting that applications sold on the App Store have accessed the conolidated.db file [36]. Their investigation discovered that Pandora Music Inc., an application which is available on the App Store, has collected and transmitted users' sensitive data to advertisement agencies. The Wall Street Journal claimed that the popular music application sent users' age, gender, location, password, contacts and UDID to various ad networks [36].

After acknowledging Pandora's behavior, the Wall Street went on to closely examine the behavior of other top applications sold on the market. As a result, they found out that of the top 101 most popular applications, fifty-five had shown to have transmitted similar information to other companies without user's awareness [36].

Further on, a research team, Veracode, took apart various applications found on the App Store that had been accused of exploiting users' personal information. They found that applications such as Pandora, sold on the market for free had precompiled advertisement libraries. These library codes contained "variable references that appear to transmit the user's birthday, gender, and postal code information" to advertisement networks [33].

2 Research Question

It is now clear that these facts lead to this ethical question:

Was it ethical for Apple to allow the continued transmission of sensitive user data to application vendors and advertisement agencies?

The applications not only have access to the UDIDs of the phone, but also users' location, gender, age, and Internet protocol address [33]. If all of this data combined falls into the wrong hands or is used inappropriately by advertisement agencies, identity theft may occur. Since the data is collected by applications, without the consent of the user, one never knows who has access to their personal information. Therefore, the answer to this question will help software engineers better understand how to handle issues of privacy.

3 Arguments Against

It is not ethical for Apple to allow the continued transmission of user sensitive data to application vendors without the user's consent:

3.1 Uninformed Users

An anonymous user at Threatpost claims that "folks who installed [applications with] spyware on their phones weren't aware of the extent to which their personal data was being passed to others" because the users were not fully informed [30].

Further on, the user thinks that application developers must provide users with notice as to how the application works. Then afterwards it should be the choice of the users to either approve or not approve the functionality of the application. According to the anonymous users, if a consumer accepts to share his personal data, "most folks would rather decide for themselves who gets their personal information and when" [30].

3.2 Court Cases

Several class action lawsuits were filed against Apple and its applications vendors. These companies were accused by consumer for tracking users' activity and sharing consumers personal information with advertisement agencies.

On December 23 2010, Jonathan Lalo filed a complaint claiming that applications, such as Pandora, Paper Toss and Weather Channel, had access to his personal information. In addition, these application did not inform or require his consent. Thus, Lalo suggests this violated federal computer fraud and privacy laws [26].

On April 22 2011, Ajjampur and Devito sued Apple in a Florida district court. They claimed that Apple's new mobile devices , iPhone 4 and iPad, tracked users' geolocational data. Furthermore, they claimed that location data of the user is consider personal information [13]. Therefore, Apple was accused of invasion of privacy and computer fraud for tracking its users.

On May 2011, Lymaris M. Rivera Diaz sued Apple in a Puerto Rico district court. Diaz accused Apple of "intentional interception of personally identifying information." This mean that UDIDs, along with users' location data were used by advertisement agencies without the consent of users, violating their privacy [10].

Diaz also states that Apple claims to their users that they take security seriously, then he wonders how did Pandora gain access to his personal information? Diaz argues in his case that Apple didn't fully pro-

tect its users and applications didn't inform the users of their actions [10][36].

3.3 Violation of Privacy

Subsequent to following the acknowledgment that applications in fact, do collect users' personal information. A Treatpost article called "Pandora Mobile App Transmits Gobs Of Personal Data" by Paul Roberts explains that gathering personal information about a user, without their consent gives advertisers "significant insight into a person's life." These applications violate one's personal property and privacy laws [30].

4 Arguments for

It is ethical for Apple to allow the continued transmission of user sensitive data to application vendors:

4.1 Hidden Cost of Free Applications

Paul Roberts at threatpost.com defends Apple by saying services or applications labeled free on the App Store are not really free. There is a hidden cost attached. Due to the fact that companies cannot function without money, "applications that are free need to use advertisement for employing their products to the users" [30]. Also, an anonymous user further claims that since "Companies can't function without money, either pay for the full app and get rid of the ads or suck it up and realize you are paying in a non-monetary form" [30]. The anonymous consumer concludes that applications vendors have the right to sell users' personal data to advertisers in exchange of providing clients with free software [30].

4.2 User Agreement

In response to the Lalo lawsuit, Apple argues that when a user buys their iPhone, he/she is presented with Apple's terms and conditions. Apple's stipulations clearly state to users how their product is able to collect and use personal information to enhance their products [6]. The policy explicitly states that Apple "may collect information [about the user to] better understand consumers behavior and improve [its] products, services, and advertising" based on needs [17]. Apple concludes that if a user buys their products then these agreements are acknowledge by the users.

4.3 Improve Productivity

In the article, "How to See the Secret Tracking Data in Your iPhone," William Fenton explains to Apple users that Apple is tracking and collecting user locations to build a database. The database will assist Apple in improving the runtime speed of geo-locations. Applications, such as Maps, require global location to function [10]. Therefore, geo-location points are collected through the use of cellular network towers. Although, these points are not accurate and do not significantly provide insight into one's life [10]. These geo-location points do in fact aid the phone by improving its network quality and other location service applications [38].

Furthermore, in a research study by Mr. Levinson, who extracts data from mobile devices for legal cases, argues that collecting of

geo-location helps Apple improve its phone's productivity [15]. Along with the support of many security experts, he states that Apple maintains a record of users' location to help the phone "pinpoint locations more quickly. [Hence], saving bandwidth and battery life, when [device] owners use location-based services, like maps and navigation" [15]. These claims were further supported by Mark Seiden, who is a security consultant in Silicon Valley. He states that Apple do not have any intention of using the data stored on the phone to track people. However Seiden admits that the company needs to handle users' personal data more diligently [15].

5 Analysis

5.1 Why the SE Code Applies

To determine whether or not Apple's decision to allow continued transmission of user's sensitive data was ethical or not, I will analyze the situation with the use of Software Engineering Code of Ethics provided by Association for Computing Machinery. The code provides principles related to behavior and decisions made by software developers. This includes "practitioners, educators, managers, supervisors and policy makers, trainees and students of the profession" during the development of softwares [34]. Therefore, the SE code is valid in judging ethical behaviors of any one who claims themselves as software engineers.

These sets of standards apply to Apple since they label themselves as "software engineers [who] are the brains behind some of the industry's biggest breakthroughs" [7]. Hence, Apple is an organization of engineers who continue to maintain software as "beneficial and respected profession." Therefore, Apple is entitled to follow the sets of tenants listed in the Software Engineering Code of Ethics. [34].

5.2 SE Code 2.03: Unauthorized Use of Data

Apple's actions with regard to the authorized use of users private information applies to SE Code 2.03, which reads:

> **Original SE Code Tenet: 2.03 Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent [34].**

The SE code 2.03 dictates that all software engineers must use the property of the client or the employer in a properly authorized way. And only after informing and inquiring the consent of the property owners. The SE code is relevant in the case of Apple because Apple continued to allow applications to collect and share user personal identifying information with advertisement agencies without clients approval. The "clients," as stated in the tenant will be used to refer to iPhone users. In the fact section, I state that Apple's App Store was found to contain applications that collected users' personal data such as age, gender, birthday and UDID. Since this data can be used to identify a user so the personal data listed above will be used to refer to "property" of the user. The term authorized is used in the code above, which means to give permission [29]. Then "properly authorized" requires Apple and application developers to inform its users of how their personal information

will be used. After Apple's clients are informed, device owners must give consent to use their personal information.

With these appropriate substitutions, SE code 6.06 reads:

> **Transformed SE Code Tenet: Use personal information of Mobile device users only in ways properly authorized and with user's knowledge and the permission.**

5.2.1 Users' Consent

According to a lawsuit between Jonathan Lalo and Apple, Lalo concludes that Apple and applications downloaded from the App Store did not obtain consent from the product owners to have their personal data send to advertisement agencies and states the users were not aware of their actions as well. This is because Lalo explains that mobile users trust in Apple code of conduct and privacy policy [22].

Since App Store is only an exclusive application store for all iDevices, Apple believes that it is their duty to offer tight control of what applications should be allowed in its store [2]. In order for Apple to offer "strong privacy protections," developers must agree to Apple's iOS Developer Agreement [3]. This agreement ensures that applications are reliable, perform as expected and are free of explicit and offensive material [2]. Therefore, Apple reviews all applications available in the App Store before offering it to its consumers [22].

With the tight security of the App Store, Apple claims to its users that its store is free of "apps that violate a users privacy" [2]. Apple's code of conduct explicitly states to their users that "[they] cannot transmit data about a user without obtaining the user's prior permission. Therefore, providing the user with access to information about how and where the data will be used" [27]. Apple also controls the development process for Apps available on the store. The development process has Apple in full control of applications development and functionality [2].

In April 2010, Apple revised its iOS Developer Agreement to ban applications from sending data to any third parties except only when a user gave consent to the developers. The added statements reads "the use of third party software in Your Application to collect and send Device Data to a third party for processing or analysis is expressly prohibited" [3].

Therefore, Lalo felt safe downloading applications from the App Store. The Wall Street Journal's research suggests that among various applications, like Pandora Media, and Apple did in fact collect users' personal information. In addition, these Businesses sold the information to advertisement agencies. Therefore, Lalo and other mobile users claimed to be victims with regard to privacy violation. Since no prior permission was given to the applications for transmission of personal information [36] [22].

Lalo and other mobile device users trusted in Apple. Thus, users were never aware that applications had the authority to sell off their personal information [22]. In addition, applications and Apple did not inform its users or obtain consent therefore customers were led into believing that their online privacy was safe [22]. By collecting

and sharing users' personal information, Apple and applications did not respect the personal data of its users. Thus, Apple broke users' trust.

In conclusion, Apple and application developers created an unhealthy relationship with their clients by not respecting their users' private life. Furthermore, they misused consumers' personal information. The court case of Lalo vs. Apple ruled that since the common law such as the fourth amendment protects the privacy of the user, applications engaged in authorized use of personal data, Apple violated the common laws [36] [22]. Due to the fact that Apple and its applications did not notify its users of the unauthorized use of personal information. Their actions were inconsistent with their laws as well, Apple and the application developers broke SE Code 2.03.

5.3 SE Code 1.06: Deception

Apple's policy claims to its users that they provide "strong protection," but various sources such as the Wall Street Journal found that Apple allows applications to collect and sell users' sensitive data to advertisement agencies. This can be applied to SE code 1.06, which states the following:

> **Original SE Code Tenet: 1.06 Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools [34].**

The SE Code dictates that software engineers (Apple) should be fair and avoid deception in all claims made to the users. Users should never be lied to or mislead about how the company or the software itself functions. Dictionary.com defines deception as "the act of misleading another through intentionally false statements or fraudulent actions [8]. Avoid deception as used in the code tenant would require Apple and application developers to abstain from making any false statements, regarding confidentiality of the users.

Software and tools would be used to refer to applications downloaded from the App Store and Apple's mobile products. Tools such as the iPhone and iPad are the devices used by Apple's clients (public).

With these appropriate substitutions, SE code 1.06 reads:

> **Transformed SE Code Tenet: Be fair and avoid deception, particularly those regarding confidentiality of the client in all statements made by Apple regarding their product and applications.**

5.3.1 Confidentiality & Respect

In the lawsuit of Diaz vs. Apple, Lymaris M. Rivera Diaz accused Apple and application developers for "intentional interception of personally identifying information". This lawsuit was filed because an insecure file contained UDID along with user's personal data such as gender, age and location. In the previous analysis section, it was revealed that Apple reviews each application available in their store before offering it to users. Apple have implemented app privacy standards for

its customers" ensuring that the user is safe [27]. In the fact section, Veracode and Wall Street Journal found applications of collecting and sharing users data and the personal data was stored in an "insecure file." User confidential information was not protected, indicating Apple mislead their clients into believing that they were protected [10][36].

Also Bud Tribble, Apple's vice president of software technology, testified that Apple does not share customers' information with third parties without informing its users. Tribble also claims that Apple does not collect users' locational points or Apple ever plans to do so [14]. If the claims of Tribble are proven to be false, then Apple and Tribble would be seen to make deceptive promises [28].

On April 22, 2011, Ajjampur and Devito filed a lawsuit against Apple claiming that Apple's iPhones and 3G iPads kept track of users geo-locational information. Security experts Allan and Warden research on the devices led to a conclusion that the file is hidden from the users. However, it is stored unencrypted therefore making it easier for Apple or third parties to access [28]. Then Apple on behalf of Tribble made false statement to the public. Also Apple had failed to make its users aware of their actions in their Term and Conditions. Apple never required the consent to track its users. The pitfalls claimed that if the users had known that Apple planned to use its device for tracking, it would affect users' decisions to purchase the product. Furthermore, Simon Davis, a director of Privacy International, states Apple had failed to take users' privacy seriously [28] [4].

Apple did not protect the privacy of their users and neglected to provide them with respect. Hence, Apple broke two of their Business Values: Respect and Confidentiality. This is how the Apple Business Values defines these terms:

Confidentiality - Protect the confidentiality of Apple's information and the information of our customers, suppliers, and employees [7].

Respect - Treat customers, suppliers, employees and others with respect and courtesy [7].

Apple made a written statement that claimed the company will protect all confidential information of its users and thus will treat the user with respect. Therefore, by not taking appropriate steps to protect and respect confidential information of the user as claimed in their Business Values, Apple made fallacious statements to their consumers. Therefore, the court ruled that Apple's inadequate disclosures made in their privacy policy were deceptive and they treated their customers unfairly. Thus, Apple violated SE Code 1.06 by making deception statements.

5.4 SE Code 3.12: Identify Document to Clients

It was previously stated that Apple and applications did not indicate to their clients how their applications work. This form of behavior falls under SE code 3.12 which states the following:

Original SE Code Tenet: 3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software [34].

The SE code dictates that software engineers should develop software and related documents that do not violate the privacy of the products users.

In this situation, Apple and App Store developers are the ones who create softwares and it is their duty to respect the privacy of their clients. Clients or product users are the ones who are affected by the software.

Therefore with appropriate substitutions, SE Code 3.12 reads that software engineers should:

Transformed SE Code Tenet: Apple and application developer shall work to develop software and related documents that respect the privacy of its users who will be affected by that software.

5.4.1 WP29

On May 16, 2011, Europe's Working Party established a set of guidelines regarding geo-location services on smart mobile devices, known as Article 29 (WP29). These were established after mobile companies like Apple and among others, were found tracking users geo-location. The WP29 was adopted because under European privacy laws, geo-location data is considered "personal data". The party determined that the collection, use and other processing of geo-location data through mobile devices requires explicit informed consent of the individual" [32].

Among the many opinions adopted, the following few strictly apply to Apple:

- One of the main risks of location data processing is that the user is unaware that the device transmits the location data and to whom the information is provided [32]
- There risk that the consent for certain applications to use location data is invalid because the information about the key elements of the processing is incomprehensible to the user, outdated or otherwise inadequate [32].
- Because location data from smart mobile devices reveal intimate details about the private life of their users, the main applicable and legitimate ground is prior informed consent [32].
- Consent cannot be obtained through general terms and conditions; rather, consent must be specific for the different purposes that location data is collected, used or otherwise processed [32]

Apple tracking policies are not clearly presented to the users, they are unaware that the company tracks their private data. Given that collected geo-locational data can be used to identify any users under the privacy laws, a formal consent from the user must be acquired. In the previous analysis, Apple was found of not acquiring consent or making its users aware. Thus, software

developers did not develop software that respects the privacy of the users.

Furthermore, Apple did not identity or clearly present to the clients how their software functions. When a user downloads an application form the App Store, they are provided with a one sentence dialog box indicating the permission needed by the application in order to run. The users must accept the dialog in order to run the applications. Hence, users have no way of opting out from the permission. Therefore, users must accept the guidelines of the applications in order to use the software. Users state that a sentence is not enough to fully explain how an application might use its given permissions [36]. Thus, users really don't know how permissions are being used by downloaded applications [36]. If an application violates its given permission, then how can a user trust software developers?

"If a user allows an application to access [their] location information, he/she has no way of knowing if the application will send her location to a location-based service, to advertisers, to the application developer," or to any other entity [24]. Companies are tracking people everywhere they go, thus a user feels unsafe. Therefore, Aaron Mayer, an attorney, states that "If you are a federal marshal you have to have a warrant to do this kind of thing, and Apple [and other companies are] doing it without one" [35]. In addition, these companies are breaking federal laws and intruding consumers private data.

According to SMobile, "a mobile security company reports that one out of every 20 apps can place a call to any number without approval from the user. Also, 3% of apps can send an SMS to any number and 383 apps can read or use authentication credentials from another service or app" [31]. In addition, applications can send users' contact list to advertisement [31]. Thus, users friend and family personal information can also be misused by advertisement, leading to identify theft. Therefore, a user lacks visibility of how an application can use their private data. Since applications purchased from the store do not fully identify to the users how and where consumers personal information might be used [30].

Applications purchased from the App Store have abused their given permission by not providing users with clear documentation of their program's functions. Additionally, clients were not aware that the company and applications had insight into their lives and no prior consent from the users was granted [5]. Therefore, Apple violated intellectual property of the user by not identifying or acquiring prior consent from the user on how their products will track and collect users' location. Therefore Apple broke SE code 2.06.

5.5 Other Ethical System Analysis

5.5.1 Kant's Viewpoint

It can be argued that if Apple does not perform their "duty" of creating strong privacy protections for its users, Apple would commit an immoral action according to the philosophies of Kant [21]. Immanuel Kant was a German philosopher, who was born on April 22nd 1724 in Konigsberg Prussia. His philosophies are centered around "morality of duty". It says that in order to act morally is to perform one's duty, and one's duty is to obey the innate moral laws" [19].

Kant's theory of *Categorical Imperative* expands on"good will" and duty. Categorical Imperative "helps us (engineers) know which actions are obligatory and which are forbidden" [19]. It is based on the following three premises: universal law, treat humans as ends in themselves and act as if you live in a kingdom of ends[19]. The premises as a whole, state that one should always make decisions based on general laws and the decisions should treat others (clients) as one (Apple) would like to be treated. In other words, it means that Apple would be seen "good will," if Apple had taken precautions to perform their duty of protecting its users' personal information. In the court case of Lalo vs. Apple, App Store was found to contain software that exposed users' personal data without informing the users, so Apple did not perform their "duty." This indicates that Apple did not comply with their laws.

In addition, Kant's theory of categorical imperative stated previously can be used to say that Apple did not respect their clients and treated them fairly. While treating one fairly and with respect would require Apple to provide fair communication between both parties, the user and the client. Therefore, by not performing their duty to protect the user, Apple created dishonest and unfair environment, by making false statements. Thus, Kant would see Apple's actions as a wrongful act.

5.5.2 Utilitarianism Viewpoint

According to Utilitarianism, if Apple and its applications' actions do not produce an increase in "happiness" for their users then Apple would be seen immoral [37]. Utilitarianism is an ethical system whose principles states that people should act such that it causes the greatest amount of happiness for the most people. In other words, it means that Apple and applications should perform actions that provide their mobile users with a great amount of happiness [37]. Threatpost, a security news service, claimed that clients would not like their personal life to be exposed to an unknown authority (advertisement agencies) [30]. The court case of Lalo vs. Apple resulted that Lalo was "unhappy" that he was never aware and that his personal information was shared among various advertisement agencies. Given that the users were unhappy, Apple and applications will be seen immorally wrong under the principles of Utilitarian [22].

5.5.3 Deontology Viewpoint

Deontological Ethics is an ethical system, used to describe choices that are "morally required, forbidden or permitted" in society. These viewpoints help one determine what kind of person we are or should be. Deontological systems are based on the idea that humans should treat other humans as they would like to be treated with respect and dignity. Deontological ethics defines any actions performed as either right or wrong [9]. Acting unjustly, such as breaking a promise would be seen as a wrongful act under deontology [20].

Apple claims in their business policy that they will protect all confidential information of their users, but Veracode found Apple's statement to be deceptive. In addition, Apple allowed itself and applications downloaded from the store to collect and share users' sensitive data with advertisement agency. Thus, these actions violate

users' privacy. Therefore, the false marks of protecting the user would be seen wrong by a Deontologist, since they believed that one should always act in a way that does no harm or violates personal property.

6 Conclusion

After research came out indicating that there is an insecure file containing personal data on all Apple products, users began to wonder how much of their private information is being violated by the mobile industry. Since the user lacks the knowledge of how the inner hardware or the software running on Apple products work, we all trust companies to make ethical decision on treating their (clients) fairly with respect.

Apple had claimed in their privacy policy and as well in their Business Values that they will respect all confidential information of the client [3]. In addition, Apple claims to review each application before offering it to users. Furthermore, Apple contends to have implemented app privacy standards, and claims to have created strong privacy protections for its customers, ensuring that the user is protected [27].

However, this was not the case regarding Apple, as many class action lawsuits were filed against the company. Lawsuits such as Lalo vs Apple and Diaz vs Apple proved Apple to be wrong. In both of these cases, the legal court found that Apple violated privacy laws by sharing unauthorized use of users' personal data. Therefore, Apple did not develop software that respected the privacy of the users.

When considering the Software Engineering code, Apple failed to avoid deception by making false promises to their clients. Under Kant's principle of ethics, Apple was proved to be an "irrational being". This is demonstrated by the fact that Apple did not make decisions based on general laws and treating others (clients) fairly as one (Apple) would like to be treated [9] [20].

In violating the Software Engineering tenets, 1.06, 2.03 and 3.12, Apple was clearly unethical by allowing the continued transmission of sensitive user data. It is undoubtedly immoral and wrong to release consumers' data to application vendors without the user's consent.

References

[1] A. Allan and P. Warden, "Got an iphone or 3g ipad? apple is recording your moves." [Online]. Available: http://radar.oreilly.com/2011/04/apple-location-tracking.html

[2] "App store review guidelines." [Online]. Available: http://developer.apple.com/appstore/guidelines.html

[3] "App store review guidelines." [Online]. Available: http://www.insideprivacy.com/Apple%20Amended%20Complaint_https___ecf%20cand%20uscourts%20gov_cgi-bin_show_temp%20pl_file7379046-0--8163%20(2).pdf

[4] C. Arthur, "iphone keeps record of everywhere you go." [Online]. Available: http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

[5] M. Bancroft, "Using personalization to stimulate demand for mobile services." [Online]. Available: http://technews.tmcnet.com/business-phone-service/topics/enterprise-mobile-communications/articles/62561-using-personalization-stimulate-demand-mobile-services.htm

    Matt Bancroft talks about the mobile market and why there is a demand for mobile applications and advertisement.

[6] C. Beaumont, "ios4: Apple to start collecting user location data." [Online]. Available: http://www.telegraph.co.uk/technology/apple/7845853/iOS4-Apple-to-start-collecting-user-location-data.html

[7] "Apple's bussiness values." [Online]. Available: http://channelprograms.apple.com/channel/

[8] "Deception." [Online]. Available: http://legal-dictionary.thefreedictionary.com/deception

[9] "Deontological ethics." [Online]. Available: http://iml.jou.ufl.edu/projects/Spring02/Holt/deontological.html

    Deontological Ethics

[10] W. Fento, "How to see the secret tracking data in your iphone." [Online]. Available: http://www.pcmag.com/article2/0,2817,2383943,00.asp

    William Fenton talks about how Apple collects and uses geo-locational points to build a database which may help application run quickly.

[11] "Gartner says grey-market sales and destocking drive worldwide mobile phone sales to 309 million units; smartphone sales grew 13 per cent in third quarter of 2009." [Online]. Available: http://www.gartner.com/it/page.jsp?id=1224645

[12] P. Gralla, "Invade your privacy? apple has an app for that." [Online]. Available: http://blogs.computerworld.com/16483/invade_your_privacy_apple_has_an_app_for_that

Gralla talks about questionable practices of large companies specially those of Apple. He states that Apple collects real-time user information and shares them with advertisement companies. In addition, Apple under their privacy terms and condition clearly state, "[they] intends to use the data, and which Apple partners and licensees gets to share the data," which many people don't read.

[13] K. Gullo, "Apple accused in suit of tracking ipad, iphone user location." [Online]. Available: http://www.bloomberg.com/news/2011-04-25/apple-accused-in-suit-of-tracking-ipad-iphone-user-location-1-.html

[14] T. Haselton, "Apple exec to senate: apple does not track users locations." [Online]. Available: http://www.bgr.com/2011/05/10/apple-exec-to-senate-apple-does-not-track-users-locations/

[15] M. Helet and K. J. OBrien, "Inquiries grow over apples data collection practices." [Online]. Available: http://www.nytimes.com/2011/04/22/technology/22data.html?partner=rss&emc=rss

The article talks about the controversy of security of Apple products. It states that Apples use of users' personal information were unlawful since the information was marketed without the client's consent.

[16] "iphone applications & privacy issues:an analysis of application transmission of iphone unique device identifier." [Online]. Available: http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf

A research paoer by Eric Smith talks about Apple hardware devices being given a specific ID number that can be used to track device users' download and personal history.

[17] "itunes store terms and conditions." [Online]. Available: http://www.apple.com/legal/itunes/us/terms.html

iTunes terms of service. These are what every user of the iTunes store must agree to. They do not explicitly say that Apple may remotely remove software.

[18] Jeff, "Apple sued amidst privacy concerns regarding app tracking." [Online]. Available: http://www.iphonedownloadblog.com/2010/12/28/apple-sued-amidst-privacy-concerns-regarding-app-tracking/

On December 23, 2010, Apple was suit since transmission of personal information violates federal computer fraud and privacy laws.

[19] "Kant and the categorical imperative." [Online]. Available: http://members.fortunecity.com/rsrevision/kantandthecatimp.htm

Kant's theory of ethics: Moral Duty, Moral Statement, Good will and duty, and categorical imperative.

[20] "Kantian deontological system."

Describes Kantian Deontological System

[21] "Kant's moral philosophy." [Online]. Available: http://plato.stanford.edu/entries/kant-moral/

A good guide to Kant's moral philosophy, explaining his principles and believes.

[22] "Lalo vs. apple." [Online]. Available: http://www.scribd.com/doc/46073399/Lalo-v-Apple-Complaint

[23] M. Maisto, "Apple tops mobile pc rankings when ipad is included: Displaysearch." [Online]. Available: http://www.eweek.com/c/a/Desktops-and-Notebooks/Apple-Tops-PC-Rankings-When-iPad-is-Included-528131/

Masito talks about the leader of Mobile market during the Fourth Quarter of 2010. This was the year when Apple sold 4.13 million Macs and 7.33 million iPads

[24] "Many android apps leak user privacy data." [Online]. Available: http://pcatt.net/NewsEvents/tabid/76/articleType/ArticleView/articleId/165/Many-Android-Apps-Leak-User-Privacy-Data.aspx

Talks about a reported presented by NetworkWorld were researchers found permitted apps transmit phone numbers, location, and SIM card IDs to outside sources.

[25] "Mobile app stores set for solid 2011 growth." [Online]. Available: http://news.radio-electronics.co/manufacturing/mobile-app-stores-set-for-solid-2011-growth/

App Store this year is projected to bring in a revenue of $2.91 billion due to Apple devices such as the iPhone, iPod, and iPad are the leading the mobile market.

[26] T. Moccia, "Apple sued over app privacy." [Online]. Available: http://www.technobuffalo.com/companies/apple/apple-sued-over-app-privacy-2/

Jonathan Lalo filed a class suit complaint against Apple and serveral applications claiming that they violated federal computer fraud and privacy laws.

[27] R. Myslewski, "Apple slapped with ios privacy lawsuit." [Online]. Available: http://www.theregister.co.uk/2010/12/28/apple_privacy_lawsuit/

Myslewski presents large number of complains being made by customers about Apple products being untrustworthy. He states that Apple aren't concerned about user privacy since they collect and share user information and well as other applications that are available in the iPhone Market.

[28] M. D. of Florid Tampa Division, "Us district court cases of ajjampur and devito vs. apple. inc." [Online]. Available: http://www.wired.com/images_blogs/gadgetlab/2011/04/applesnoop.pdf

[29] "Respect." [Online]. Available: http://dictionary.reference.com/browse/respect

Used to define the term respect

[30] P. Roberts, "Pandora mobile app transmits gobs of personal data." [Online]. Available: https://threatpost.com/en_us/blogs/pandora-mobile-app-transmits-gobs-personal-data-040611

Roberts talks about the ethical practices of Pandora selling users' private information. The article further goes on to discuss about the "Grand Jury investigation into loose data privacy practices in the mobile application market."

[31] S. Schroeder, "1 in 5 android apps pose potential privacy threat." [Online]. Available: http://mashable.com/2010/06/23/android-apps-privacy-threat/

Author Schroeder talks about the false statement made by Google stating that "Android users' have control over permission being given to applications. Schroeder uses the facts of SMobile security company finding that "Android apps request permission to access private or sensitive information" to attack Google.

[32] B. Segalis, "Mobile location privacy opinion adopted by europe's wp29." [Online]. Available: http://www.infolawgroup.com/tags/apple-1/

Europe's Working Party adopt the WP29, sets of opinions regarding privacy compliance guidance for mobile geolocation services.

[33] T. Shields, "Mobile apps invading your privacy." [Online]. Available: http://www.veracode.com/blog/2011/04/mobile-apps-invading-your-privacy/

Veracode research team took apart in breaking various accused applications to see what type of information was being sold of to advertisment agency.

[34] "Software engineering code of ethics." [Online]. Available: http://www.acm.org/about/se-code

The Software Engineering Code of Ethics is the basis upon which this paper is written.

[35] A. Staff, "Apple already hit with lawsuit over ios location tracking file." [Online]. Available: http://www.appleinsider.com/articles/11/04/25/apple_already_hit_with_lawsuit_over_ios_location_tracking_file.html

[36] S. Thurm and Y. I. Kane, "Your apps are watching you." [Online]. Available: http://www.techgearx.com/wall-street-journal-says-apps-may-violate-privacy-fingers-myspace-and-pandora/

The article talks about how Pandora used its user' granted permission to access users' personal information such as phone numbers, current location, and phone unique id.

[37] "Utilitarianism." [Online]. Available: http://www.qcc.cuny.edu/socialsciences/ppecorino/introtext/Chapter%208%20Ethics/Utilitarianism.htm

An explanation of Utilitarian ethics. Useful in analyzing problems like the one this paper deals with.

[38] M. Yam, "Why apple is tracking your iphones and ipads." [Online]. Available: http://www.tomsguide.com/us/apple-tracking-iphone-ipad-location,news-10942.html

Marcus Yam gives reasons into why Apple collects user's geo-location points from its iPhone and iPad devices. This data helps improve the performace of location service applications.