2015

The spy in your pocket: Smartphones and geo-location data

Krishnun Sansurooah
Security Research Institute, Edith Cowan University, k.sansurooah@ecu.edu.au

Bradley Keane
Edith Cowan University, bakeane@our.ecu.edu.au

DOI: 10.4225/75/57b3fb68fb88e
13th Australian Digital Forensics Conference, held from the 30 November – 2 December, 2015 (pp. 95-103), Edith Cowan University Joondalup Campus, Perth, Western Australia.

THE SPY IN YOUR POCKET: SMARTPHONES AND GEO-LOCATION DATA

Krishnun Sansurooah[1,2], Bradley Keane[1]
[1]School of Computer and Security Science, [2]Security Research Institute
Edith Cowan University, Perth, Australia
k.sansurooah@ecu.edu.au, bakeane@our.ecu.edu.au

Abstract

The integration of Global Positioning Systems and Smartphones has seen the significance of location based services rise. Geo-location data could prove to be an invaluable source of evidence in a forensic investigation. An attempt to extract geo-location data from an iPhone4s and Huawei Ascend G526 in a forensically sound manner revealed significant geo-location data embedded within geo-tags within photos taken on the devices. Other limited evidence was located on the devices.

Keywords
Smartphone, Geo-location data, Global positioning systems, Location based services, digital forensics.

INTRODUCTION

The rapid adoption of smartphones has changed with way we communicate. Smartphones perform far more functions than that of their earlier counterparts and are similar to a desktop computer. The types of data contained within mobile devices is constantly evolving and includes, call history, sms, mms, calendar, email, photos and internet browser history (M2 Presswire, 2012). The introduction of Global Positioning Systems (GPS) into smartphones has further contributed to the range of services available. GPS allows for satellite navigation, geo-location based social networking, personal sports performance tracking, and geo-location targeted advertising. GPS also allows for a smartphone to be located when lost or stolen. Smartphones contain a wealth of valuable information, and with the introduction of GPS into these devices, geo-location data may have significant forensic value in legal proceedings.

As such this analysis will seek to identify how GPS and location based services are used within smartphones and identify any digital artefacts' that are contained within in smartphones. In order to achieve this an attempt will be made to recover geolocation data in a forensically sound manner from an Apple iPhone 4s (iOS) and a Huawei Ascend G526 (Android platform). A comparative analysis will be undertaken to see any variations in geolocation data that is recorded between the two devices.

GLOBAL POSITIONING SYSTEM

Hannay (2009) identified that TRANSIT was the first known Global Positioning System, developed to provide location data to the US Navy's Polaris submarine forces. Use of the TRANSIT network commenced in 1963 and with competing interest between the US Navy and US Air force in the use of this technology led to the implementation of the NAVSTAR network.

NAVSTAR satellites were launched in the 1970's and were designed as a system to be shared between military and civilian users. However in order prevent potential enemies of the United States of America from accessing precise location data the civilian signal was degraded, also referred to as 'selective availability leading to variations of up to 500m (Hannay, 2009).

As a result of the cold war the USSR created their own satellite navigation network known as GLONASS. This network become available for civilian use in 1995. It was not until 2000 that selective availability in the NAVSTAR network was set to zero which made the technology feasible for use in a range of commercial contexts (Hannay, 2009).

How Global Positioning Works

The GPS network consist of more than 30 satellites, equally spaced in different orbital plans approximately 20 00 kilometres above the Earth, that transmit signals to earth. GPS receivers process these signals to compute the latitude, longitude, of the GPS receiver. In order for GPS to work effectively, the receiver needs a clear view of the sky and signals from at least three satellites, these three satellites are used to pinpoint the location of the receiver through the process of trilateration (Dujuknic, 2001).

Implementation of GPS

The use of GPS is now widespread and is used in varying contexts which include;

- Navigation by road, air, and sea
- Tracking cargo
- Tracking of vehicles
- Tracking of convicted criminals
- Geo-tagging photographs
- Personal health tracking equipment
- Incorporation into mobile phones (Hannay, 2009)

The implementations of GPS are wide spread and offer a significant number of benefits. The incorporation of GPS into mobile phones has provided users with the ability to access a number of services that previously did not exist. Mobile phone users are able to gain access to local traffic information, turn by turn directions to their chosen destination, information about restaurant, hotels and other services within proximity to their current location (Hannay, 2009).

Assisted GPS

With the implementation of GPS into mobile phones it was possible to further enhance the technology with the introduction of Assisted-GPS (AGPS). AGPS uses the cellular mobile phone network to speed up the process of finding the location of a device (Zandbergen, 2009).

Mobile phone operators divide geographical areas into cells, within each cell is a base station, which communicates with individual handsets within the cell area. This information helps to identify the location of a phone user, by identifying the cell area they are currently in. Once this is known, information is relay to the mobile about which satellites it should be visible to in the sky, allowing the device to search for signals from specific satellites which should be visible. AGPS is particularly useful in urban areas where environmental factors can inhibit communication between satellites and receivers (Zandbergen, 2009).

LOCATION BASED SERVICES

Location Based Services (LBS) use location information to deliver services to the user to provide value. Generally Location Based Services are overt in nature and users consent to the disclosure of their location and are provided with information regarding how their information will be used. The user is also generally provided with the option to decline to participate in the sharing of location data.
Location Based Services are quite diverse, and websites and applications which provide information to users based on their location. These include services that provide information on maps, restaurants, entertainment, targeted advertising and social networking.

Location Based Services and Mobile Devices

With the rise of smartphones and the incorporation of GPS into these devices, Location Based Services continue to grow in significance. Apple's iPhone (iOS) and Google's Android dominate the smartphone market. Both of these companies have come under the spotlight in the past for the ways in which they collect and store location data (Chow, 2013).

Apple was highly criticised as location data was stored on the device and then transferred to a computer when synced and backed up. Apple denied using this information to track the locations of iPhone's, and identified that the industry had failed to educate users about the complexities of location based services (Chow, 2013).

In Google's case when Google Street View cars as they drove around and took photos of houses, recorded the street address, the locations of Wi-Fi access points and the individual Media Access Control (MAC) address for each access point. They then made this information publicly available on their website. Whilst Google indicated that they would not do this again, this information is sent to Google through the use of Android devices (Chow, 2013).

Apple's Location Services

Apple identifies in its support information that with the users permission, location services will allow apps and websites to use cellular, Wi-Fi, GPS and Bluetooth to determine their approximate location. These services include:

- Maps
- Camera
- Find My iPhone
- Traffic
- Popular Near Me
- Frequent Locations
- Location Based iAds
- Spotlight Suggestions
- Location Based Alerts
- Share My Location (Apple, n.d)

Google's Location Services

Google identifies in its support information that it seeks to provide users with useful information based on where they have been with their device, when signed in to their Google Account. Such as predictions related to future frequent commutes and better search results. Additionally location information can be used by third party apps to provide similar service. Google also identifies that location services can be turned off and location history deleted (Google, n.d).

Third Party Applications

Numerous third party applications provide location based services, the following specific services have been examined due the popularity:

- Facebook
- Twitter

Facebook is a social networking service and identifies in its privacy policy that it collects information about the hardware and software being used on devices used to access Facebook. It also collects specific information relating to geographic locations through GPS, Bluetooth and WiFi, (Facebook, n.d).

Twitter is a social networking service and identifies that it may receive information about a user's location through the use of GPS, wireless networks, cell tower information and a user's IP address. Twitter also indicates that location data may be used to provide recommendations about services they offer. A person may also reveal information about their location if they choose to share it in the publication of tweets (Twitter, n.d)

Location Based Services and Privacy

Once the most common concerns expressed about Location Based Services is in relation to privacy. Privacy concerns include, how service providers store and use the information they obtain in relation to individual users and also the risks associated to individuals who inadvertently disclose their location (Hannay & Baatard, 2011).

The defence that is often used to counter these concerns, is that users can choose to turn Location Based Services on or off. Hannay & Baatard (2011) argue however that users often communication location based information about themselves unaware that they are doing it.

An example that highlights this is that of Taliban spokesman Zabihullah Mujahid who accidentally turned on Twitter's geolocation tracking in posts he made on the social networking service. To the surprise of those interested in his whereabouts these post showed that he was in Sindh, Pakistan instead of Afghanistan (Noak, 2014).

The value of geo-location data

Geo-location data has the potential to be invaluable in legal proceedings. It provides a means of placing a person at a particular location at a particular time. This information could either place a person at the scene of crime or provide them with an alibi.

A number of cases have come before the courts in which evidence obtained for a GPS receiver has been tendered into evidence to establish relevant facts in a given case. Two notable cases are those of Pownceby and Simotosas, in both case both men produced evidence from GPS receivers in defence of speeding fines that they were issued by Police (Hannay, 2009).

Location information from mobile phone cell towers was used to convict Mr Phuong Ngo of the murder of NSW Politician John Newman. The soundness of the verdict was questioned in this case as a result of the use of this evidence and the supporting expert witness testimony. Whilst GPS data was not available in the trial of Phuong Ngo, these examples identify potential uses for geolocation data from mobile devices (Coutts & Selby, 2008).

MOBILE FORENSICS

Evidence extracted from mobile phones is increasingly being used in legal proceedings and Al-Zarouni (2006) suggests that there has been an explosion in the use of mobile forensics, in order to prove necessary facts in legal proceedings.

The primary aim of a forensic examination is obtain evidence in a forensically sound manner, so that the extracted evidence can be admitted into evidence in legal proceedings. Alghafli, Jones and Martin (2011) identify the following types of evidence that can extracted from smartphones:

- Phonebook/Contact information
- Calendar information
- Text messages
- Outgoing, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging
- Web browsing activities
- Electronic documents
- Social media related data
- Application related data
- Location information
- Geolocation data

However gathering evidence from mobile devices brings a number of significant challenges. These challenges include, the large variety of mobile devices in the market, proprietary operating systems, embedded file systems, numerous applications, and various connections. Additionally the tools available for forensic analysis vary in their ability to support all of these devices and the extent to which they support the range of devices in the market (Murphy, 2009).

In order to ensure that evidence contained within mobile devices remains forensically sound Wilkinson & Haagman (2010, p.46) in The Good Practice Guide for Computer-Based Electronic Evidence identify four guiding principles. These principles are listed below:

1) "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court."

2) "In circumstance where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions."

3) “An audit trail or record of all processes applied to the computer-based electronic evidence should be created and preserved. An independent third party should be able to examine the processes and achieve the same result.”

4) “The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and the law and these principles are adhered to.”

Mobile Forensics Process

According to Alghafli, Jones and Martin (2011), they identified the following four stages in a forensic investigation:

1) Preservation
2) Acquisition
3) Examination and Analysis
4) Presentation

In the preservation stage, the aim is to preserve the evidence in the state in which it is found. In mobile forensics there are a number of challenges associated with preserving the evidence. If a mobile device is on when discovered services on the device may allow for the device to be remotely wiped, destroying any evidence on the device. Additionally any loss of power will result in changes to the device, and if access locks are enabled it may result in prevention of access to the device in the future (Murphy, 2009).

Whilst a device is on it is susceptible to change as it continues to receive signals from the network. For that reason it is essential to isolate the device from the network as soon as possible. This can be achieved by placing the device in an RF shielded bag or by using the graphical user interface and activating flight mode (Murphy, 2009).

In the acquisition stage the forensic examiner identifies the mobile device and determines the best tools to be used to acquire an image of the device. Once an image of the device has been acquired efforts can be made to examine and analyse the evidence (Alghafli, Jones and Martin , 2011).

In the examination and analysis phase the forensic examiner utilises previously identified tools to analyse the evidence acquired form the device. Once the evidence has been analysed the forensic examiner must present this evidence in a way that it can be easily understood (Alghafli, Jones and Martin , 2011).

There are a number of methods for extracting evidence from a mobile device this include;

- Manual
- Logical
- Physical
- JTAG/Chip-Off
- MicroRead (Murphy, 2009).

A physical copy or bit by bit copy of the device is highly desired, as it allows for the recovery of deleted data. However in order to obtain a physical copy of a device it is essential to obtain root or super user access on the device. A number of methods exist to obtain root or super user access however if these methods result in permanent changes being made to the device which would render the evidence as inadmissible. A number of exploits have been developed which allow a physical copy of a device to be obtained. As these are temporary and do not result in a permanent change to the device they are considered to be forensically sound (Hoog, 2011).

Where it is not possible to obtain a physical image of a device, a logical image may still provide sufficient evidence to establish a set of facts. A logical image only obtains a portions of data available with the devices files (Hoog, 2011).

Manual examinations of devices are discouraged as actions taken on the device may result in altering the evidence. For example if a text message that was unopened is opened and later relied on to establish that the message was received by a person (Hoog, 2011).

JTAG and Chip-Off or are both physically invasive methods of obtaining evidence from a device and require opening the device. Whilst they both can result in obtaining physical image of the device, the device must be damaged and altered in order to gain the evidence (Hoog, 2011).

DESIGN AND SEARCH FOR GEO-LOCATION ARTIFACTS

In order to identify if geo-location data could be recovered from mobile devices both an Apple iPhone 4s and Huawei Ascend G526 were forensically examined using a combination of commercial and open source mobile forensics tools.

These tools included;

- Santoku Linux – Aflogical, Exif Tool, and IphoneBackupAnalyzer2
- viaExtract – NowSecure
- Mobile Phone Examiner – AccessData
- MOBILedit Forensic Lite 7.5

Both the devices were used over a two week period and seeded with data including, calls, messages, photographs, internet searches, map searches, Facebook, and Facebook messenger.

Both devices were fully charged, and were imaged on the same day and were isolated from the network to prevent modification.

The Examination Process – Apple Device

A logical image of the iPhone 4s was obtained using Mobile Phone Examiner. Efforts were made to obtain a physical copy of this device using this program but they were unsuccessful. Mobile Phone Examiner provided a report of the logical information extracted from the device and allowed for the logical files to be examined within the program.

Efforts were made to examine the device using MOBILedit Forensic Lite 7.5 however, the program continually reported a connection error preventing extraction. Similarly efforts to create a backup of the iPhone using Libimobiledevice within Santoku Linux were unsuccessful, and repeatedly returned an error.

iTunes was used to create a backup of the iPhone that was been investigated. Prior to connecting the device to create the backup, necessary precautions were taken to disable the automatic syncing. This approach was selected to prevent iTunes from modifying the iPhone at any point in time. Once the backup of the device was created, it was then used and through the forensics workstation, it was examined and analysed with both MOBILedit Forensic Lite 7.5 and IphoneBackupAnalyzer2.

The following files extracted from the device were examined for evidence of geo-location data;

- AppDomain > com.apple.maps
- Library/Maps > GeoBookmarks.plist
- MSPFAILEDSEARCH
- Library/Preferences > com.apple.maps
- RootDomain > Library/Cashes/locationd > Consolidated.db & GyroCal.db

In addition, the files within AppDomain relating to Facebook and Facebook messenger were examined and analysed for evidence of any geolocation data. All photos that were recovered from the device were examined using the Exiftool within Santoku Linux.

The Examination Process - Android Huawei Ascend G526

A review of the compatible devices list in Mobile Phone Examiner identified that the device was not able to be imaged by the program. Functionality exists within the program to gain an Android Physical copy of devices. An attempt was made to obtain a physical copy of the device using this program but this was unsuccessful.

Aflogical was used within Santoku Linux to obtain a logical copy of the contents of the device. viaExtract was used in order to obtain evidence contained on the device. viaExtract provides a function which utilises a temporary exploit for Android devices to gain a physical copy of the device. Attempts were made to utilise this exploit and whilst this was ultimately unsuccessful it appeared to show promising signs, however viaExtract crashed repeatedly whilst trying to use this function.

MOBILedit Forensic Lite 7.5 was also used and was able to obtain a logical back up the devices content. All photo’s recovered from the device were examined using the Exiftool software within Santoku Linux.

RESULTS

Apple (iPhone)

The performance of each of the tools varied in their acquisition of the device. None of the tools were able to obtain a physical copy of the device. However logical evidence extracted from the device was still beneficial to the investigation.

Within the GeoBookmarks.Plist file, two geo-location searches that were done in the phone were located these were;

- South St Kogarah NSW
- Aldi Grafton Casino

Within the MspFailedSearch a search was found for StanhopeGardens Leisure Centre.

However no time or date stamps could be associated with these searches.

In the System Preferences > System Configuration file the following details were able to be extracted about WiFi connections which the device had been associated with.

SSID	BSSID	Last Connection
Dogpatch6 - Investigator's Network		10 May 2014 11:27AM
Target Wifi	e8:ba:70:31:60:	3 May 2015 4:23:16
Castle Towers Free Wifi	cc:b2:5:8d:6:90	3 May 2015 2:19PM

Table 1. Shows the Wi-Fi connections details which the devices been associated with. .

Photographs taken with the devices camera revealed geolocation data and time and date stamps embedded within the EXIF data.

Android Huawei Ascend G526

No geo-location data could be located within the Android file system. Information related to WiFi connection were able to be identified through the use of MOBILedit Forensic Lite 7.5.

Photographs taken with the devices camera revealed geolocation data and time and date stamps embedded within the EXIF data.

DISCUSSION

The greatest source of geo-location data in this analysis was extracted from photos from both devices which had associated geo-tags. This information allowed places and times the device had been to be correlated with activities the device user was engaging in at the time of use. This may prove helpful in any reconstruction of the times, places and activities a person has been.

The calendar was able to be recovered for both devices, information within calendar entries identified time, date and location of activities the user had been involved in and was to be involved in within the future.

The inability to gain root access and obtain a physical copy of the devices may have adversely impacted on the ability to identify geo-location data within the devices. Whilst some geo-location data was able to be identified within the iPhone 4s, the absence of time and data stamps would likely hinder its use as evidence in legal proceedings.

CONCLUSION

The introduction of Global Positioning Systems, and Smartphones and their integration has revolutionised the significance of location based services (M2 Presswire, 2012). These services seek to provide users with value by providing them with information and services based on their current location. However, privacy concerns are cited as one of the biggest criticisms within the use of location based services. Providers of these services argue that user are provided with the option to either turn these services on or off if they do not want to share

information about their location. However users frequently inadvertently disclose information about their location (Hannay & Baatard, 2011).

With the presence of features like location based services, the forensic examination of an Apple iPhone 4s and Android Huawei Ascend G526 was undertaken using various mobile forensics tools to identify if geo-location data could be found within the devices. Therefore, the examination revealed that photographs taken with the devices camera's left geo-tags within EXIF data, which identified the date, time and location where the photo was taken. Other types of information extracted from the devices such as the calendar dates and schedule also revealed geo-location information.

Whilst some information about location searches was identified within the iPhone it is considered that without specific date and time stamps this information would unlikely be value in legal proceedings. Failure to obtain a physical copy of both devices, was identified as a possible barrier to obtaining this data. However ensuring that the forensic integrity of the evidence was maintained was a key aim of this investigation which maintained the integrity of the experimentations that were carried out.

REFERENCES

Apple, (2015). About privacy and Location Services using iOS 8 on iPhone, iPad, and iPod touch. Retrieved from https://support.apple.com/en-au/HT203033.

Alghafli, K. A., Jones, A., & Martin, T. A. (2011). Guidelines for the digital forensic processing of smartphones. Retrieved from http://ro.ecu.edu.au/adf/90

Coutts, R., & Selby, H (2008). The Safe and Unsafe Use of Mobile Phone Evidence. In Record of the Communications Policy & Research Forum 2008 (p. 316).

Djuknic, G. M., & Richton, R. E. (2001). Geolocation and assisted GPS. Computer, 34(2), 123-125.

Brunty, J., Miller, L., & Helenek, K. (2014). Social media investigation for law enforcement. Routledge.

Chow, R. (2013). Why-Spy: An Analysis of Privacy and Geolocation in the Wake of the 2010 Google Wi-Spy Controversy. Rutgers Computer & Tech. LJ, 39, 56.

Djuknic, G. M., & Richton, R. E. (2001). Geolocation and assisted GPS. Computer, 34(2), 123-125.

Facebook. (2015). Data Policy. Retrieved from https://www.facebook.com/about/privacy/

Google. (2015). Manage and delete your Location History, Retrieved from https://support.google.com/accounts/answer/3118687?hl=en

Hannay, P. (2009). Satellite navigation forensics techniques. Retrieved from http://ro.ecu.edu.au/adf/62/

Hannay, P. (2013). Geo Forensics: Classes of Locational Data Sources for Embedded Devices. Retrieved from http://ro.ecu.edu.au/ecuworks2013/603/

Hannay, P., & Baatard, G. (2011). GeoIntelligence: Data mining locational social media content for profiling and information gathering. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.214.3970

Hoog, A. (2011). Android forensics: investigation, analysis and mobile security for Google Android. Elsevier

Jenkins, L. R., & Gan, D. E. (2011). Investigation into Privacy Issues of Using Social Media. Retrieved from cms1.gre.ac.uk/research/csafe/publications/JenkinsGan-CFET2014.pdf

Murphy, D. C. A. (2009). Developing process for mobile device forensics. Retrieved from http://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf

Noack, R. (2014, Oct 07). How twitter's geolocation settings embarrassed the taliban. Washington Post – Blogs Retrieved from http://ezproxy.ecu.edu.au/login?url=http://search.proquest.com/docview/1609292562?accountid=10675

RNCOS, (2013). Smartphones to drive stronger GPS growth. Retrieved from http://www.rncos.com/Press_Releases/Smartphones-to-Drive-Stronger-GPS-Growth.htm

Twitter, (2015). Twitter Privacy Policy. Retrieved from https://twitter.com/privacy?lang=en

Wilkinson, S., & Haagman, D. (2010). Good practice guide for computer-based electronic evidence. Association of Chief Police Officers. Retrieved from http://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/

Zandbergen, P. (2009) Accuracy of iPhone Locations: A Comparison of Assisted GPS, Wi-Fi and Cellular Positioning, Transactions in GIS, 13(s1): 5–26.

Retrieved from http://www.researchgate.net/profile/Paul_Zandbergen/publication/227652878_Accuracy_of_iPhone_Locations_A_Comparison_of_Assisted_GPS_WiFi_and_Cellular_Positioning/links/0912f50f50eb1005a4000000.pdf