CMP416 Digital Forensics 2

Jack Bowker - 1803838

In the field of mobile forensics, what are some of the key challenges facing law enforcement?

Investigating the potential impact of different privacy features of iOS and Android on mobile forensics and law enforcement.

Mobile phones are quickly becoming the primary devices for more and more people, as modern devices are able to fill most of the basic functions desktop computers or laptops were traditionally used for. As of October 2020, it's shown for example that 79.9% of users worldwide exclusively access Facebook using a mobile device (Statista, 2020). As mobile technology becomes widely adopted and, in most countries, mostly unanimous. Mobile forensic techniques are rapidly evolving due to the fast pace of mobile technology, but despite this the challenges are different due to the major differences in the security architectures of mobile devices. For example, one of the major differences is the fact that Full Disk and File Based Encryption are near universal on recent phones. This means the traditional methods of static imaging used on PCs are less useful as files are only unencrypted after the user's passcode is entered after a reboot (Afonin, 2019). As of 2020, according to Stat Counter data Google and Apple have a near duopoly on smartphone Operating Systems with a combined 99% share of devices, with Android making up 72% and Apple 26% respectively. This exemplifies the importance of the default preferences and features of these platforms as they make up such a large portion of the market.

The aim of this essay is to research the challenges for law enforcement of the different privacy approaches the two major mobile operating systems take. Specifically, this report will look to compare the different default settings and features of Apple's iOS and Google's Android to see if the companies claims about privacy are true, as well as looking into the amount of on-device processing done versus cloud based, along with the attitude and process each platform takes to storing this data. Along with this, the amount of data generated on each platform will be looked into, for example how a Google or Apple iCloud account could tie together possible evidence.

With mobile devices near universal worldwide, the two biggest mobile Operating Systems differ on their approach on how privacy should be handled. Smartphones in general are storing more and more personal data as time goes on and they replace wallets, calendars and computers. Google and Apple take quite significantly different stances on how they deal with the collection of user data in their products. Google for example offers advanced artificial intelligence features in their cloud-based Google Photos app and for articles to be recommended to users in Google News based on their search and browsing history. Along with this, Google has the incentive to target relevant ads to users since they own the Google Ads platform, the biggest online advertising marketplace in the world.

On the other hand, Apple has focused on letting users know with an advertising campaign that "What happens on your iPhone stays on your iPhone" (Savov, 2019) and emphasises that they aren't interested in targeting users. This theme of privacy ties into the company's controversial decision in 2015 after the San Bernardino terrorist attack, where after killing multiple people and dying in a shootout with police, the Federal Bureau of Investigations acquired the work phone of one of the attackers. The FBI requested for Apple to create a backdoor into this phone, as it was protected by a 4 digit passcode that after 10 incorrect attempts would wipe the device. Apple made a public response to this request, stating that the potential risk to customer privacy with a purpose built backdoor is too large for them to take. This difference in approaches results in the platforms collecting different amounts data on users and storing it in different places.

One of the best areas to see this difference is in the way each Operating System deals with location data, as both of them by default track locations visited by the user. Both Apple's Significant Location and Google's Location History feature periodically locates the mobile device and stores co-ordinates, along with a timestamp and what mode of transport it guesses was used. Apple's Significant Locations feature will use this data in conjunction with machine learning to customize how the device works, including suggesting apps when a user is at certain locations, or enabling optimized battery charging by learning when the user arrives and leaves home. Google's Location History will also use machine learning to suggest relevant applications, as well as suggesting nearby events and businesses. The main privacy difference between these two features is that on iOS, location data isn't readable by Apple as although this location data can be synced between an iPhone and a MacBook laptop or iPad for example meaning it runs through Apple's servers, in order to sync this data, 2 factors of authentication are needed – an Apple ID/Password for the account, as well as the Lock screen passcode used on the iPhone which Apple doesn't know, meaning the data can't be parsed by Apple.

In comparison with Google, movement information is similarly uploaded to Google's servers, but the platform provides an accessible web interface for viewing your movements meaning it is being parsed and is readable by Google. From a law enforcement perspective, this gives an additional avenue for investigation. Sensorvault is a tool created by Google specifically for law enforcement, which uses the aggregated location and movement information gathered from Location History to allow for geofence warrants, issued to determine who is located within a certain area at a certain time (Cohen, 2020). These warrants issued to Google allow law enforcement to access sensitive information if a device and therefore the person who owns it is deemed as suspicious. "It labels them with anonymous ID numbers, and detectives look at locations and movement patterns to see if any appear relevant to the crime. Once they narrow the field to a few devices they think belong to suspects or witnesses, Google reveals the users' names and other information" (Valentino-DeVries, 2019) In the past this has resulted in an innocent passer-by riding on a bike getting involved in criminal case due to having Google's location services active on their phone (Schuppe, 2020).

The default texting experience between the two platforms is another factor that could affect forensic investigations. The SMS protocol in use since 1992 (BBC News, 2002) remains mostly unchanged and although it's difficult to intercept messages in transit, once sent and received by the carrier these messages are readable. This method is used in law enforcement regularly in the UK as under the RIPA (Regulation of Investigatory Powers Act) carriers are required to store a years' worth of records. The iOS Messages application, when prompting to send a message to a contact, the phone will query Apple to see if the phone number is registered to another iPhone. If so, the message will automatically be sent using the more secure iMessage protocol, which includes end-to-end encryption. On Android, SMS is still the default for most users despite Google trying to push for the RCS (Rich Communication Service) protocol to become standard in their own Google Messages app. They are also planning to add end-to-end encryption to this but due to the saturation of mobile devices running Android it's unlikely this will become the default for the majority of users soon if ever (Bohn, 2020). Secure alternatives to text messaging are available on both platforms such as WhatsApp, but neither platform provides a way to backup WhatsApp data to the cloud whilst keeping it encrypted and unreadable by the platforms.

Pedometer and step data can be valuable in Forensic investigations for tracking movements and the intensity of this movement, and this has been used in high profile cases in the past. For example, proving someone was running away from a crime scene at a certain time. Some Android manufacturers offer this as an opt-in feature - Samsung Health will automatically turn on the step recording function "Once you've opened the Samsung Health app for the first time". On all iPhones since the introduction of the Apple motion coprocessor in 2013, step tracking has been enabled by default and is quite accurate "Steps registered by the iPhone Health App agree very closely to those measured manually with an averaged error of about 2%" (Zandwijk, 2019) making it more likely this data is available to be analysed on iOS devices.

A common criticism of Apple's public stance on protecting user privacy is that it's undercut by the fact that most users will end up installing Google services on their devices, anyway, enabling a lot of the same tracking to be done on iPhone users. For example, when Google Maps is installed the user will first be prompted to sign into their account to enable saved locations or downloading maps offline. After this they will be prompted to enable Location History as well as giving the app the "Always" location permission which allows for the same always on location data collection as Android. When asked about Google's Sensorvault by journalists, an intelligence analyst in North American law enforcement stated that "most Android devices and some iPhones" have this data available, confirming that the same data aggregation is being done on Apple devices. This has resulted in lawsuits between the two tech giants, where between 2011 and 2012 Google "collected data on health, race, ethnicity, sexuality and finance" through the Safari web browser, even while users had chosen the "Do not track" privacy setting. Google agreed to pay $22.5m USD in damages related to this in the United States.

Both companies encourage indulging in their respective ecosystems, with for example iPhone users more likely to use Apple's Email service and Apple Music streaming service. A potential advantage in law enforcement investigations on Android devices is the fact that the parent company Google is the preferred search engine for around 90% of internet users, that number being nearer 95% for Android users. Along with this, Google owns the biggest Email service Gmail. This results in a large portion of Android users spending much of their time on their device using Google services, increasing the amount of data available to warrants, of which Google gets issued more than 81,000 requests for data on nearly 175,000 accounts worldwide from July – December of 2019. Information on what is requested is publicly available from Google's Transparency Report, stating that Email content, private YouTube videos, along with text message and voicemail content is commonly requested information. Overall, the top down platform – offering services like free photo backups along with Google's detailed activity logs of search, app launch and location history, give a good picture of someone's digital life from a single online account. iCloud accounts are also accessible via warrant, with similar email/Photo data if a user enables these features, but this can't be tied to search history. Apple also publicises information about how it works with law enforcement and how it deals with warrants stating that from July – December 2019, over 31,000 requests for more than 159,000 devices were made similarly to Google, but Apple does not publicise which services are most commonly requested access to.

Another important aspect of how platforms deal with privacy is App Permissions. Grantable and revocable permissions allow the user to control which areas of the phone applications can access, and recent versions of Android and iOS allow control of these to varying extents. An ongoing privacy issue that has been taken advantage of by law enforcement in the past is users being careless about location permissions, and downloading apps that sell data such as location, contact information or other identifying information to the highest bidder. In the past, American law enforcement has taken advantage of apps such as "games, weather and e-commerce" to detect undocumented immigrants going through the United States border (Tau, 2020). iOS has had limited app permission management since iOS 4 in 2010, with the binary option to enable or disable location access to individual apps, in 2015 improving this with the permission either to allow access "Always" or only "When Using" an app. More recently in iOS 13 & 14 the ability to "Ask every time" location is requested was added along with the ability to give apps coarse cell location data instead of more accurate GPS data. Android added the ability to grant/revoke permissions to apps in 2015, with Android 11 rolled out in September 2020, privacy was a primary focus especially regarding third party apps. Along with updated location permissions similar to the iPhone's "When Using" and "Ask every time" location permissions, Android introduced "One time permissions" for device features like the camera, access to contacts, or location. Additionally, Android introduced a feature in version 11 that iOS doesn't yet have which results in the permissions for apps that haven't been used recently being revoked. This combined with the enhanced one time permissions mean that the likelihood of apps unknowingly sharing location data is much lower than with previous versions of the OS.

In mid-2018, Apple pushed out a software update to iOS 11.4 enabling a new feature called “USB Restricted Mode”, which when examined was built to stop Forensic firms such as Grayshift and Cellebrite from gaining entry to devices by disabling access to the device via Lightning cord without first entering the device’s passcode. These companies work with law enforcement in North America and around the world with Grayshift working directly with police forces in multiple US states, and since this update Apple has been in an arms race with Forensic firms finding new loopholes to extract data from devices, with iOS 13 containing another update to the protection (Katalov, 2019).

Due to the open nature of the Android platform, different manufacturers can implement their own applications and system features that in some cases improve the privacy and security of devices but can also result in manufacturers or carriers adding invasive bloatware or tracking into devices. For example, in 2017 Samsung introduced a “Secure Folder” feature, allowing users to store sensitive documents, images or applications in a secure enclave called Samsung Knox, which is an encrypted area of storage separate from other data on the phone. On the other hand, manufacturer-added applications have resulted in backdoors allowing malicious access to data on the phone, for example a vulnerability in a theming engine which needs a higher level of privilege in order to run being taken advantage of by a rogue theme, which grants access to administrator privileges on some Android devices (Schmidt, 2020).

Both Apple’s iOS and Google’s Android provide useful additional avenues for investigation respectively, but there are real world differences between how the platforms deal with this data and what exactly gets collected. Overall Google collects more user data due to the company’s business model of targeting advertising to individual users, which in turn enables projects like Sensorvault due to their ability to search their library of aggregate data, as well as their ability to deanonymize this location data when requested in order to assist with law enforcement. On the other hand, Android has made large strides towards limiting the access potentially malicious apps have on their platform with new permission management introduced in Android 11. Both platforms have vulnerabilities that vary but Apple appears to be making an ongoing attempt to stop Forensic firms using these to extract data from their devices with features like Restricting USB access, however due to Apple’s relative secrecy regarding the state of the security of their devices it’s never certain whether their devices are entirely secure. With physical access to the devices, extensive data can be gathered from both iOS and Android using techniques such as Logical or file system acquisition, however in regards to how the platforms differ, it appears that Google’s cloud and personalisation services result in more data available during investigations due to their top-down structure of owning both the Operating System as well as the internet services people use. With access to possibly decades of search history, photos, emails as well as more traditional SMS/voice data, it’s not something to be overlooked.

References

Afonin, O., 2019. *Challenges in Computer and Mobile Forensics: What to Expect in 2020.* [Online]
Available at: https://blog.elcomsoft.com/2019/12/challenges-in-computer-and-mobile-forensics-what-to-expect-in-2020/

BBC News, 2002. *Hppy bthdy txt!.* [Online]
Available at: http://news.bbc.co.uk/1/hi/uk/2538083.stm

Bohn, D., 2020. *Google is rolling out end-to-end encryption for RCS in Android Messages beta.* [Online]
Available at: https://www.theverge.com/2020/11/19/21574451/android-rcs-encryption-message-end-to-end-beta

Cohen, L., 2020. *What are geofence warrants and how can police use them against protesters?.* [Online]
Available at: https://www.dailydot.com/debug/geofencing-warrants-surveillance-police/

Katalov, V., 2019. *USB Restricted Mode in iOS 13: Apple vs. GrayKey, Round Two.* [Online]
Available at: https://blog.elcomsoft.com/2019/09/usb-restricted-mode-in-ios-13-apple-vs-graykey-round-two/

Savov, V., 2019. *Apple trolls CES with a giant dig at Android and Alexa privacy.* [Online]
Available at: https://www.theverge.com/2019/1/5/18169781/apple-google-privacy-troll-billboard

Schmidt, F., 2020. *Pre-installed malware: Your Android phone may spy on you!.* [Online]
Available at: https://www.dw.com/en/pre-installed-malware-your-android-phone-may-spy-on-you/a-52526377Pre-installed malware: Your Android phone may spy on you!

Schuppe, J., 2020. *Google tracked his bike ride past a burglarized home. That made him a suspect..* [Online]
Available at: https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

Statista, 2020. *Facebook access penetration 2020, by device.* [Online]
Available at: https://www.statista.com/statistics/377808/distribution-of-facebook-users-by-device/

Tau, B., 2020. *Federal Agencies Use Cellphone Location Data for Immigration Enforcement.* [Online]
Available at: https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

Valentino-DeVries, J., 2019. *Tracking Phones, Google Is a Dragnet for the Police.* [Online]
Available at: https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

Zandwijk, J. P. v., 2019. *The iPhone Health App from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence?.* [Online]
Available at: https://www.sciencedirect.com/science/article/pii/S1742287619300313