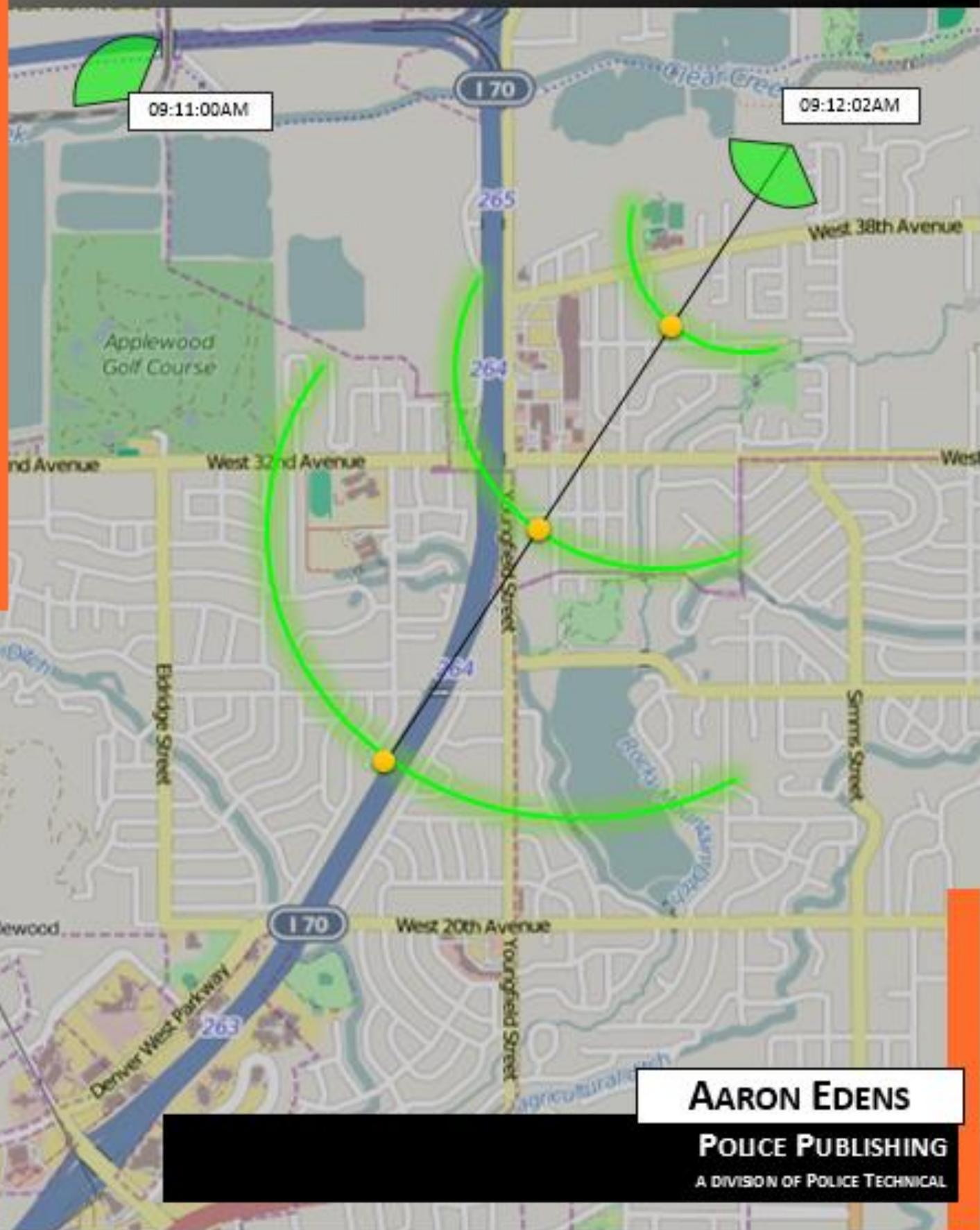


CELL PHONE INVESTIGATIONS



AARON EDENS

POLICE PUBLISHING

A DIVISION OF POLICE TECHNICAL

Note from the Publisher about the EVALUATION COPY

Thank you for downloading this evaluation copy of Cell Phone Investigations by Aaron Edens.

The following materials are excerpts (Table of Contents, Introduction and Chapter 1) from the upcoming book, Cell Phone Investigations by Aaron Edens, first in the “Cell Phone Investigations Series” from POLICE PUBLISHING, a Division of POLICE TECHNICAL.

At nearly 600 pages in length, Cell Phone Investigations’ first edition will be released in December 2014. Over three years in development, it represents the broadest examination of the subject yet to appear in print. Recently re-edited to include the summer 2014 Supreme Court rulings on Cell Phone Searches, it contains 11 Chapters ranging from Device Forensics to Cell Towers to Sample Search Warrants.

This evaluation copy is provided to U.S. law enforcement personnel for evaluation and comment.

If you would like to share your comments about this document please contact:

Brianne Hofmann
POLICE PUBLISHING, Editor
bhofmann@policetechnical.com
812-232-4200

Pre-Sale Orders

If you would like to purchase pre-sale copies of Cell Phone Investigations by Aaron Edens, please visit POLICEPUBLISHING.com or POLICETECHNICAL.com. The single distribution price will be set at \$65.00; the pre-sale order price is \$50.00. Presale orders will be taken until December 2015.

Thank you for reading the following excerpts from Cell Phone Investigations by Aaron Edens, and thank you for your interest in POLICE PUBLISHING.

Respectfully,

Thomas M. Manson
POLICE TECHNICAL, CEO
POLICE PUBLISHING, Publisher
tmanson@policetechnical.com

Table of Contents

Introduction	4
Chapter 1: Search Warrants	6
Before the commission of the crime?	8
During the commission of the crime?	8
After the commission of the crime?	9
Common Search Warrant and Affidavit Errors	9
Operating System Warrants: Google	16
Chapter 2: Phone Records	47
§ 2703. Required disclosure of customer communications or records	48
How about the assault and battery case?	57
Preservation Letters	62
Search Warrants	64
Chapter 3: Tools for Examining Records	80
Understanding How Providers Work	81
Cell Phones in Prisons	83
Call Detail Records (CDR)	84
AT&T Records	125
Using Cell Phone Data to Reveal Patterns	134
Specialized Records Searches	138
Calls -to -Destination Searches	141
International Phone Records	146
Caller ID Spoofing	149
Chapter 4: Cell Towers and Cell Sites	156
Cell Site Infrastructure	157
Site Identification	163
Mapping Cell Site Information	166

Cell Site Dumps	170
Mobile Phone Tracking	182
Per Call Measurement Data (PCMD)	184
Chapter 5: Cell Phone Forensics	199
Physical Evidence Preservation	202
Documenting Characteristics of the Phone	205
Preserving Electronic Evidence	209
Preventing the Phone from Communicating with the Network	209
Storing the Phone Evidence	217
Chapter 6: Digital Evidence	219
Call Logs	224
Calendar	224
Image Files	225
Graphic Files	235
Video Files	236
Text Messages	236
Memos or Notes	238
Voice Recordings	238
Internet Activity	239
Maps	239
Chapter 7: Types of Examinations	241
Basic Examination of Cellular Devices: SIM Cards	242
External Storage Media	250
Recovering Deleted Files	251
Imaging the Card	254
Recovery Tools	262
Chapter 8: Using Cell Phone Forensics	273
Cameras	274
Cables	276

Improvised (Free) Tools	276
Nokia PC Suite	278
Samsung PC Studio 7	291
Free Android Forensics Tool for Law Enforcement	291
Recoverable Data	292
Required Equipment and Software	293
Magic Berry by Mena Step Innovative Solutions	312
iOS Research	322
Paid Forensic Tools	324
Logical Versus Physical Forensic Examination Tools	325
Platform Specific Tools	340
Smartphones	340
Chapter 9: Locked Devices	345
Consent	345
Deception	346
Physical Screen Examination	348
Provider Unlock: Android Passcode Bypass Procedure	349
Provider Unlock: iPhone/iPad/iPod Touch Passcode Bypass Procedure	352
Properly Identifying the Device	353
Smartphone Passcode Bypass	359
Chip-Off	360
Chapter 10: iPhone Backup Files	363
Seizing the Backup File	365
Simple Mode	375
Expert Mode	395
Wide Angle Software's Ibackup Extractor	403
iBackup BoT	409
Chapter 11: Sample Search Warrants	426
Search Warrants	429

Pen Registers/Traps and Traces	432
Templates	434
Appendix	515
Regional Information Sharing Systems® (RISS) Nodes	515
RISS Centers:	517
CDR Indexes	518
High Intensity Drug Trafficking Areas (HIDTA) Program	519
Fusion Center List	536
Cell Phone Investigation	547
Index	551

Introduction

“If I have seen a little further it is by standing on the shoulders of giants.”

- Isaac Newton, 1676

The cellular phone forensics field is advanced by a small group of visionary and tenacious hackers, technicians, programmers, and code writers, some who are law enforcement and some who are not.

Evidentiary examinations of cell phones are a complex and often frustrating process. However, the rewards can frequently justify the time and costs associated with its procedure. This book will provide an introduction to the basics of cell phone forensic examination but is in no way a complete or comprehensive treatise. Cell phone forensics is a dynamic field and the available tools do not always keep up with technology, which is one of the constant challenges to those involved in forensic examinations.

The National Institute of Standards and Technology (NIST) in their 2007 report entitled Guidelines of Cell Phone Forensics states: “Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.” Unfortunately, cell phone technology rapidly outpaces the forensic sciences and often times there are no “forensically sound conditions using accepted methods” available.

Often cell phone forensics requires an examiner to use techniques that have not been evaluated as an “accepted method.” Frequently the examination technique involves the use of non-forensic methods such as using a manufacturer’s content management software, highly technical programming or repair tools, and third party software designed to modify the operating systems of phones.

Law enforcement has resisted the concept that a cell phone carries the same evidentiary weight as any other item of evidence or contraband. Perhaps it is the ubiquity that causes veteran investigators to treat a cell phone differently than a firearm or package of narcotics. Trends such as this only change course when a significant case is lost or an adverse legal precedent is established.

From physical evidence contained on the handset itself, to the digital evidence contained within the device, there is a wealth of evidence and intelligence to be recovered from even the most primitive cell phones. Combined with the information retained by the cell service providers, it is possible to glean critical insights into criminal activities and conspiracies that eluded earlier generations of law enforcement officers.

Writing a book is a challenge, particularly when the field involves the topics of law, technology, and forensic principals. My personal goal is to arm the reader with knowledge of the techniques and tools available in field of cell phone forensics, as well as, avoid the many pitfalls you may encounter in this new and ever-evolving field. I hope that by reading this book you will gain an insight into these various disciplines and be able to apply some of the investigative techniques into the noble profession of law enforcement.

I would like to express my gratitude to those who comprise the tip of the spear in the field of cell phone forensics. I would especially like to thank those who freely make their research, tools, techniques, and programs available to the law enforcement community.

One of the greatest aspects of being a police officer is the community that exist nationwide. I can think of no other occupation where a person can travel across the county and be immediately accepted by his or her counterparts. No other job or career sees the outpouring of support from departments and agencies across the nation when one of our brothers or sisters falls. Equally important is the sharing of information, techniques, and tactics. While I have tried to put to paper the best tools and methods, I eagerly await those that are discovered by others. If I can be of any assistance to you or you would like to share something not covered in this book, I invite you to contact me at aedens@policetechnical.com.

Stay Safe,
Aaron Edens

Chapter 1: Search Warrants

On June 25th 2014, the Supreme Court of the United States announced their decision in two cases, *People v. Wurrie* and *Riley v. California*. The result of those decisions requires a search warrant, or other valid warrantless search exception, before a mobile device may be searched. This decision presents unique challenges and opportunities for both veteran and entry level law enforcement officers.

The first challenge is writing the search warrant affidavit itself. For many law enforcement agencies, seeking a search warrant is the exclusive dominion of seasoned detectives, narcotics officers, and other investigators. However, the Supreme Court decision is likely to push the responsibility for seeking and executing search warrants for mobile devices down to the patrol level. Nearly everyone has a cell phone. A 2013 study by the Pew Research Center's Internet and American Life Project found that cell phone ownership among adults in the United States is 91%. Consequently, there is a statistical probability a criminal suspect will own a cell phone or other mobile device. There is also an increasing likelihood a cell phone or other device will be integral to the investigation of many crimes.

Cell phone investigations are a common investigative tool in conspiracy crimes investigations where communication between co-conspirators is an operational necessity. However, the use of a cell phone or other mobile device as a communication mechanism is not limited to these types of crimes. Certainly there are certain types of crimes where a mobile device is unlikely to be used, but those crimes are few and far between. Common criminal investigations involving the use of mobile devices include:

- Pedophiles using their mobile devices to communicate with and recruit victims and to store images, videos, and other mementos of their heinous crimes.
- Intoxicated drivers who communicate their location, plans, and intoxication level using social media, digital photos and videos displaying themselves in their intoxicated state, phone calls, and text messages from their mobile devices.
- Burglars targeting specific locations and communicating about the presence of alarm systems, dogs, street lighting conditions, access points, and egress routes.
- Organized retail theft 'booster rings' targeting specific stores and possessing digital 'shopping lists' of preferred items to steal and fence.
- Car thieves looking for specific makes and models of vehicles and describing the best way to steal them, as well as, communications regarding police pursuit policies in the area.

The fact nearly everyone has at least one cell phone or other mobile device coupled with their involvement in the nearly every major type of crime creates a need for proper search warrant preparation and procedure. For many law enforcement agencies it will not be sufficient to wait for the experienced detective to come in and write the search warrant. Not only will this burden an investigator with completing search warrant affidavits for which he or she has no direct knowledge, but it will rob the other officer of an incredibly valuable learning experience. Search warrant preparation is one of the key investigative tools in many law enforcement investigations. Once an officer has experienced the process a few times it becomes progressively easier and faster to complete one. Officers who might otherwise delay or abandon a case because a search warrant is required to advance the investigation will have increased confidence in their ability to seek, and be granted, a search warrant.

Law enforcement officers sometimes struggle with the proper nomenclature and technology for mobile devices. Many rely on search warrant templates or ‘boilerplate’ handed down from other investigators. Sometimes these ‘go-bys’ have not been updated to reflect the changes in technology. In some cases, they still refer to antiquated technology associated with rotary dial telephones and numeric pagers. To address the unique needs of a modern mobile device search warrant, it is helpful to start by addressing the correlation between the crime and the device.

Some crimes inherently require the use of mobile communication devices. For example, it is nearly impossible to be a successful narcotics dealer without the use of a mobile phone. Some crimes, such as those involving gangs, are inherently conspiratorial and require the use of electronic communications, frequently using mobile devices such as cell phones and tablets to coordinate the activities of the group. The articulation of these facts is essential in an affidavit to support the search of any seized device. When you consider applying for a search warrant, think about the nexus of the device to the crime. Is it probable the suspect(s) used the device?

Before the commission of the crime? As noted above, some crimes such as narcotics violations and gang activity require communication and coordination before the act is carried out. Another example is the crime of robbery. While some street level robbers will commit the crime with little or no pre-planning, many will perform surveillance on the target person or location. They will coordinate with lookouts and getaway drivers to insure there is no immediate police presence and easy escape routes from the scene. The articulation of this knowledge is based on the prior training and experience of the office and may be documented in a search warrant example.

Based on your Affiant’s prior training and experience and the experience and training of other veteran law enforcement officers, your Affiant is aware [robbery/narcotics/weapons trafficking] is an inherently conspiratorial crime. The nature of the conspiracy requires participating members to communicate in order to coordinate their planning prior to the commission of the crime, as well as, during the actual commission of the crime. Such communications are commonly made using mobile devices such as tablet computers, mobile phones, and Wi-Fi capable portable gaming consoles.

During the commission of the crime? Similarly, suspects may communicate during the commission of a crime. Narcotics, robbery, and other crimes require the suspects to actively communicate while the crime is being committed.

Based on your Affiant’s prior training and experience and the experience and training of other veteran law enforcement officers, your Affiant is aware [robbery/burglary] is commonly a conspiratorial crime involving the use of others to assist during the commission of the crime. This assistance comes in the form of other suspects, both known and unknown, who will monitor police radio traffic and alert the perpetrators of the impending arrival of law enforcement, lookouts who will maintain visual surveillance on the approaches to the crime scene to alert their associates of the presence of law enforcement, and getaway drivers who will assist the perpetrators with their escape. Communications between co-conspirators is essential to the successful commission of the

crime and the subsequent escape from the area of the crime. Such communications are commonly made using mobile devices such as tablet computers, mobile phones, and Wi-Fi capable gaming consoles.

After the commission of the crime? Once a crime has been committed, the suspect is also likely to use their phone after the fact. Law enforcement officers are aware those who commit crimes will take steps to conceal their activities and make the subsequent law enforcement investigation more difficult. This is true of almost every crime type, including those not traditionally associated with conspiratorial activities. For example, many domestic violence investigators will tell you suspect's frequently contact the victim after the crime to apologize thereby demonstrating consciousness of guilt. Others will take steps to create alibis for their whereabouts during the crime, conspire with others to conceal or destroy evidence, or make plans to flee the jurisdiction where the crime occurred.

Based on your Affiant's prior training and experience and the experience and training of other veteran law enforcement officers, your Affiant is aware suspects who commit the crime of [homicide/assault/domestic violence] will often attempt to conceal or destroy physical evidence of the crime, conspire with others to create alibis, boast or brag about the commission of the crime, and/or attempt to flee the jurisdiction where the crime occurred. Communications between the perpetrator and those who knowingly or unknowingly assist them is essential to the concealment of the crime and possible flight from the area of the crime. Such communications are commonly made using mobile devices such as tablet computers, mobile phones, and Wi-Fi capable gaming consoles.

Common Search Warrant and Affidavit Errors

The second challenge is adapting existing search warrants to make sure all available evidence it being collected but also to prevent future challenges due to antiquated language or omissions in the search warrant affidavit.

Once probable cause to believe a mobile device was used before, during, or after the commission of a crime. The next step is to describe with reasonable particularity the items to be searched for and seized. However, a review of current law enforcement search warrant affidavits revealed many common errors and deficits in the standard language used to search a cell phone or other mobile device. Law enforcement investigators should review their search warrants and consider the following common errors and omissions:

Failing to request the corresponding call detail records in addition to a search of the phone

Law enforcement has traditionally treated searching cell phones and mobile devices and investigating the records maintained by cellular service providers as two separate and distinct disciplines. In fact, both avenues of investigation should be explored simultaneously. The Supreme Court ruling provides an opportunity to blend the investigation of the mobile device and the corresponding records from the cell phone company together. If an officer has probable cause to search the contents of a mobile device for evidence of the crime under investigation they also have probable cause to search the records of cellular service providers for corresponding evidence that may assist their investigation and/or prove their case. In many cases a search warrant was required to obtain information such as cell site location information (CSLI), GPS data, other historical location data, and the stored content maintained by the provider, such as incoming or archived voicemail messages and email messages. With the addition of a few lines to a search warrant affidavit and the face sheet of the warrant, law enforcement officers are now able to gain access to a number of different sources of data that were previously overlooked. The following language was adopted from a search warrant by Santa Clara County Deputy District Attorney Mike Galli.

The following items that may be contained in or at the cellular service provider, [INSERT PROVIDER] who has been determined to have provided service to the listed phone number [INSERT PHONE NUMBER] associated with the seized device.

- a. *Subscriber information, including by way of example and not limitation:*
 - i. *Subscriber name*
 - ii. *Subscriber address*
 - iii. *Identifying information such as date of birth, driver license number, and/or social security number*
 - iv. *Subscriber contact information including electronic mail addresses, contact phone numbers also referred to as ‘can be reached numbers’*
- b. *Billing and credit information, including by way of example and not limitation:*
 - i. *Method and source of payment information including credit card numbers, electronic funds transfers, and locations of cash payments.*
 - ii. *Credit information including any credit report run by the provider prior to authorizing service*
- c. *Service information, including by way of example and not limitation:*

- i. Purchase and activation location*
 - ii. Types of service subscribed to*
 - iii. Additional phone numbers associated with the same account*
 - iv. Make, model, and serial numbers of the phone(s) associated with the account*
- d. Call detail records*
 - i. Incoming/outgoing phone calls, SMS/MMS text message, including the content thereof, data events date, time, and duration of same*
 - ii. Cell site location information including beginning and ending cell sites for any recorded events, per call measurement data (PCMD) and/or timing advance (TA) information alternately known Real Time Data or Round Trip Data.*

Using overly broad language such as “Any and all...”

The use of the phrase “any and all” has been used as a catch all by law enforcement officers writing search warrants for many years. Unfortunately, the phrase has been found to be unconstitutionally vague, overly broad, burdensome, and failing to meet the reasonable particularity requirement of the Fourth Amendment of the Constitution by many courts in the United States. Depending on the requirements of the local jurisdiction, some law enforcement agencies have begun using the alternate phrase “including by way of example and not limitation...”

Failing to support the items to be searched in the affidavit

Every item to be seized pursuant to the search warrant must be supported in the affidavit. However, some search warrant templates include a long list of items to be seized from the mobile device without supporting language in the affidavit. There are two competing schools of thought with regards to the appropriate wording in a search warrant. The first, commonly used by federal law enforcement agencies, is a 40-60 page affidavit describing in painstaking detail all of the locations to be searched including: contact information stored in the electronic phone book, phone call logs, including recordation of incoming, outgoing, and missed calls, short message service (SMS) and multimedia message service (MMS) text/media messages, calendar events, etc. The problem with this type of search warrant is if the officer misses anything by not specifying it in the warrant, such as the file system or application data, they risk losing it during a suppression hearing. The second, school of thought with regards to mobile device search warrants is to specify evidence of the crime under investigation wherever it may be located on the mobile device. The challenge with this type of warrant is it may be viewed as overbroad and not specific enough. The solution is a warrant that addresses the potential negatives from either type of search warrant; specific enough to search for and locate the relevant evidence and while not requiring the time and often unnecessary obsession with detail. Santa Clara County Senior Deputy District Attorney Mike Galli has created what is a nearly ideal balance between brevity and meeting the reasonable particularity requirement. DDA Galli has made his template available to the law enforcement community via this download link <http://policetechnical.com/model-cell-phone-search-warrant/>. While specific to California and referencing California statute, DDA Galli’s warrant not only strikes the balance between the two types of search warrants but also includes language to obtain information from the cellular service provider.

Not listing external storage media, including by way of example and not limitation, Micro SD cards

Micro SD cards are external storage media inserted into a mobile device to increase the storage capacity. Micro SD cards are an important source of information during mobile device forensic examinations as they have large storage capacity and can retain deleted data, such as images and videos, for a considerable length of time. However, most law enforcement search warrants do not specify Micro SD cards as an item to be searched. While there is no specific case law addressing this issue, an argument could be made the Micro SD card is a separate container within the mobile device and, if not specifically addressed in the search warrant, would fall outside the purview of the search warrant. One needs only to look at current law enforcement practice to find the similarities. A good search warrant for a residence is not limited to a search at 123 Main Street. Most search warrants include language such as "... and any outbuildings, garages, sheds, basements, and safes." Even those these buildings and containers are on the property to be searched, they are viewed as separate containers and judicial authorization is specifically sought to include them in the search. Similarly, Micro SD cards, and other external storage media should be treated in the same manner and as separate containers specifically addressed in the search warrant.

Failing to authorize password bypass

When a person engages handset security on their mobile devices, they express a higher expectation of privacy. While there is no specific case law requiring judicial authorization for bypassing a handset security lock, the actual mechanics of the process may make proactively seeking it a convenience. Apple and Google are able to either circumvent handset security features and provide data from the device or remotely reset the security features. These methods require specific judicial authorization to compel the companies to provide assistance. There are also technical methods for retrieving or bypassing the handset security codes from many of the popular models and operating systems. However, these methods are invasive and can, at times, be destructive to the evidence. When seeking a search warrant for an Apple or Google device, it may be prudent to include the appropriate language in the original warrant to prevent repeated trips to the magistrate.

Failing to specify deleted data

A user who deletes data from their mobile device considers the material to be gone. For many models of mobile devices and operating systems, modern forensic techniques are able to recover data even after it has been deleted. While no known precedent exists regarding specific judicial authorization to recover deleted data, it may be wise to proactively address the issue in the initial search warrant. This limits potential suppression challenges by criminal defense attorneys.

Failing to list the possible need for assistance from other agencies

Many law enforcement agencies do not have the requisite equipment or expertise to examine a mobile device. It is common for these agencies to rely on larger municipal, state, and/or federal law enforcement agencies to assist them with the recovery of evidence from a device. While not a statutory requirement, some law enforcement agencies require specific judicial authorization to assist with an investigation. This is particularly true of federal law enforcement agencies who assist their municipal, state, county, or tribal partners. For law enforcement officers who routinely send their mobile devices to another agency for examination, it is good practice to build judicial authorization for this practice into the search warrant.

Failing to seek a waiver of statutory timelines for execution of the mobile device search warrant

Every state has a statutory time requirement for the execution of the warrant. However, this time limit may not correspond to the operational capabilities of a forensic examiner and their agency. It is rare to find a mobile device forensic examiner who doesn't have a back log of cases. This backlog may vary based on the number of devices waiting for examination, the operational or investigative urgency regarding a particular device, and the time and methods used to facilitate the examination. It is a good practice to check with the forensic examiner prior to submitting a search warrant for a mobile device. If the forensic examiner is not going to be able to begin their examination prior to the statutory time limit, it may be sensible to seek a judicial waiver.

On 6//25/2014 your Affiant spoke with Detective John Smith with the ABC High Tech Crimes Task Force. Detective Smith is a forensic examiner assigned to the task force. Detective Smith told your Affiant there is a 21 day back log of mobile devices submitted for forensic examination. Many of these previously submitted devices are considered a priority based on the crime type or pending court cases. Furthermore, Detective Smith told me a complete forensic examination may take between eight to forty hours to complete depending on the complexity of the device, any internal and external storage media associated with the device, and whether it is password protected or not. Therefore, in light of the information from Detective Smith, your Affiant is requesting a waiver of the ten day statutory requirement pursuant to California Penal Code section 1534(a) for execution of this search warrant. Your Affiant requests 30 days for the execution and return of the search warrant for the listed device and any internal and external storage media.

Failing to investigate applications installed on the device

Increasingly, many people, including criminal suspects are using alternate communications methodologies from their mobile devices. Most frequently these are applications and services installed on a device that use Wi-Fi for voice, messaging, and email outside of the services provided by the cellular company. Additionally, there are many covert applications used to store images, videos, text and multimedia messages, contacts, files, and other data that may be concealed as an innocent appearing application during a manual or forensic examination. Knowing what applications were downloaded by the suspect can help identify any other communications channels for follow-up investigations. Both Google and Apple are able to search for applications downloaded and installed on devices associated with their customers' accounts, device serial numbers, and/or phone numbers.

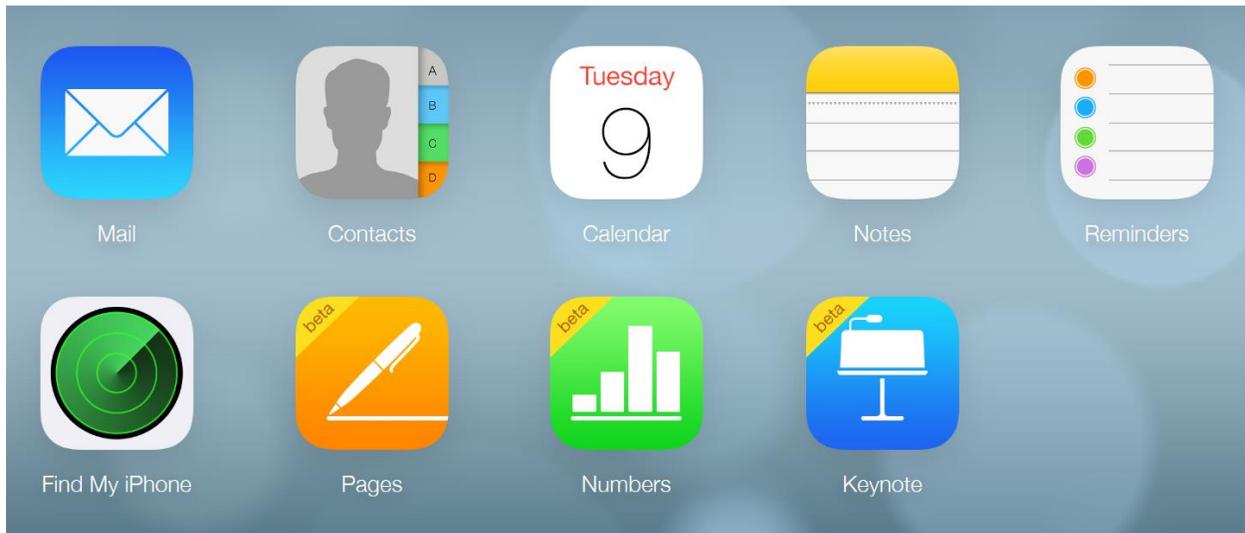
Failing to search associated cloud storage and backup files

There are numerous cloud storage applications that allow a user to store and transfer documents and files. Depending on the type of case under investigation, cloud storage services such as Dropbox and Google Drive may contain relevant evidence that is not recovered during a routine forensic examination of the mobile device. Additionally, Apple allows customers to back up their data to the iCloud storage system including contact lists, photos, application data, internet browsing tabs and bookmarks, calendar events, and electronic mail. There may be evidence located in the backup files that was deleted or inaccessible on the mobile device. Some cellular service providers have additional backup functionality that can be accessed with a search warrant. AT&T's Mobile Locate service periodically backs up contacts,

photos, and videos from their customer’s mobile devices. If this information is not specified in a search warrant, the company will not provide it or even notify law enforcement of its existence.

Failing to search the operating system provider

The two major operating system providers in use today, Apple and Google, both store information from devices in associated cloud, storage, or backup files. The data retained by both of these operating system providers can be recovered, with an appropriate search warrant, even if the device is handset locked or protected by other security features such as encryption. The available data from Apple consists of associated mail accounts, contacts, calendar entries, notes, reminders, and documents created using Apple’s Pages, Numbers, and Keynote applications.



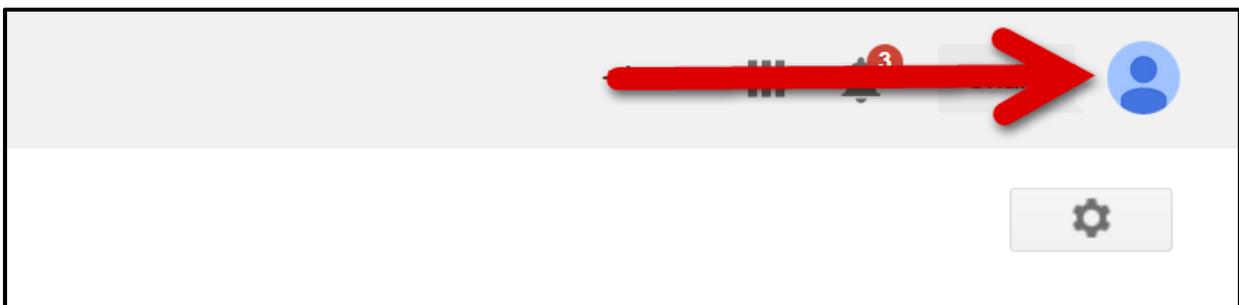
Operating System Warrants: Google

The amount of recoverable data from Apple is relatively minimal when compared with Google. In fact, the amount of data available from Google is more than some current forensic hardware and software programs recover from the mobile device. In order to create a search warrant affidavit that captures all relevant data, it is helpful to examine exactly what kind of data Google retains.

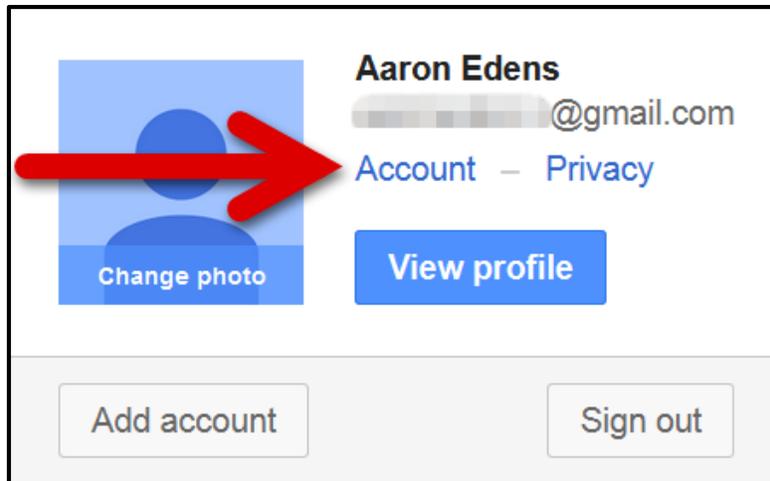
The following pages demonstrate the information available from Google pursuant to a search warrant. As long as law enforcement officers are now required to seek a search warrant to examine a mobile device, there is no reason to leave data “on the table” by the operating system provider. This is particularly true when the breadth and depth of data collected by Google is fully understood.

One of the first arguments encountered at this stage is how do I know the suspect has a Google account and how do I find it? The first half of the argument is relatively simple to answer. If the phone uses the Android operating system there is likely an associated Google account. When a customer takes their brand new Android phone out of the box and turns it on one of the first things they are prompted to do is to associated an email account for recovery purposes. The system prompts the user to associated an existing account or create a new one in case the user forgets their password. When this account is created it automatically begins collecting data even if the user does not primarily use Google’s service such as Gmail. Google is able to search their records by the phone number of the device and the unique serial numbers; the international mobile equipment identifier (IMEI) and the mobile equipment identifier (MEID.) Both of these numbers can be located by removing the battery cover and the battery and examining the manufacturer’s sticker underneath.

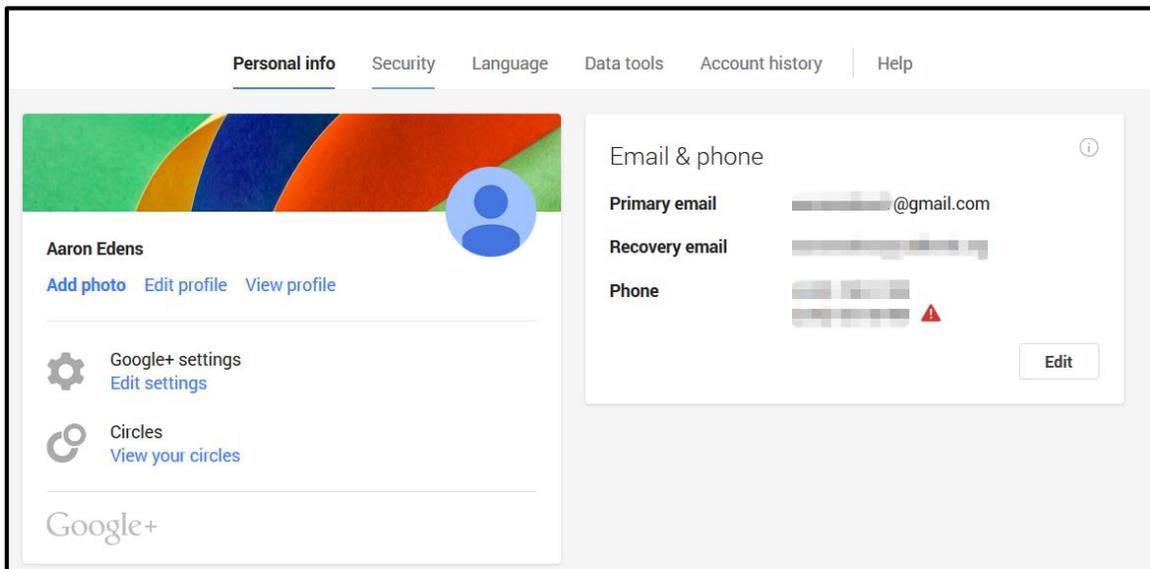
To see what information Google collects simply click on the icon located in the upper right corner of the main search page.



Select the **Account** link.

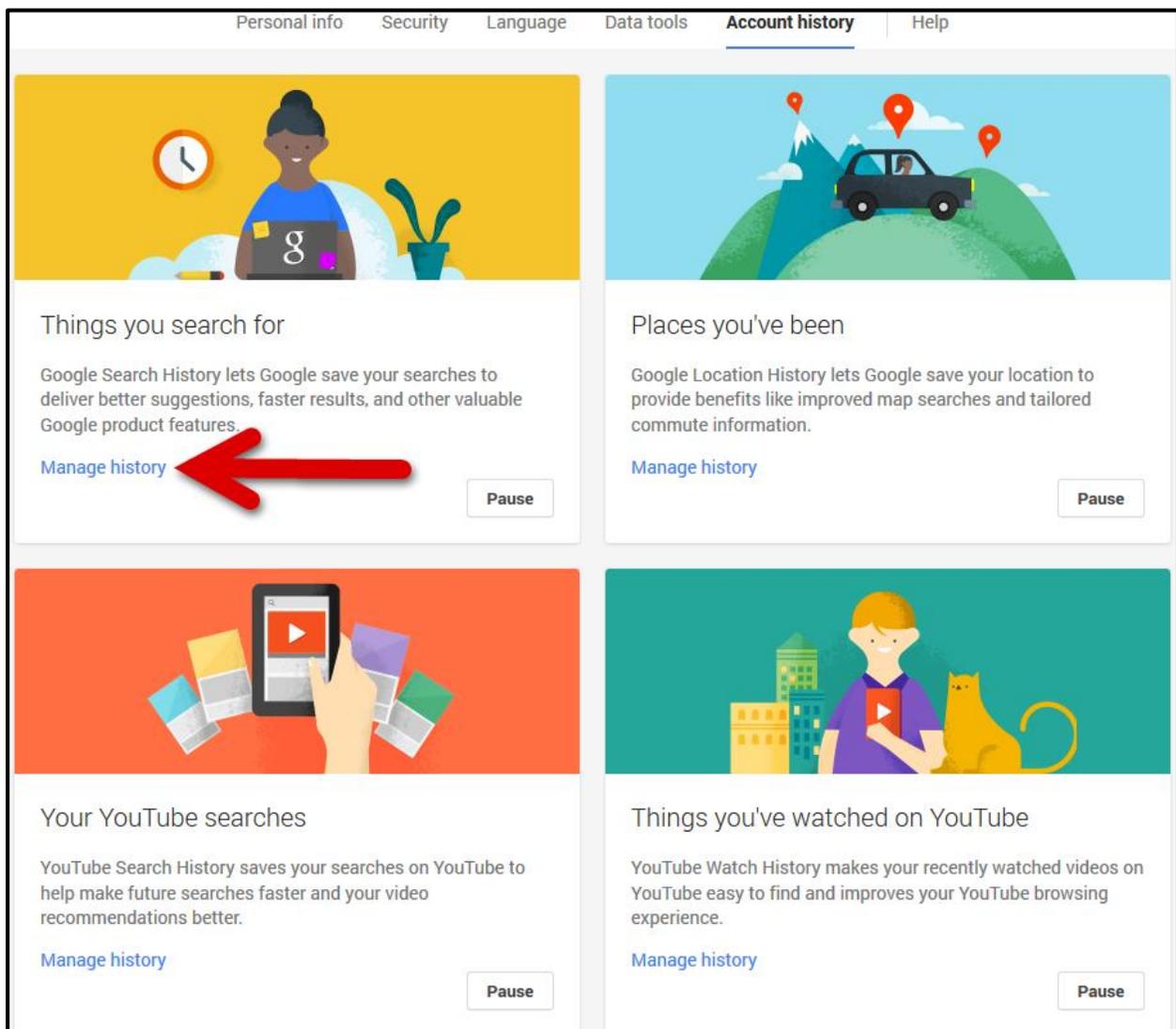


Under the **Personal info** tab at the top of the screen are the email accounts and phone numbers linked to the Google account. In this example there are two email accounts, a primary email and a recovery email. This is an opportunity to discover any previously unknown email accounts and follow-up with additional legal demands. There are also phone numbers linked to this account. In this example there are two phone numbers; the mobile number for the device and a Google Voice number.

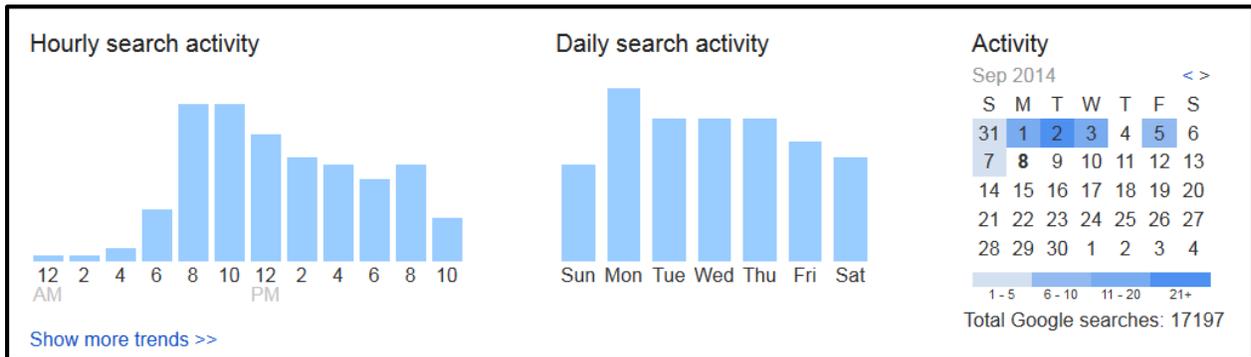


The **Account history** tab at the top of the screen has additional information of significant investigative value. This data is available elsewhere but this interface is a very user friendly for exploring some of the data Google collects and retains.

The first option is the search history. If you have ever started typing a search query into the Google search bar you have no doubt encountered the autofill option. These responses are based on previous searches and are stored by Google to assist the user. However, this data can provide a wealth of evidence and intelligence on many types of cases. Obtaining the search history from Google was previously limited to cases involving known or suspected uses of the search engine in a criminal investigation. Depending on the type of investigation, it may be probable evidence of the crime under investigation can be found in the search history. For example, a marijuana cultivator may use the Google search engine to obtain hydroponic growing equipment or to research a potential grow location. It is up to the investigator to associate the search history with the criminal investigation. This is not a difficult task as the Google search engine is the default on Android phones and Google accounts for approximately 66-68% of search queries worldwide.



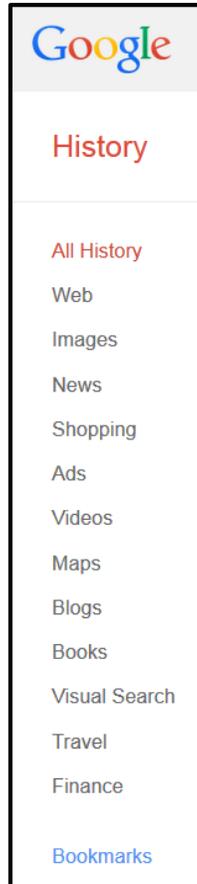
Selecting the **Manage history** link will demonstrate the types of search query data available from Google. There is a user friendly graph of search activity by hour and day. There is also a calendar function. The calendar function shows the specific search history by day. This data can be critical in date/time specific crimes such as homicide. However, the search data as a whole can also be relevant in conspiracy crimes investigations such as narcotics, gangs, and organized crime.



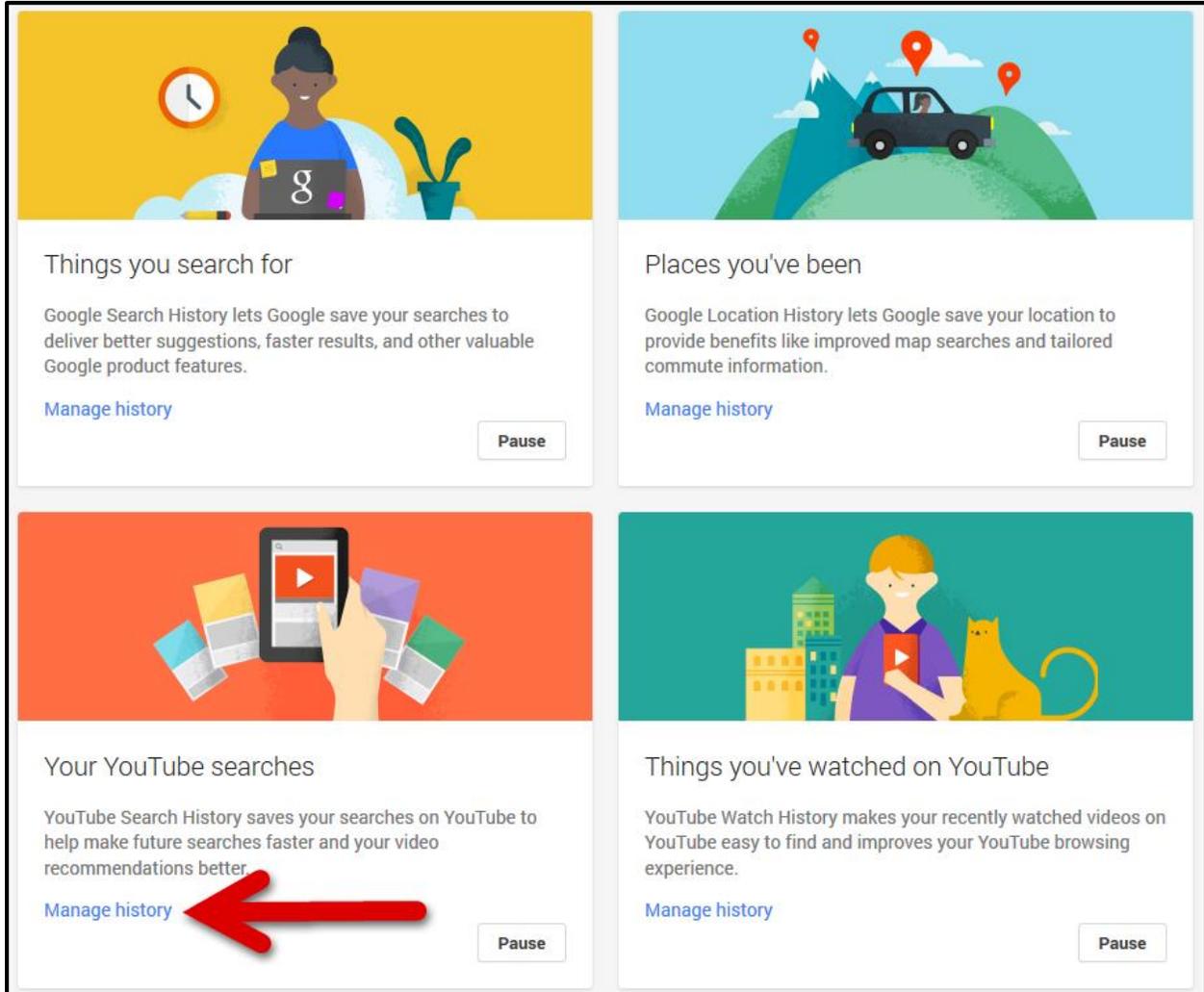
Sep 5, 2014

<input type="checkbox"/>	Searched for From Current Location To Sheraton Sonoma County - Petaluma	8:28am
<input type="checkbox"/>	Searched for directions Sheraton Hotel Petaluma	8:28am
<input type="checkbox"/>	Searched for directions	8:28am
<input type="checkbox"/>	Searched for directions to della Fattoria bakery Petaluma	8:28am
<input type="checkbox"/>	Penry Park - google.com	7:26am
<input type="checkbox"/>	Searched for From Current Location To Della Fattoria Downtown Café	7:19am
<input type="checkbox"/>	Searched for directions to della Fattoria bakery Petaluma	7:14am
<input type="checkbox"/>	Searched for Safeway Petaluma, CA	7:14am

The Manage history link also has an available feature to narrow the search results by category such as web search, image search, maps, etc. Clicking on any of the hyperlinks will take you to the search results.



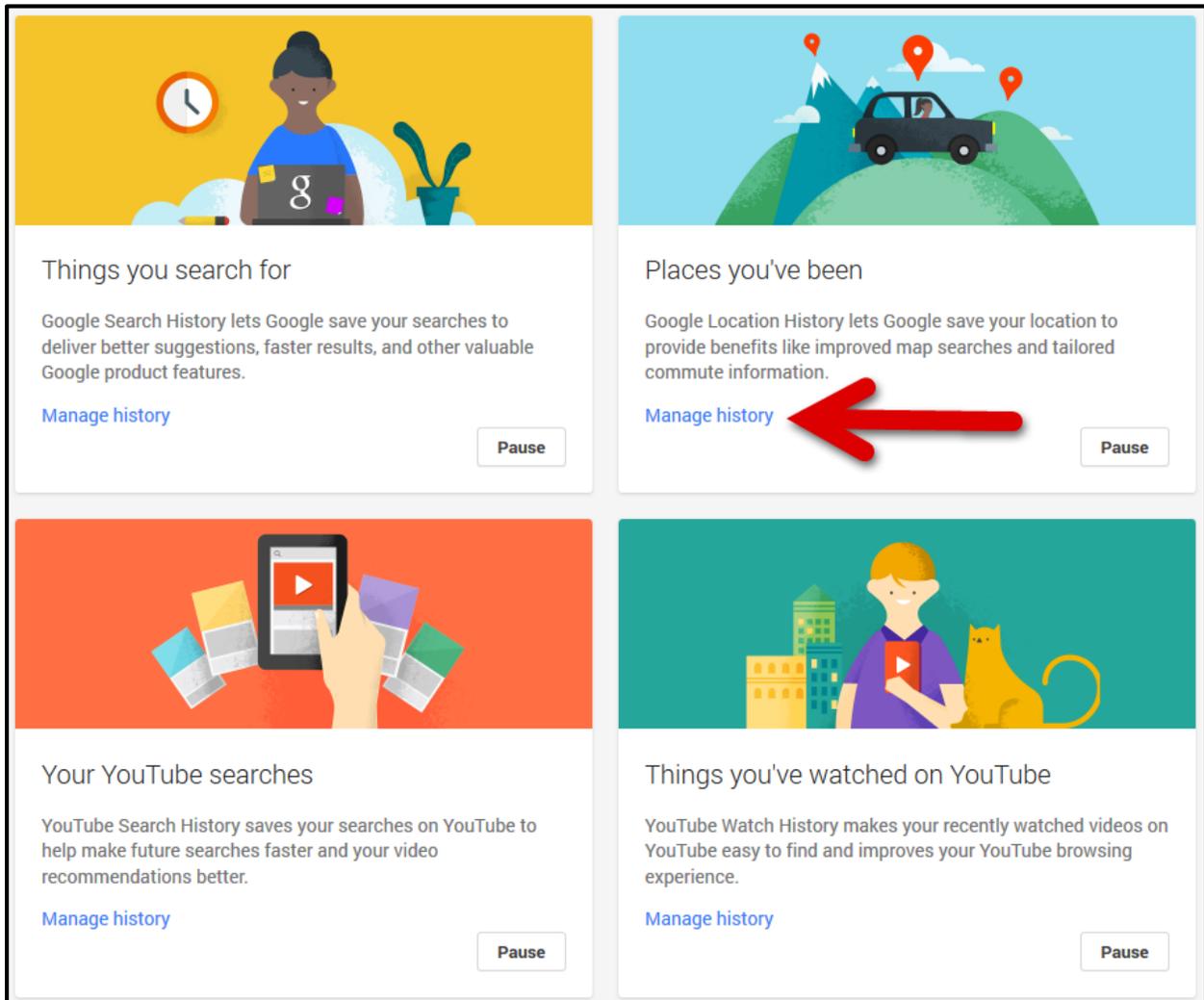
The YouTube search history is self-explanatory. It shows the search history and links to the viewed video. This data is also available from other locations but many be of investigative interest depending on the type of criminal case.



The image shows a grid of four settings cards for a Google account. Each card has a header illustration, a title, a brief description, a 'Manage history' link, and a 'Pause' button.

- Things you search for:** Header shows a person at a laptop. Description: "Google Search History lets Google save your searches to deliver better suggestions, faster results, and other valuable Google product features." Link: [Manage history](#). Button:
- Places you've been:** Header shows a car on a hill with location pins. Description: "Google Location History lets Google save your location to provide benefits like improved map searches and tailored commute information." Link: [Manage history](#). Button:
- Your YouTube searches:** Header shows a hand pointing at a tablet with a play button. Description: "YouTube Search History saves your searches on YouTube to help make future searches faster and your video recommendations better." Link: [Manage history](#). Button: . A large red arrow points to the 'Manage history' link.
- Things you've watched on YouTube:** Header shows a person with a cat and a play button. Description: "YouTube Watch History makes your recently watched videos on YouTube easy to find and improves your YouTube browsing experience." Link: [Manage history](#). Button:

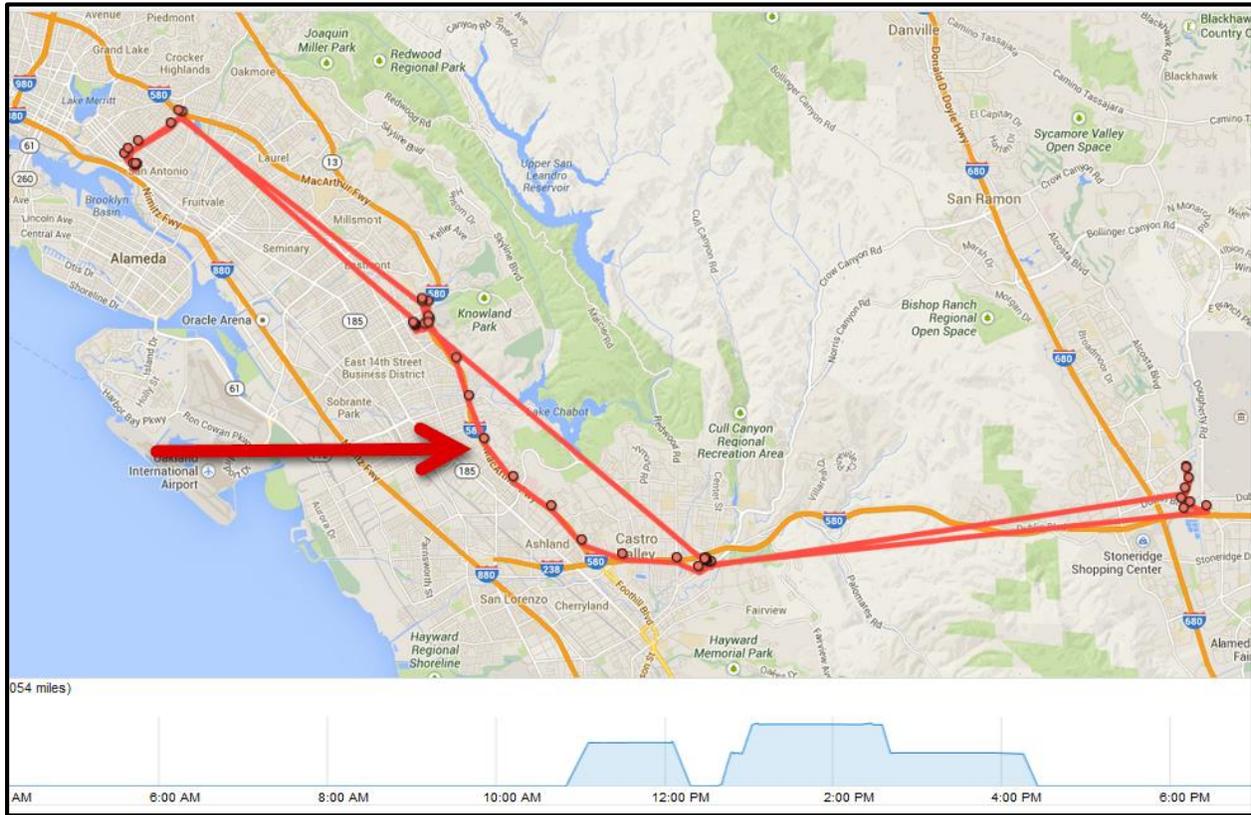
Perhaps one of the most intriguing and useful data sets collected by Google and obtainable with a search warrant is the **Location history**.



Most Android users are unaware there is passively collected historical GPS capability built into the operating system. From the interface above or it can be accessed at the website <https://maps.google.com/locationhistory/b/0>.

The historical GPS location data is not comprehensive as the data is captured when a GPS application is activated on the device. However, it can provide valuable leads and location based intelligence. The example below is from the author's device. It illustrates the historical movements of the mobile device. Note there can be large areas and time periods where GPS location data is not recorded, such as the movements of the device from West to East. Alternately, the regularly spaced data points highlighted with the red arrow are recordings taken approximately every minute while a GPS navigation application

was active. The table below the illustration gives a visual representation of the time periods when the most GPS data was captured.



On the location history map page is a calendar feature. Individual days may be selected by clicking on a specific data on the calendar. Selecting **Show timestamps** will display all of the times a GPS location was recorded on the selected date.

Location history

« June 2014 »

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Show: 1 Day

June 8, 2014

- ▶ Show timestamps 
- [Export to KML](#)
- [Delete history from this day](#)
- [Delete all history](#)

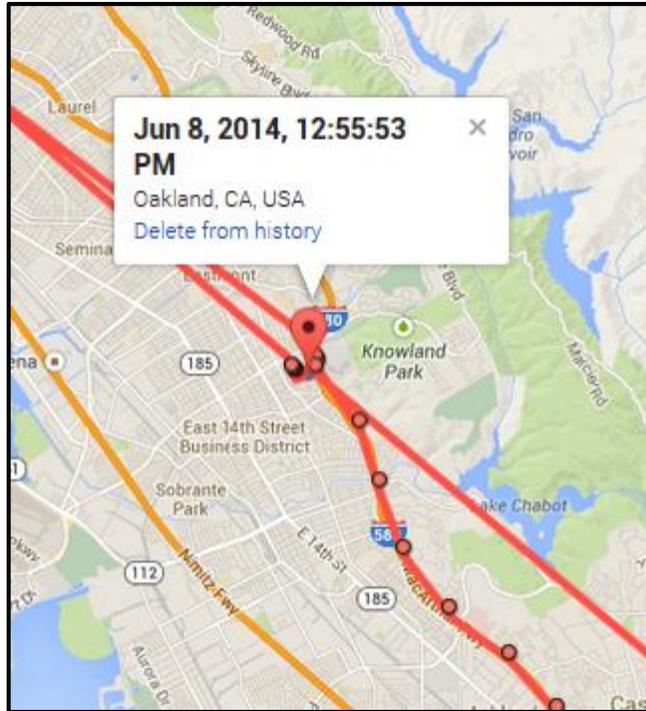
Some points have been hidden from view. [Show All Points](#) [Learn More](#)

10:00 AM - 11:00 AM
10:04 AM 10:48 AM 10:50 AM

11:00 AM - 12:00 PM
11:06 AM 11:41 AM

12:00 PM - 1:00 PM
12:02 PM 12:03 PM 12:04 PM 12:05:08 PM
12:05:53 PM 12:06 PM 12:19:10 PM
12:19:56 PM 12:30 PM 12:31 PM 12:36 PM
12:37 PM 12:39 PM 12:41 PM 12:42 PM
12:43:00 PM 12:43:46 PM 12:44 PM
12:45 PM 12:46:01 PM 12:46:47 PM
12:47 PM 12:48 PM 12:49:03 PM

Selecting a time will show the corresponding hit on the interactive map.

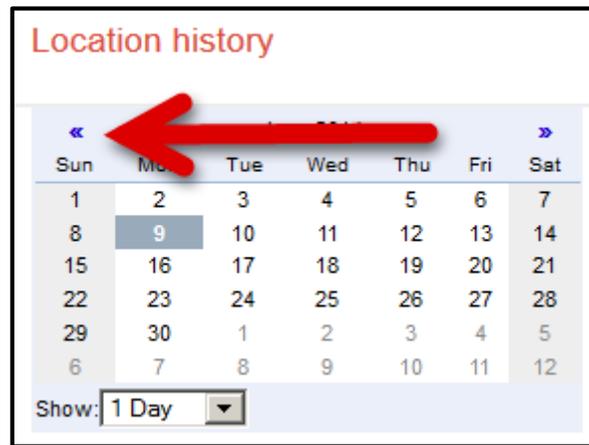


There is also a drop down feature that will show the aggregated location data over a 1,2,3,5,7,14, and 30 day time period.



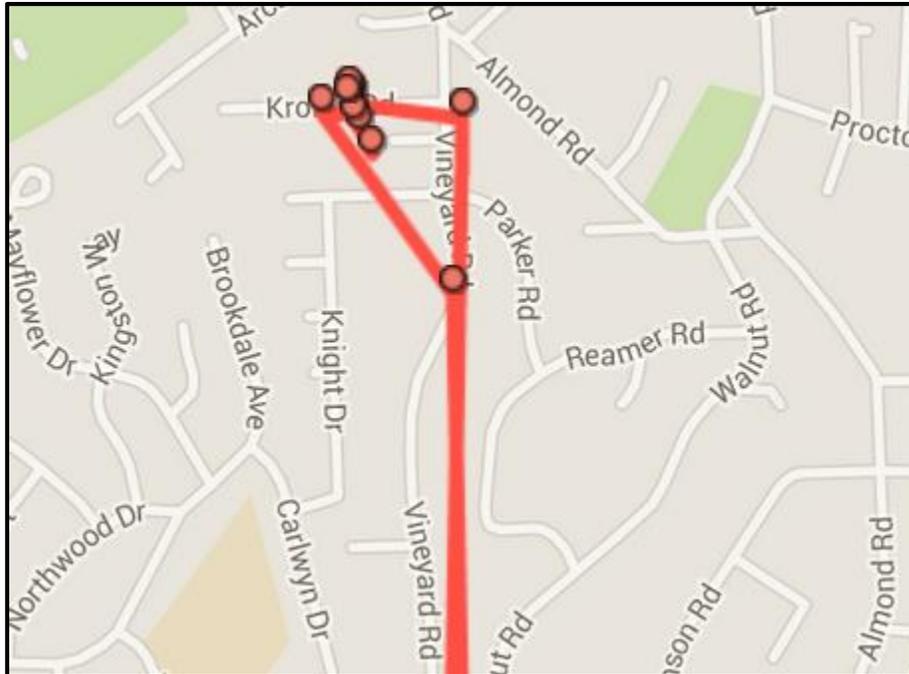
The collection and recording of location based data by Google appears to extend for at least 10 months. In June 2014, the author was able to view the movements of the mobile device as far back as August,

2013. Selecting the left and right scroll arrows to access data points beyond the maximum 30 days permitted in the drop down box.



Data Points

Google is less than transparent when it comes to exactly when location data is collected. Their privacy policy states: “When you use a location-enabled Google service, we may collect and process information about your actual location...” The inference is this location information is collected when the user activates a Google service such as Google maps. However, experimentation and research shows this data is passively collected when there are events on the phone. This appears to include browsing the internet and email pushes to the mobile device but the exact extent and frequency this data is collected is not entirely known. For example, the data points in the illustration below were obtained when there was no activity on the device-no phone calls, no browsing, no application usage, or mapping functions.

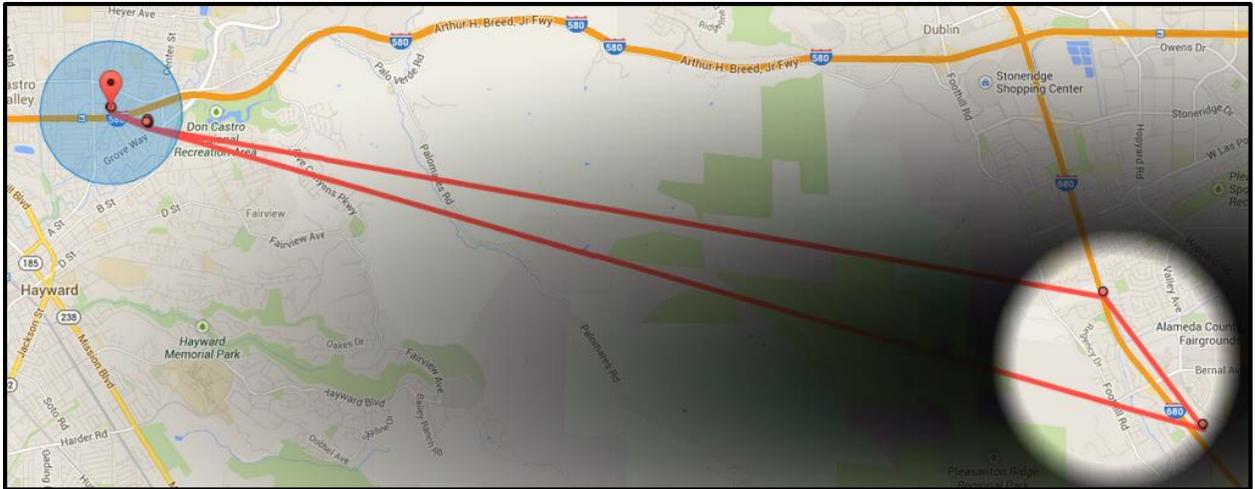


How the data is collected

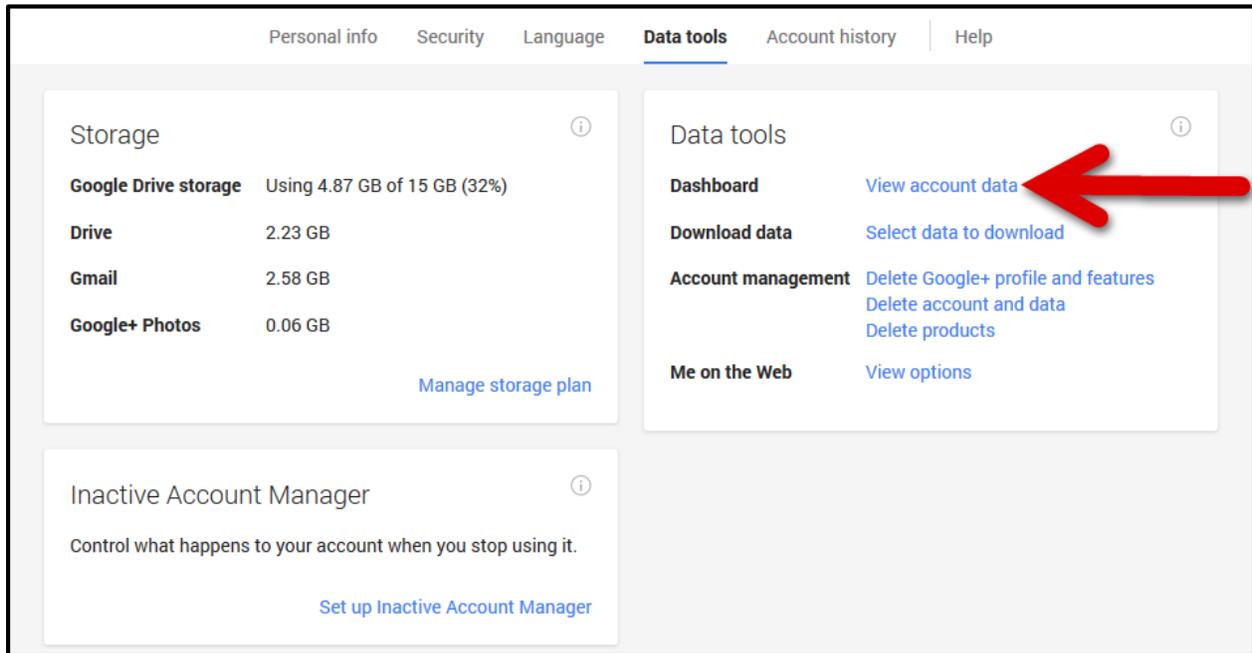
Google states: “Location Services uses GPS, Wi-Fi hotspots, and cellular network towers to determine your location. Location Services uses Wi-Fi only if it's enabled on your device. Because Wi-Fi provides better accuracy than cellular towers, we recommend that you enable Wi-Fi.” Experimentation has shown this to be the case. Disabling the GPS decreases the accuracy of historical location data but it does not eliminate it. It appears the use of cell site location information and Wi-Fi access points give the non-GPS enabled location data nearly the same accuracy.

Aberrant Data

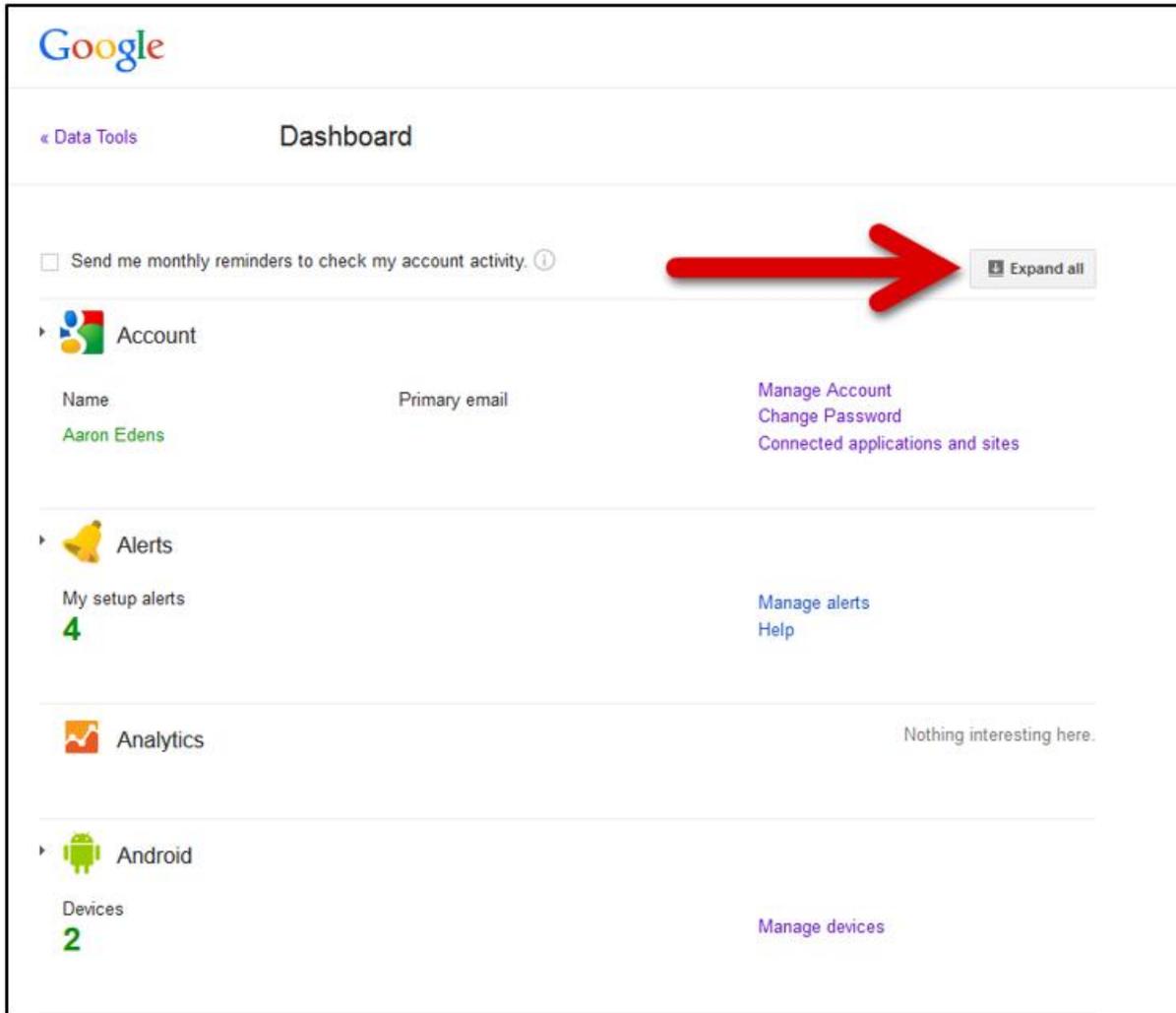
Likely every law enforcement investigator who has dealt with GPS location data has been confounded by the appearance of aberrant data. Specifically, GPS plots that seem illogical in the context of the larger data set. For example, the screen capture below shows GPS activity on the left part of the screen and then two outliers in the highlighted area on the right of the image. The device was never in those locations and, based on the limited understanding of Google’s historical GPS data collection, the appearance of those data points is unexplainable. Equally confounding is the fact those data points later disappeared from the map.



To further understand the available data from Google it is helpful to move beyond the user friendly **Account history** tab into the **Data tools**. From the tab select **View account data**.



To fully appreciate the types and amount of data available from Google, select the **Expand all** tab. This dramatically increases the display of information available to an investigator.



Each category has specific data sets contained within the drop down menu. The facts and circumstances of each investigation are different but there are some common areas of interest. The first is the **Account** field. Initially this information appears to be fairly innocuous, particularly when the view is not expanded. However, selecting the **See the full list** link brings up recent log-in activity. This is not general activity but when the user logged into a Google account from their mobile device, laptop, or desktop computer. Included is geographic information about where the device was located that logged into the service.

The screenshot shows a Google Account page for 'Aaron Edens'. It includes sections for 'Overview' with 8 connected applications and sites, and 'Account activity last 28 days'. Under 'Account sign-ins', it lists 'Locations' (United States), 'Browsers' (Firefox), and 'Platforms' (Android, Windows). A red arrow points to the 'See the full list' link. 'More links' include 'Google privacy policy' and 'Privacy and security help'.

Date	Event	Location
9:13 AM	Signed in from Firefox (Windows)	Castro Valley, CA, USA
Sep 3	Signed in from Chrome (SAMSUNG-SM-G870A)	Castro Valley, CA, USA
Aug 28	Signed in from Firefox (Windows)	Pleasanton, CA, USA
Aug 26	Signed in from Chrome (SAMSUNG-SM-G870A)	San Francisco, CA, USA
Aug 25	Signed in from Firefox (Windows)	Castro Valley, CA, USA
Aug 19	Signed in from Chrome (SAMSUNG-SM-G870A)	San Francisco, CA, USA
Aug 13	Signed in from Firefox (Windows)	Las Vegas NV, Paradise, NV, USA
Aug 13	Signed in from Firefox (Windows)	Las Vegas NV, Paradise, NV, USA

Selecting any of the dates and events brings up a map showing the general geographic area and the internet protocol (IP) address of the connection. The IP address can be resolved to a service provider which in turn can provide the location of the connection such as a Wi-Fi hot spot.

Your Recent Activity ?

Date	Event	Location
9:13 AM	Signed in from Firefox (Windows)	Castro Valley, CA, USA
Sep 3	Signed in from Chrome (SAMSUNG-SM-G870A)	Castro Valley, CA, USA
Aug 28	Signed in from Firefox (Windows)	Pleasanton, CA, USA
Aug 26	Signed in from Chrome (SAMSUNG-SM-G870A)	San Francisco, CA, USA
Aug 25	Signed in from Firefox (Windows)	Castro Valley, CA, USA
Aug 19	Signed in from Chrome (SAMSUNG-SM-G870A)	San Francisco, CA, USA
Aug 13	Signed in from Firefox (Windows)	Las Vegas NV, Paradise, NV, USA
Aug 13	Signed in from Firefox (Windows)	Las Vegas NV, Paradise, NV, USA

Signed in
August 28 4:48 PM (11 days ago)

Recognize this activity?
If you don't, someone else may have your password.

[Change password](#)

Approximate location (based on IP)
Pleasanton, CA, USA

Details
IP address ?
38.110.158.250
pleasanton.ca.us

The **Android** section displays all of the devices that were linked to Google's services and displays the IMEI or MEID and file backup dates and times.

Android

Devices [Manage devices](#)

2

samsung SAMSUNG-SM-G870A AT&T IMEI: [REDACTED]
 Last activity seen on: Sep 2, 2014
 Registered date: Jul 29, 2014

Applications with backup on servers

- Android Wallpaper
Backup date: Sep 8, 2014 8:57 AM
Backup size: 115 B
- Android System Settings
Backup date: Sep 6, 2014 9:22 AM
Backup size: 2.25 KB
- Android Market
Backup date: Sep 6, 2014 8:19 AM
Backup size: 16 B

samsung SAMSUNG-SGH-I747 AT&T IMEI: [REDACTED]
 Last activity seen on: Jul 28, 2014
 Registered date: Jul 9, 2012

Applications with backup on servers

- Android Wallpaper
Backup date: Jul 28, 2014 8:46 AM
Backup size: 505.44 KB
- Android System Settings
Backup date: Jul 23, 2014 12:44 PM
Backup size: 5.88 KB
- Android Market
Backup date: Jul 28, 2014 8:46 AM
Backup size: 17 B
- Gmail
Backup date: May 29, 2014 11:03 PM
Backup size: 1.34 KB

Calendar, unsurprisingly, shows the Google calendar linked to the account. The calendar events may be relevant in certain types of investigations. Additionally, in the case of linked calendars, it may be beneficial to see who has access to the calendar. This would likely be someone closely linked either personally or professionally.

31 Calendar

My Calendars
2 calendars

Time zone
(GMT-08:00) Pacific Time

View Calendar
Manage calendars
Manage mobile devices

Overview

Aaron Edens Shared with 3 people
Most recently modified event: Meeting with Shannon on Aug 28, 2014

Police Technical Availability Shared with 2 people
No recent events.

Account activity last 28 days

Aaron Edens My events: 7 events
Event acceptance:
Yes: 7
Maybe: 0
No: 0
Not responded: 0

The **Contacts** section has a complete listing of all contacts entered by the user or imported from their Google Mail. The data includes anything entered by the user such as name, phone numbers, pictures, and email addresses. This may be an alternative source of contact information in the event a law enforcement officer is confronted with a locked Android device and no way around the passcode. By serving Google with a search warrant an investigator can replicate the contacts section on the Android device without actually accessing the device itself.

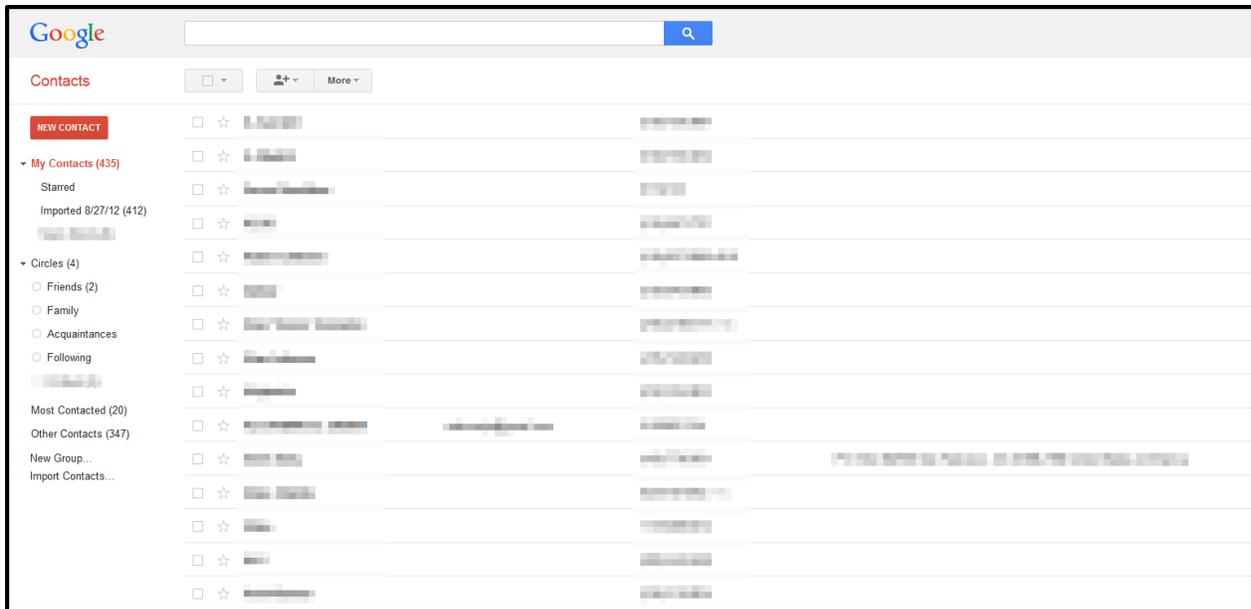
Contacts

All contacts
785

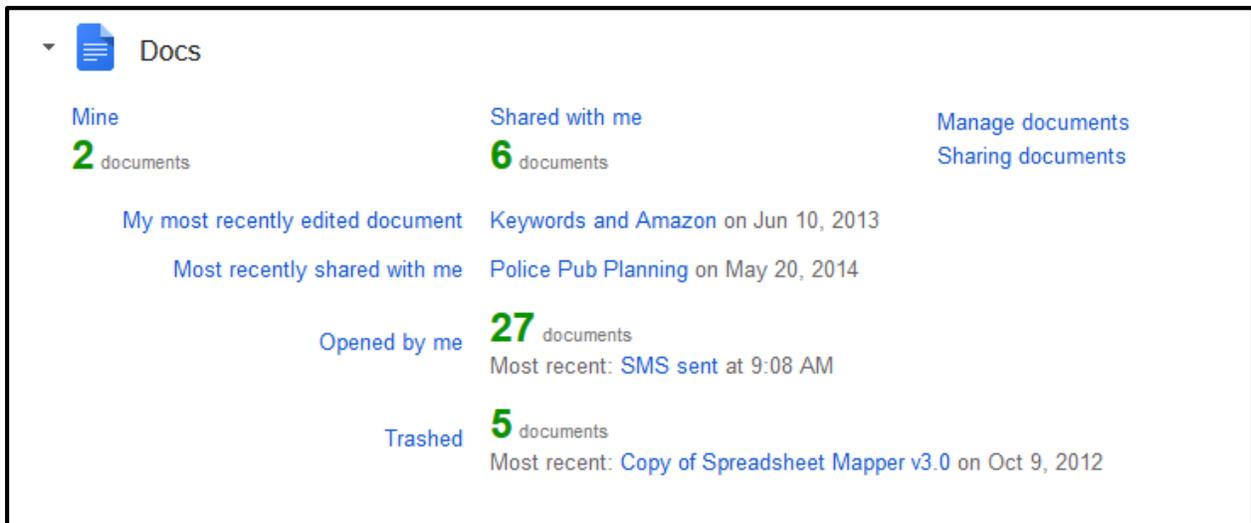
My contacts
435

Manage contacts

Most contacted



The **Docs** section shows links to the users Google docs and any downloaded or received documents using this service. Google Docs is increasing in popularity as a replacement to Microsoft's products as Google's are available for free.



Many street level criminals are unlikely to make use of Google's **Finance** services but the data may be useful in organized crime and money laundering investigations.

The screenshot shows a 'Finance' section with a dropdown arrow and a green square icon. Below the header, there are two main categories: 'Portfolios' and 'Securities'. Under 'Portfolios', there is a large green number '2' and a link 'Manage Portfolios'. Under 'Securities', there is a large green number '6'. Below these, there are two sub-sections: 'My Portfolio' and 'Market'. 'My Portfolio' shows '3 securities' and a 'Portfolio value' represented by a green bar chart, with the text 'at 9:51 AM'. 'Market' also shows '3 securities' and a 'Portfolio value' of 'USD0.00 at 9:51 AM'.

The **Gmail** section contains information regarding any associated Gmail accounts. It is troublesome that many criminal investigators will obtain call detail records and other data from the cellular service provider and neglect to obtain email conversations. The same probable cause for searching a mobile device is likely applicable to email content as well. In fact, email content may have more investigative value than text and multi-media messages as the content is not limited to a finite number of characters or by certain file types. An often overlooked feature in Gmail is that deleted emails are stored in the Trash file and are not actually deleted unless the user empties that file. Therefore, it is possible to recover 'deleted' emails from Google with a search warrant. Note that once the Trash file is emptied the email files are not recoverable from Google but may still be recoverable from the device or an associated computer.

The screenshot shows a 'Gmail' section with a dropdown arrow and a red envelope icon. Below the header, there are several statistics and links. On the left, 'Conversations' is listed with a large green number '11,011'. To the right, there are links for 'Manage Chat History', 'Settings', and 'Privacy and security'. Below these, there are four categories of conversations: 'Inbox' with '3,512 conversations' and a 'Most recent' link; 'Sent Mail' with '1,435 conversations'; 'Saved drafts' with '3 conversations'; and 'Chat history' with '2 conversations'. At the bottom, 'Trash' is listed with '9 conversations' and a 'Most recent' link.

Google Photos stores images shared with the Google+ social network and any pictures taken with a mobile device that are uploaded to Google Drive cloud storage. Depending on the user, the images in Google Photos may be the same as the images taken with the associated mobile device. Investigators who are familiar with EXIF data, also called metadata, should be aware the GPS coordinates of where the picture was taken are not encoded in the image. This feature is turned off by default on the Google Pictures settings and must be turned on by the user in order to be active.

Google Photos

Albums **23** Photos **241** Settings
Privacy
Help

Albums **1** public **0** unlisted **22** sign-in required
Most recent: 2014/09/06 #2 on Sep 6, 2014

Photos **0** public **0** unlisted **241** sign-in required

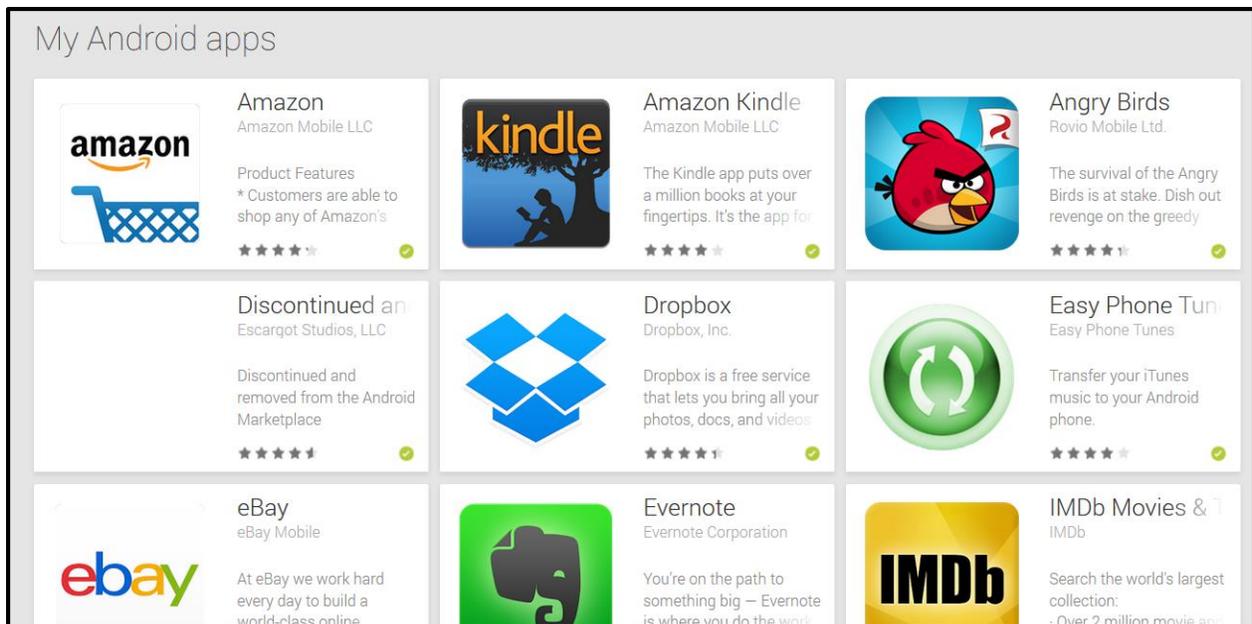
More links [Face tags](#)
[Picasa Web Albums Settings](#)
[Picasa Web Albums album visibility settings](#)

A commonly overlooked area of mobile device investigations are the applications installed on a device. Records of purchased and downloaded applications is available via search warrant from Google's **Play Store**. The application history can provide a wealth of information and leads regarding a suspect's purchasing history via apps like Amazon.com, financial institution information indicated by an installed banking application, cloud storage accounts, and social media sites used by the suspect.

Play Store

Installed applications **175**

Most recent app **ANT+ Plugins Service** on Sep 1, 2014 [View applications](#)



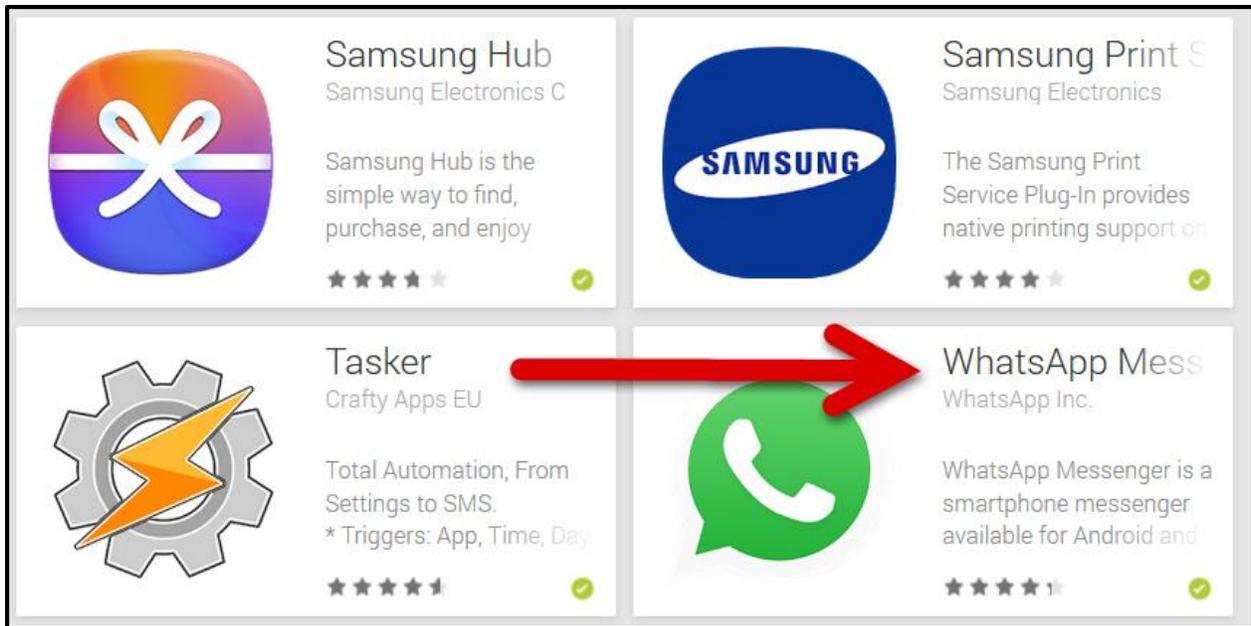
According to two Nielsen surveys the average smart phone user has 41 applications installed on their device. The average user spends 30 hours, 15 minutes using apps per month. Compare this with the average use of the cellular phone function of a device at 7 hours 35 minutes per month. This means most users spend roughly four times as much time using applications than they do the actual phone. The same Nielsen study broke down the use of smart phone applications and broke down the three app usage categories by type and time:

Search engines, search portals, and social media 10:56

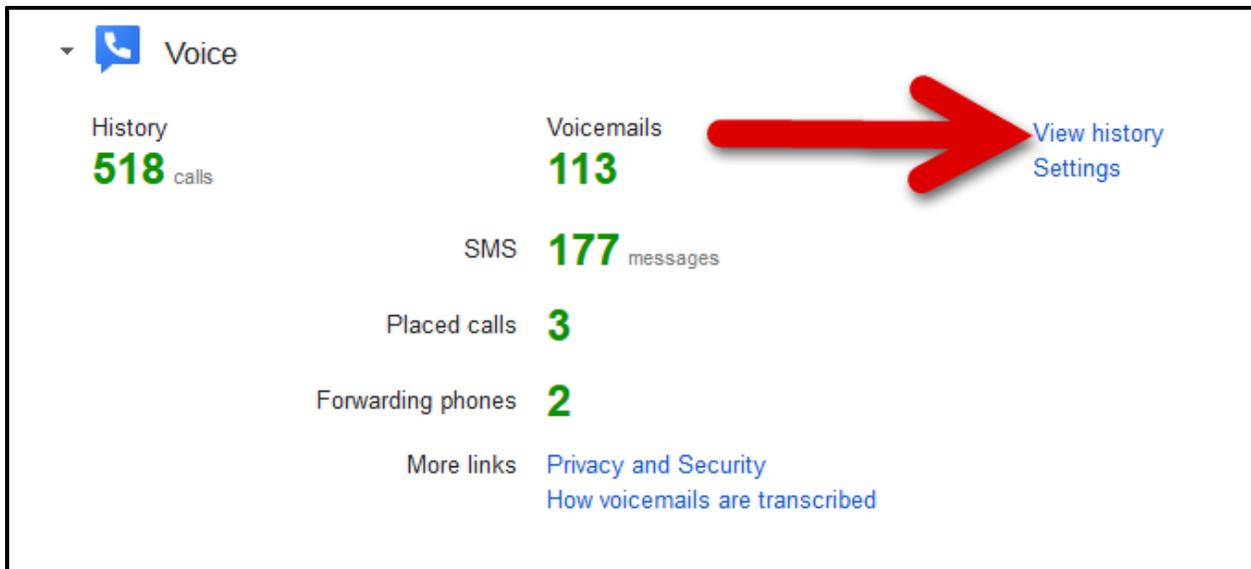
Entertainment/games 10:34

Communication 3:48

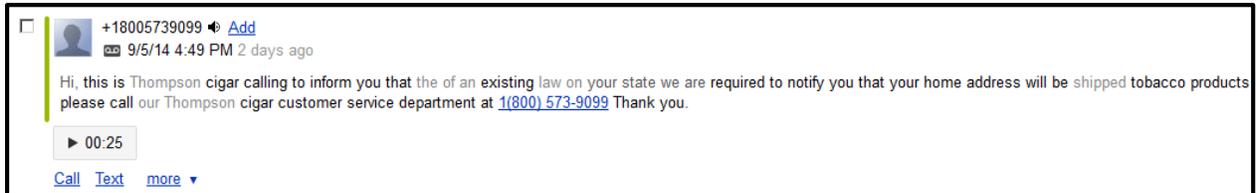
The Nielsen statistics are revealing and have a significant imperative for law enforcement investigators. If you are not investigating the applications and are only focusing on call detail records you are missing a significant amount of evidence and intelligence. The use of communications applications on smart phones is roughly half that of the cellular use. Neglecting communications applications means you may be missing as much as 50% of the available records and data.



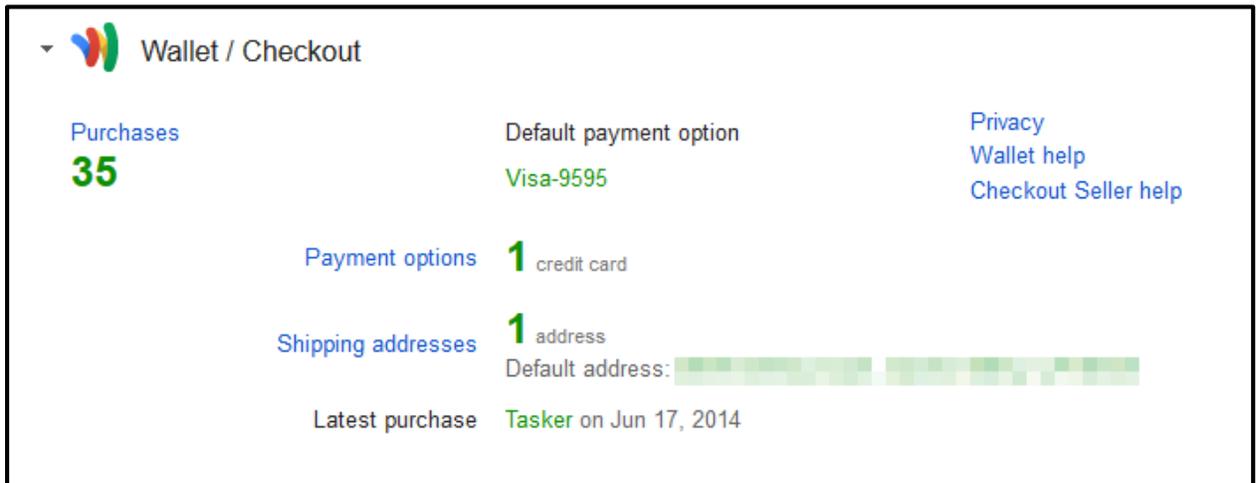
If the suspect in a criminal investigation is using Google’s **Voice** service then there is a substantial amount of information available from the company pursuant to a search warrant. Many investigators lament the minimal call detail record information they obtain from Google. While minimalist, the wealth of information from the other features more than compensate. Specifically, the text messaging and voicemail features. This data is retained indefinitely in Voice until it is deleted by the user. This translates into potentially hundreds of text messages and voice mail messages available pursuant to a search warrant.

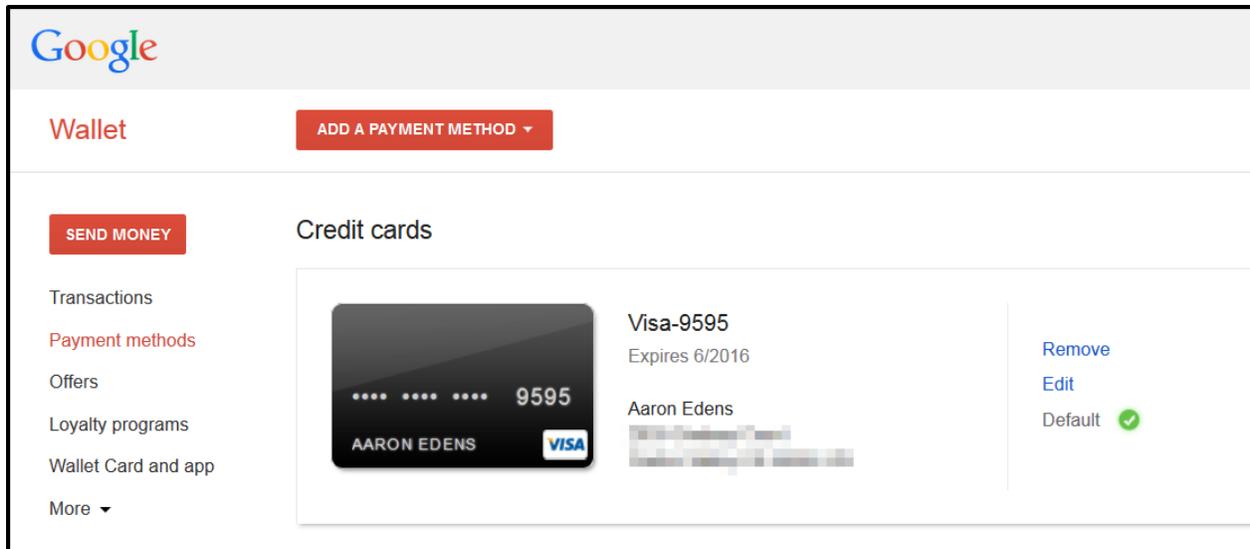


Google Voice makes an attempt at translating voicemail messages. Depending on the clarity of the speaker it is possible to quickly preview voicemail messages of investigative interest and bypass those that do not appear relevant.



In order to purchase applications for an Android device, a subject must make use of Google's **Wallet/Checkout** service. While most users are familiar with this in conjunction with application purchases, Google's service also works for other internet purchases. It is possible to view the user's entire purchase history made with the Wallet/Checkout service. There is also information about linked credit cards which may be of assistance in organized crime, money laundering, and fugitive investigations.





Each investigation is different and the information requirements are based on what the investigator needs. Each item to be seized from Google pursuant to a search warrant must be supported in the probable cause affidavit. While each jurisdiction is different, some suggested language may include:

Based on your Affiant's prior training and experience, I am aware users of Android operating system phones, such as the one list is Exhibit 1A and which this affidavit seeks a search warrant for, commonly have an associated account with Google. When a user purchases and activates a mobile device one of the initial prompts during the set-up phase is to associate a Google Gmail account with the device. The purposes of this account are to facilitate a password reset in the event the consumer forgets their passcode or pattern unlock. If the consumer does not have an existing Gmail account, the operating system prompts the user to create a new account. Whether the Gmail account is new or existing the association of the account with the device allows Google to collect and store information relevant to this criminal investigation. This information includes, by way of example and not limitation:

Account Information-User name, primary email address, secondary email addresses, connected applications and sites, and account activity for the previous 28 days, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses.

Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.

Android Information-Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device.

Google stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account and/or known device(s).

Calendar-All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees.

Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and remains so unless the user adds a third party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. I believe this information will identify relevant dates and appointments germane to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses.

Contacts-All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images.

When a user links their Android device to their Google account the names, addresses, phone numbers, email addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process continuously updates so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. I believe this information is pertinent to the investigation as it will assist with identifying previously unknown co-conspirators and/or witnesses.

Docs (Documents)-All Google documents including by way of example and not limitation, Docs (a web-based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web-based presentation program.) Documents will include all files whether created, shared, or downloaded.

Google offers their users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user's account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. I believe this information may contain notes, files, and spreadsheets containing information relevant to this investigation including recordation of sales, communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation.

Finance-All records of securities, funds, and portfolios associated with the target Google account and/or target device.

Google allows users to create custom portfolios of stocks, bonds, and mutual funds. These portfolios are updated based on the market conditions and contain the investment type and the dollar value of the investment. I believe this data may contain information about income, investments, and previously undiscovered assets derived as proceeds from the ongoing criminal enterprise.

Gmail-All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files.

As noted previously, when user of an Android device first activates the device they are prompted to associate the device with a Google mail, commonly referred to as Gmail, account. The purpose of this account is to facilitate password recovery in the event the user forgets their password or pattern lock. If the user does not have an existing Gmail account they are prompted to create one. The Gmail account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages. Messages deleted from Gmail are not actually deleted. They are moved to a folder labelled Trash and are stored there until the user empties the Trash file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. I believe these messages would reveal motivations, plans and intentions, associates, and other co-conspirators.

Google Photos-All images, graphic files, video files, and other media files stored in the Google Photos service.

Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user's mobile device. In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. I believe a review of these images would provide evidence depicting the suspect, their associates, and others performing incriminating acts. I also believe these image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation.

Location History-All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period ____ to ____.

Google collects and retains location data from Android enabled mobile devices. The company uses this information for location based advertising and location based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access. I believe this data will show the movements of the suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation.

Play Store-All applications downloaded, installed, and/or purchased by the associated account and/or device.

Google operates an online marketplace whereby Google and other third party vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can be used to communicate outside the cellular service of a mobile device by accessing the internet via Wi-Fi. These various applications facilitate communication via voice using voice over internet protocol (VOIP) technology, short message system (SMS) text messages, multi-media message system (MMS) text messages, audio transmission of recorded messages, and recorded or live video messages. As these services operate independently of the cellular service network there is no corresponding information regarding communications from the cellular provider. Identifying communications applications purchased, downloaded, and/or installed on the mobile device would assist investigators by determining what application provider should be served with additional search warrants. Furthermore, identifying the user's applications would assist investigators with determining banking and other financial institution information and social media sites used. Identifying the purchased or installed applications would assist locating those with potentially criminal implications such as applications that appear to the observer to be a calculator or other innocuous appearing program but in actuality are used to conceal pictures, videos, and other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices as existing technologies are not designed to detect and locate them and the information they conceal.

Search History-All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance.

Google retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user selected results. Furthermore, these searches are differentiated by the specific type of search a user performed into categories. These categories include a general web search, and specialty searches where the results are focused in a particular group such as images, news, videos, and shopping. I believe a review of the suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it.

Voice-All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device.

Google offers users access to a free voice over internet protocol (VOIP) communications system called Google Voice or simply Voice. This system is layered on top of any existing cellular service. Users are provided with a phone number they select from a pool of available numbers. These numbers can be from whatever area code and prefix they desire and have no correlation with the user's actual location when the number is selected. Google allows users to access this system to make and receive phone calls and text messages. The service also has a voicemail feature where incoming phone calls are permitted to leave a message that is subsequently transcribed by Google and delivered by electronic mail and/or text message. Google maintains call detail records similar to those of a traditional cellular or wireline telephone company. Additionally, they also store the text message content of sent and received text messages, as well as, any saved voicemail messages and the associated transcriptions.

Wallet/Checkout-All information contained in the associated Google Wallet account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book.

Google operates a financial services division that allows users to make online purchases through Google and other vendors, as well as, send and receive money from other users. Applications that are purchased and installed on a mobile device are handled by Google's Wallet/Checkout service. The purchase and installation of applications on a mobile device requires the use of the Google Wallet service. Therefore, any applications installed on the suspect's mobile phone have a transaction record in Google Wallet. Google stores information regarding the transactions including the date and time of the purchase. Additionally, they have method of payment information such as associated credit card numbers used to facilitate the purchase. Other data includes the billing address of any linked credit card and any addresses where purchased products were shipped to. I believe identifying the method of payment information would assist investigators with identifying any previously unknown financial institutions and that these financial institutions may have additional relevant information pertinent to this investigation.

A thorough understanding of the data retained by Google services reveals an unprecedented amount of information relevant to criminal investigations. Failing to include Google as a place to be searched in investigations involving Android devices may lead to critical evidence and intelligence being 'left at the table.'