Hack In The Box

Smartphone Privacy:

How Your Smartphone Tracks Your Entire Life

Vladimir Katalov, ElcomSoft

What’s Inside?

- Account passwords and tokens
- Web and application passwords
- Messages (including iMessage)
- Health data (Apple Health)
- Payment data (Apple Pay)

- Call logs
- Emails and chats
- Wi-Fi passwords
- Documents, settings and databases
- Web browsing history, tabs, searches
- Pictures and videos
- Geolocation history, routes and places

Apple and Law Enforcement

How Apple Serves LE Requests

- Law enforcement can obtain evidence via government information requests
- **The process is fully transparent** (by extent allowable by law)
- Annual stats published and available to general public:

  https://www.apple.com/legal/privacy/transparency/requests-2017-H2-en.pdf

- Guidelines:

  https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf

  https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

Apple and Law Enforcement

How LE Requests Work

- **Account Preservation Request** followed by **Account Information Request**
- All requests are handled in compliance with Apple’s privacy policy
- Serving government requests, Apple provides information in a proprietary format
- Investigators receive encrypted information. Decryption key is provided, but no tools to decrypt data
- The decryption process is complicated
- Many experts use third-party tools or services such as Kleopatra, GPG, Cellebrite, or BlackBag

Apple and Law Enforcement

LE Requests: Pros and Contras

- Government requests don’t need the user’s authentication credentials
- If login and password unavailable, a government request may be the only way to obtain information
- Authentication credentials aside, government requests have many significant drawbacks compared to in-house cloud acquisition

Apple and Law Enforcement

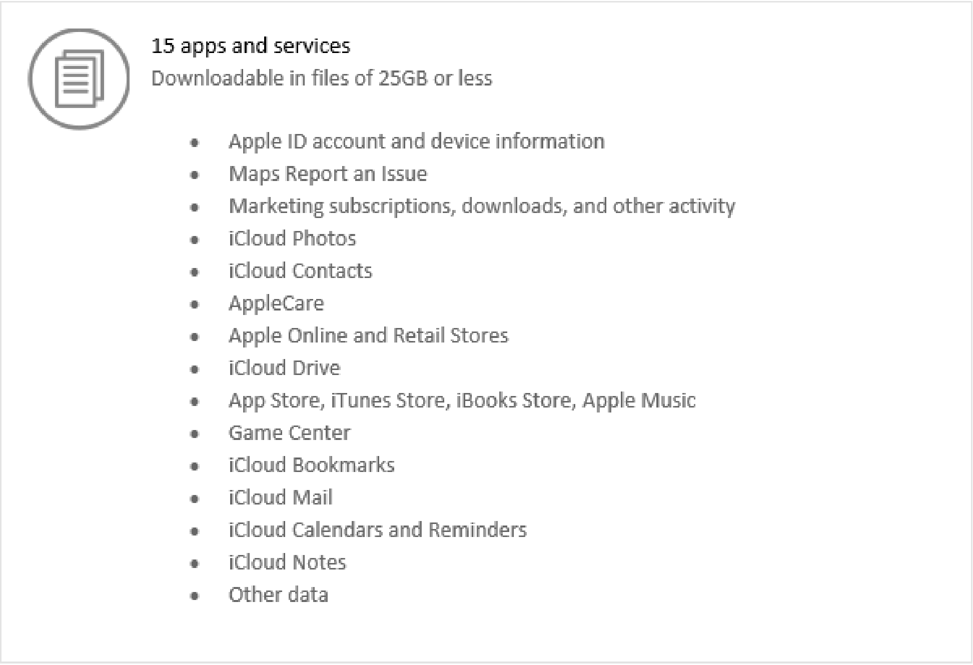
The Ugly Side of LE Requests

- Lots of legal paperwork
- **Account Preservation Request** must be submitted ahead of acquisition
- The process is lengthy
  - Up to two months
- Apple provides data in binary format, encrypted
  - Decryption key is provided, but no decryption tools
  - Third-party tools and services add extra costs and delays
- Apple will NOT deliver **messages** or **passwords** (iCloud Keychain)
  - Additional encryption with a different encryption key

Apple and GDPR

What Is There…

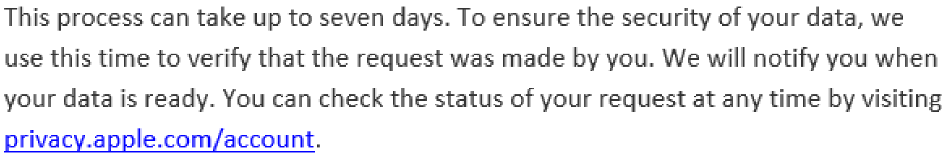
- All major data is there
- Pictures included
- Browsing history, files, iCloud Mail
- 7 days to process request
- Delivers snapshot taken on Day 1 of the request



15 apps and services

Downloadable in files of 25GB or less

- Apple ID account and device information
- Maps Report an Issue
- Marketing subscriptions, downloads, and other activity
- iCloud Photos
- iCloud Contacts
- AppleCare
- Apple Online and Retail Stores
- iCloud Drive
- App Store, iTunes Store, iBooks Store, Apple Music
- Game Center
- iCloud Bookmarks
- iCloud Mail
- iCloud Calendars and Reminders
- iCloud Notes
- Other data

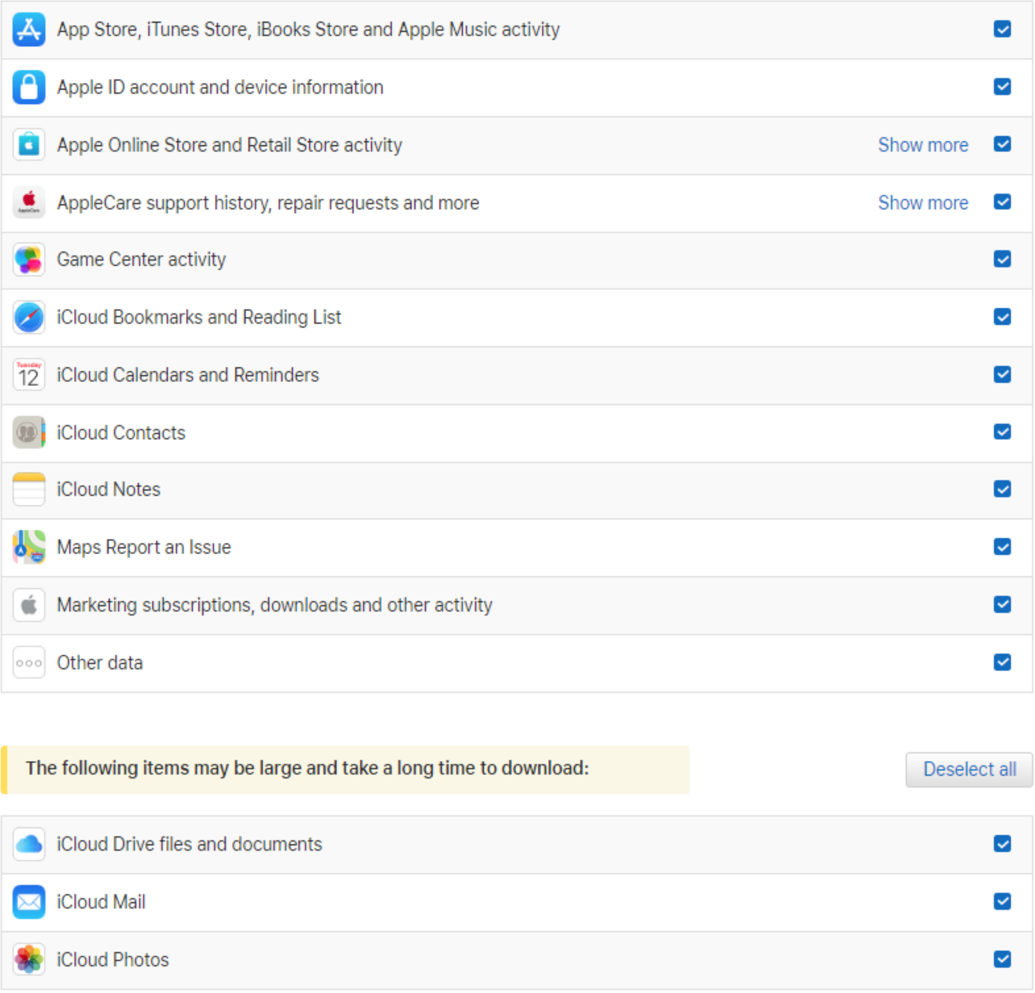


This process can take up to seven days. To ensure the security of your data, we use this time to verify that the request was made by you. We will notify you when your data is ready. You can check the status of your request at any time by visiting privacy.apple.com/account.

Apple and GDPR

And What Is Not

- **Certain things are missing**
- **Apple Pay** – never synced with iCloud
- **Screen Time** – why?
- **Messages** – additional encryption
  - We can decrypt it
- **Passwords** – iCloud Keychain has additional encryption
  - We can decrypt it



App Store, iTunes Store, iBooks Store and Apple Music activity ☑

Apple ID account and device information ☑

Apple Online Store and Retail Store activity Show more ☑

AppleCare support history, repair requests and more Show more ☑

Game Center activity ☑

iCloud Bookmarks and Reading List ☑

iCloud Calendars and Reminders ☑

iCloud Contacts ☑

iCloud Notes ☑

Maps Report an Issue ☑

Marketing subscriptions, downloads and other activity ☑

Other data ☑

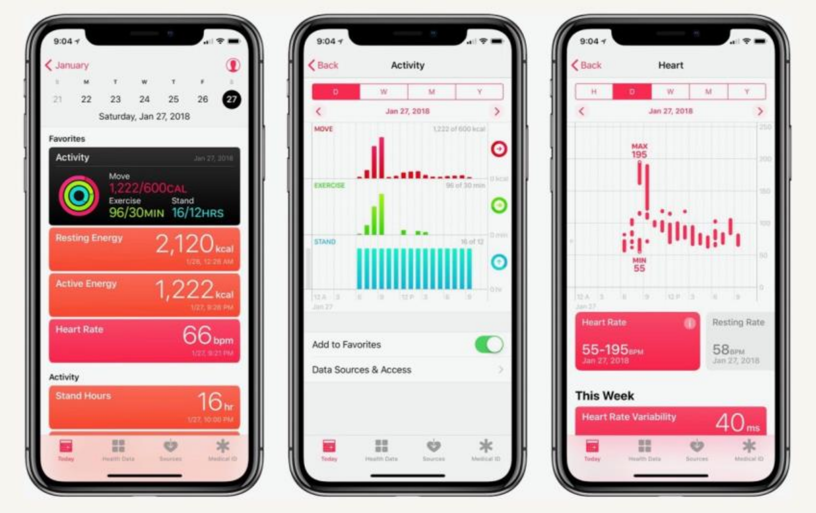
The following items may be large and take a long time to download: Deselect all

iCloud Drive files and documents ☑

iCloud Mail ☑

iCloud Photos ☑

Apple Health



Saturday, Jan 27, 2018

Favorites

Activity Jan 27, 2018
Move 1,222/600CAL
Exercise 96/30MIN
Stand 16/12HRS

Resting Energy 2,120 kcal 1/28, 12:28 AM

Active Energy 1,222 kcal 1/27, 9:28 PM

Heart Rate 66 bpm 1/27, 9:21 PM

Activity

Stand Hours 16 hr 1/27, 10:00 PM

Jan 27, 2018

MOVE 1,222 of 600 kcal

EXERCISE 96 of 30 min

STAND 16 of 12

Add to Favorites

Data Sources & Access

Jan 27, 2018

Heart Rate 55-195BPM Jan 27, 2018

Resting Rate 58BPM Jan 27, 2018

This Week

Heart Rate Variability 40 ms

- **Activity** – how much you move
- **Nutrition** – breakdown of your diet
- **Sleep** –your sleep habits
- **Mindfulness**

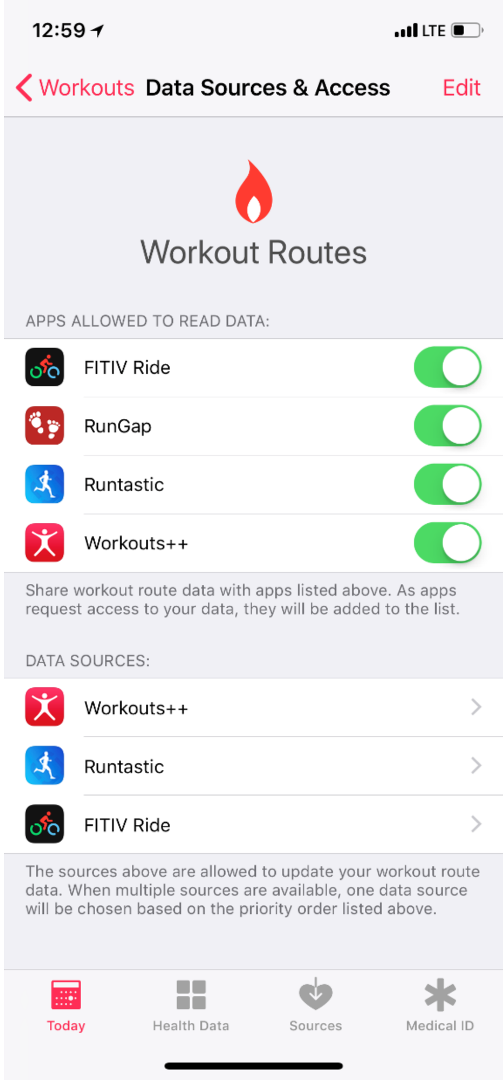
<u>**Additional data categories**</u>

- **Body Measurements** – height and weight
- **Health Records** - CDA + Health Records
- **Heart** – blood pressure, heart rate
- **Reproductive Health** – sexual activity and menstruation cycles
- **Results** – various medical test results (e.g. sugar level)
- **Vitals** – blood pressure, body temperature, heart rate, breathing rate
- **Medical ID** – essential medical data

Apple Health

Where Apple Health Gets Data From

- Data received from HealthKit devices (iPhone, Apple Watch, compatible fitness trackers etc.)
  - Automatic data submission
  - Pulse, blood pressure
  - Data for Mindfulness, Heart and Activity
  - Apple Watch collects Sleep data; **no automatic mode** (third-party apps can be used)
- Third-party apps (Nike+, Strava, Workouts++)
  - All data categories supported
  - Each data category has a list of “Recommended” third-party apps for collecting that type of data
  - Third-party apps must be activated in categories tracked in Health > Sources



Workout Routes

APPS ALLOWED TO READ DATA:

- FITIV Ride
- RunGap
- Runtastic
- Workouts++

Share workout route data with apps listed above. As apps request access to your data, they will be added to the list.

DATA SOURCES:

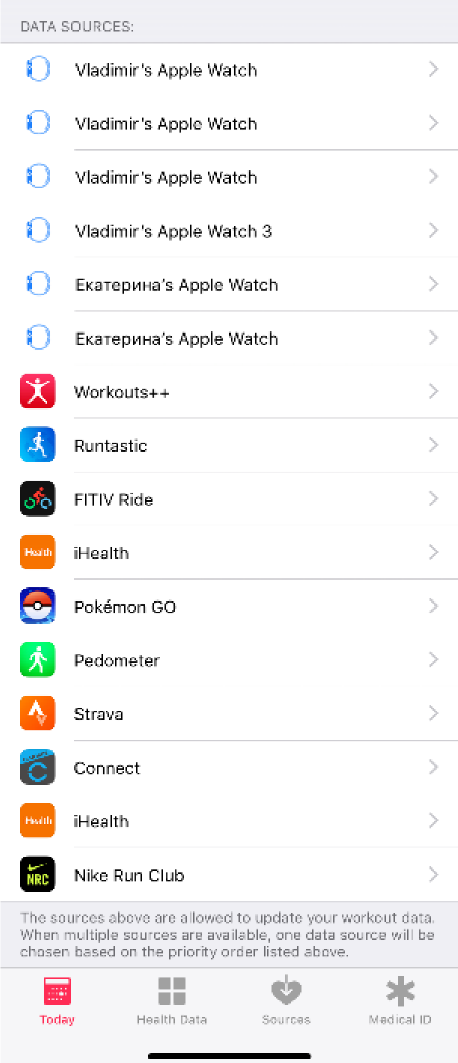
- Workouts++
- Runtastic
- FITIV Ride

The sources above are allowed to update your workout route data. When multiple sources are available, one data source will be chosen based on the priority order listed above.

Apple Health

How Apple Health Data Is Stored

- Main data stored at **/private/var/mobile/Library/Health/**
- Two linked SQLite databases: **healthdb.sqlite** and **healthdb_secure.sqlite**
- Training geodata: **healthdb_secure.hfd** (encrypted)



DATA SOURCES:

Vladimir's Apple Watch

Vladimir's Apple Watch

Vladimir's Apple Watch

Vladimir's Apple Watch 3

Екатерина's Apple Watch

Екатерина's Apple Watch

Workouts++

Runtastic

FITIV Ride

iHealth

Pokémon GO

Pedometer

Strava

Connect

iHealth

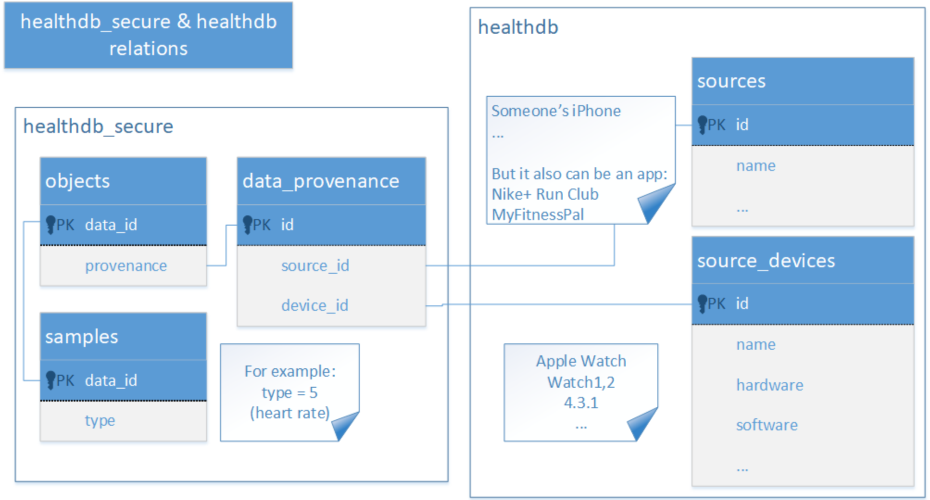
Nike Run Club

The sources above are allowed to update your workout data. When multiple sources are available, one data source will be chosen based on the priority order listed above.

Apple Health

Database Structures

- healthdb.sqlite mainly contains information about data sources
- healthdb_secure.sqlite stores basic health information with frequent links to the first DB



healthdb_secure & healthdb relations

healthdb_secure

objects
PK data_id
provenance

samples
PK data_id
type

data_provenance
PK id
source_id
device_id

For example:
type = 5
(heart rate)

healthdb

Someone's iPhone
…
But it also can be an app:
Nike+ Run Club
MyFitnessPal

sources
PK id
name
…

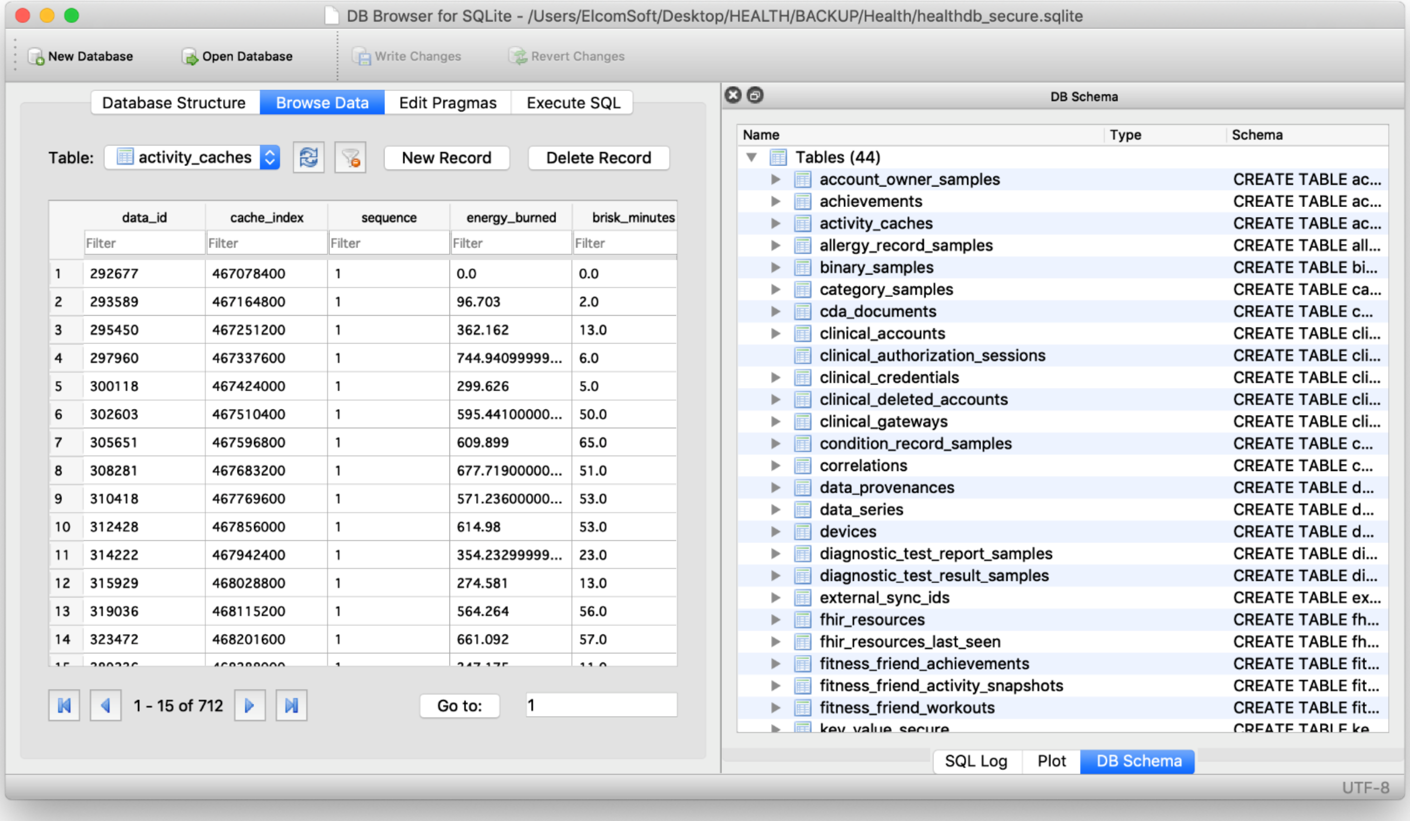
source_devices
PK id
name
hardware
software
…

Apple Watch
Watch1,2
4.3.1
…

Prior work

A Forensic Exploration of iOS Health Data (Heather Mahalik)
https://www.sans.org/summit-archives/file/summit-archive-1528385073.pdf

Apple Health



DB Browser for SQLite - /Users/ElcomSoft/Desktop/HEALTH/BACKUP/Health/healthdb_secure.sqlite

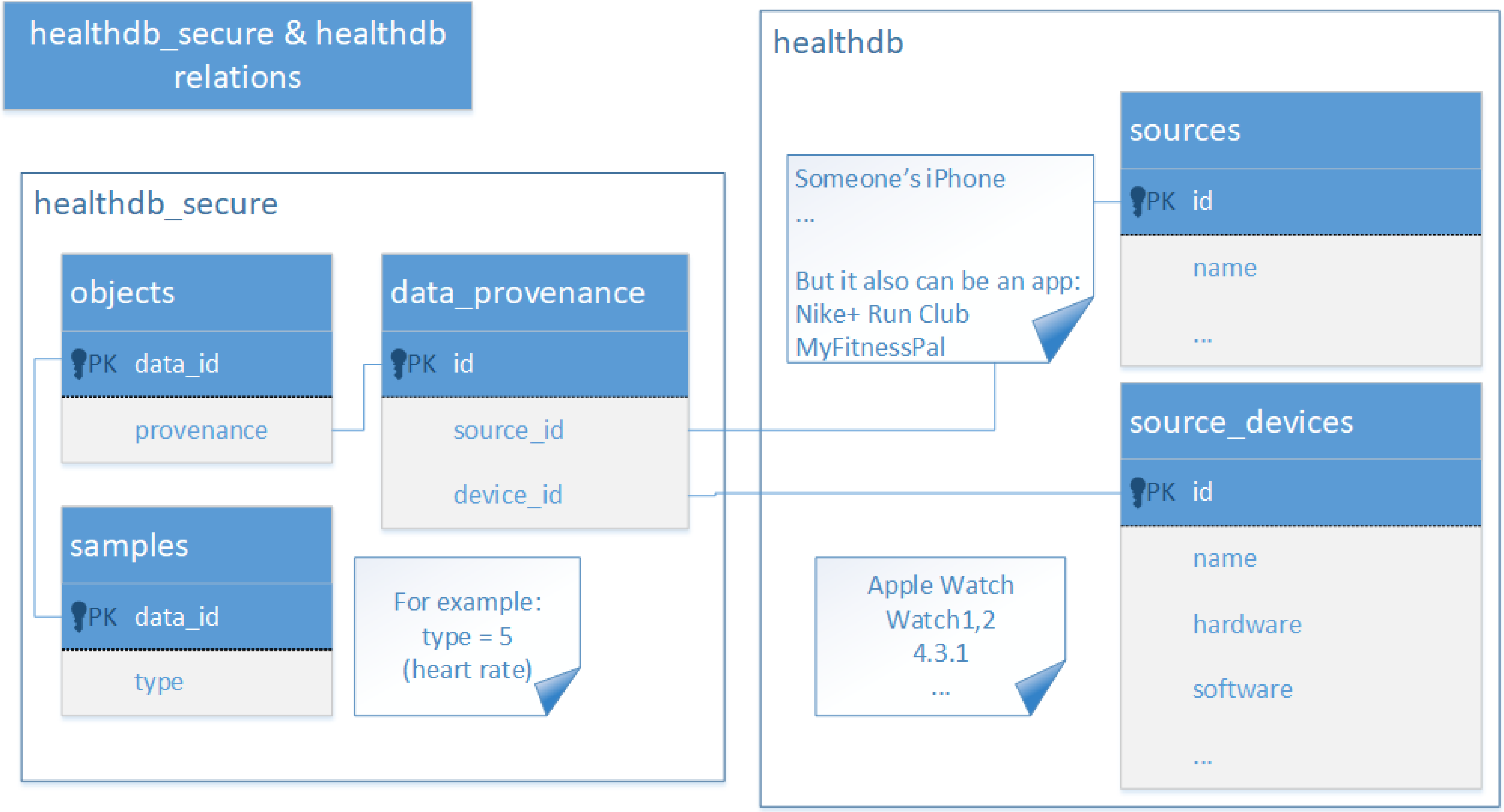
Table: activity_caches

	data_id	cache_index	sequence	energy_burned	brisk_minutes
	Filter	Filter	Filter	Filter	Filter
1	292677	467078400	1	0.0	0.0
2	293589	467164800	1	96.703	2.0
3	295450	467251200	1	362.162	13.0
4	297960	467337600	1	744.94099999...	6.0
5	300118	467424000	1	299.626	5.0
6	302603	467510400	1	595.44100000...	50.0
7	305651	467596800	1	609.899	65.0
8	308281	467683200	1	677.71900000...	51.0
9	310418	467769600	1	571.23600000...	53.0
10	312428	467856000	1	614.98	53.0
11	314222	467942400	1	354.23299999...	23.0
12	315929	468028800	1	274.581	13.0
13	319036	468115200	1	564.264	56.0
14	323472	468201600	1	661.092	57.0
15	380336	468288000	1	347.175	11.0

1 - 15 of 712

Go to: 1

Name	Type	Schema
Tables (44)		
account_owner_samples		CREATE TABLE ac...
achievements		CREATE TABLE ac...
activity_caches		CREATE TABLE ac...
allergy_record_samples		CREATE TABLE all...
binary_samples		CREATE TABLE bi...
category_samples		CREATE TABLE ca...
cda_documents		CREATE TABLE c...
clinical_accounts		CREATE TABLE cli...
clinical_authorization_sessions		CREATE TABLE cli...
clinical_credentials		CREATE TABLE cli...
clinical_deleted_accounts		CREATE TABLE cli...
clinical_gateways		CREATE TABLE cli...
condition_record_samples		CREATE TABLE c...
correlations		CREATE TABLE c...
data_provenances		CREATE TABLE d...
data_series		CREATE TABLE d...
devices		CREATE TABLE d...
diagnostic_test_report_samples		CREATE TABLE di...
diagnostic_test_result_samples		CREATE TABLE di...
external_sync_ids		CREATE TABLE ex...
fhir_resources		CREATE TABLE fh...
fhir_resources_last_seen		CREATE TABLE fh...
fitness_friend_achievements		CREATE TABLE fit...
fitness_friend_activity_snapshots		CREATE TABLE fit...
fitness_friend_workouts		CREATE TABLE fit...
key_value_secure		CREATE TABLE ke...



healthdb_secure & healthdb relations

healthdb_secure

objects
PK data_id
provenance

data_provenance
PK id
source_id
device_id

samples
PK data_id
type

For example:
type = 5
(heart rate)

healthdb

Someone's iPhone
...

But it also can be an app:
Nike+ Run Club
MyFitnessPal

sources
PK id
name
...

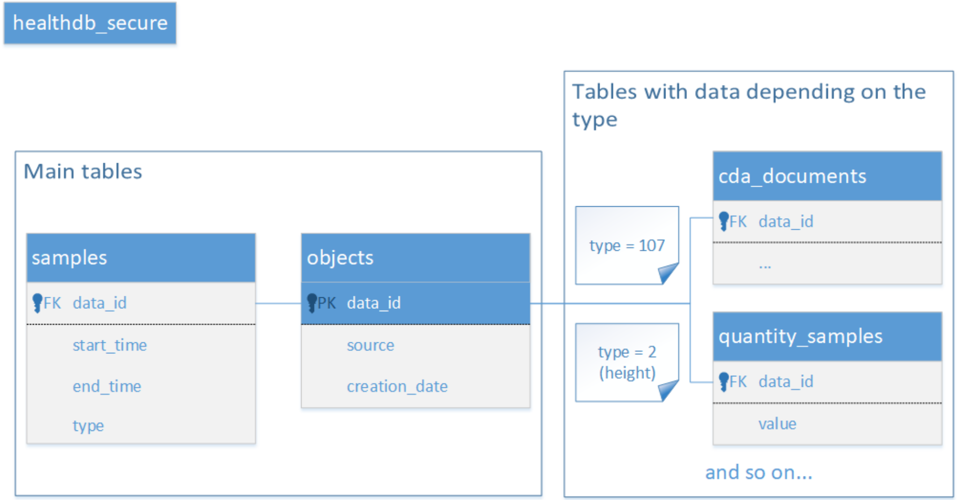
Apple Watch
Watch1,2
4.3.1
...

source_devices
PK id
name
hardware
software
...

Apple Health

healthdb_secure

- **objects**: information on “samples” including ID and source
- Samples contain information including timestamp, type, numerical data (e.g. “10 steps”) or category data (“test result positive”), and ID
- Samples are linked with “samples” table via ID
- Data values may be stored in various tables, e.g. **quantity_samples** or **cda_documents**



healthdb_secure

Main tables

samples
FK data_id
start_time
end_time
type

objects
PK data_id
source
creation_date

Tables with data depending on the type

type = 107

cda_documents
FK data_id
...

type = 2 (height)

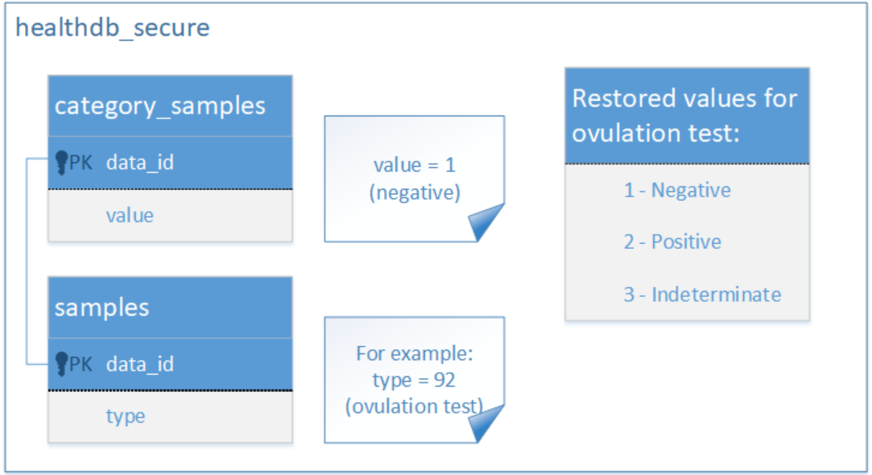
quantity_samples
FK data_id
value

and so on...

Apple Health

Category Samples

- Category samples contain non-numerical data
- Corresponds to list view selection in the app
- category_samples table stores these values
- Restoring category_samples values to meaningful data is essential for understanding Apple Health data



Researching healthdb_secure

Table	Description
objects	Sample’s uuid and source
samples	id, event type and time
quantity_samples	Source of numeric values
category_samples	Non-numerical category samples (e.g. “positive” or “negative” test result)
correlations	Keeps references to data instances, allowing to corellate quantitative data with activities
key_value_secure	Information about the user
metadata_values, metadata_keys	Sample metadata. Could be a note, time zone etc.
workouts,workout_events	Cumulative information about the workout: length, calories burned, distance walked, workout type etc.
fitness_friend_activity_snapshots	Data received via "share with friends & family". The contact is linked via an extra file ActivitySharing/contacts.dat. This file contains information about the contact (name, phone number and e-mail)
cda_documents	Binary data of a corresponding CDA document
data_provenance	Allows linking data sample with data source (device, app etc.)
unit_strings	Metric type (lb/kg etc.) from quantity_samples

Known healthdb tables

Table	Descripion
authorization	Authentication and sync data
cloud_sync_stores	Last sync data
key_value	App-specific values (e.g. if emergency sos mode is active)
source_devices	Information about devices the data was synced from
sources	Information on received data (source, modification date)
subscription_data_anchors	Data about synchronization
sync_stores	List of synchronization sources

Apple Health

Accessing Apple Health Data

- Export from Health app (XML)
- Local backup (encrypted only)
- File system acquisition (requires jailbreaking)
- GDPR request
- Government/LE request
- Cloud extraction

Apple Health

Extracting Apple Health Data: The Easy Way

- Apple Health is available via logical acquisition
- **No Apple Health data in unencrypted backups!**
    - Unlike keychain, which is still present in unencrypted backups, protected with a hardware key
- Set a known password before making a backup
- Make local backup with iTunes
- Decrypt backup, access Apple Health data
- View with forensic software (or analyse databases manually)

Apple Health

Extracting Apple Health Data: The Complex Way

- Apple Health is available via file system acquisition
- **Jailbreak required**
    - At this time, jailbreak is available for all versions of iOS from 8 to 11.3.1
- Jailbreak, use ssh (or forensic software)
- Obtain TAR image
- View with forensic software (or analyse databases manually)
- *Needed only if backup if password-protected*

Apple Health

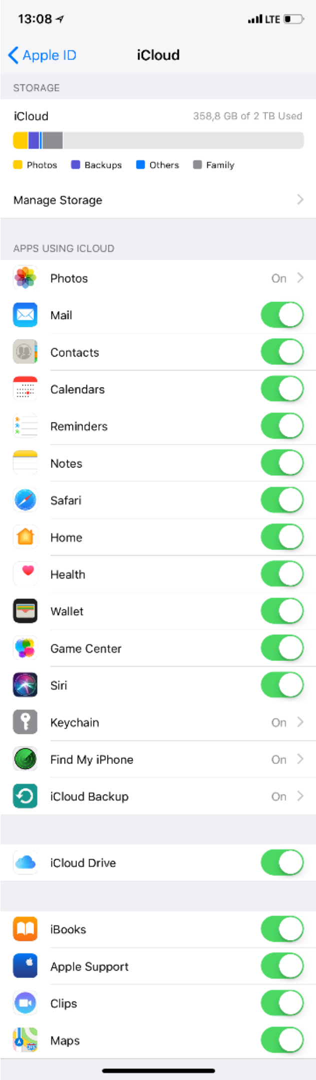
Extracting Apple Health Data: GDPR

- EU users can access their Health data by pulling a GDPR request
- Registering GDPR request: **privacy.apple.com**
- **Apple ID, password, 2FA required**
- Takes up to 7 days to receive the data
- Multiple binary and text formats

Apple Health

Apple Health and Cloud

- Native Apple Health data is synced with iCloud to all registered devices
- Third-party apps operate through HealthKit
- Some third-party app data is not shared with Apple Health
- Certain apps use proprietary cloud sync (Strava, Endomondo)
- **Medical ID** data is unique per device and **does not sync**
- **CDA records** do not sync (to the best of our knowledge)



13:08 LTE

< Apple ID iCloud

STORAGE

iCloud 358,8 GB of 2 TB Used

Photos Backups Others Family

Manage Storage >

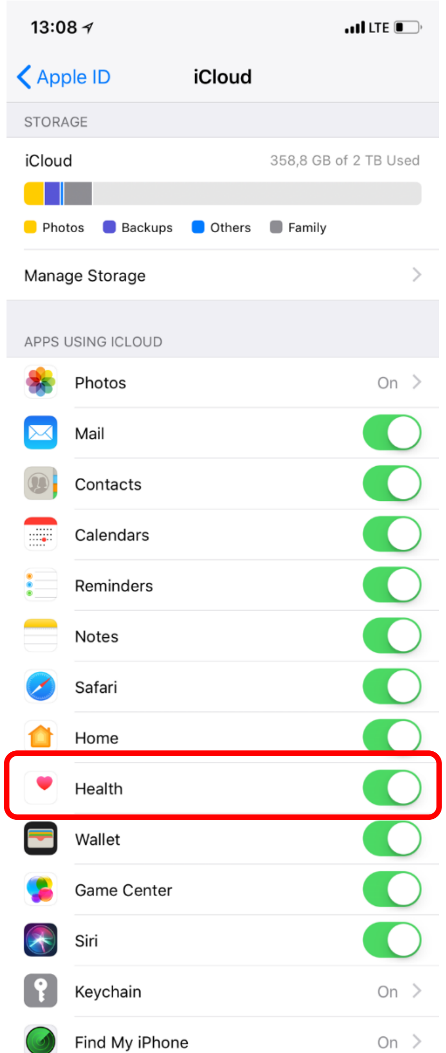
APPS USING ICLOUD

Photos	On >
Mail	☑
Contacts	☑
Calendars	☑
Reminders	☑
Notes	☑
Safari	☑
Home	☑
Health	☑
Wallet	☑
Game Center	☑
Siri	☑
Keychain	On >
Find My iPhone	On >
iCloud Backup	On >
iCloud Drive	☑
iBooks	☑
Apple Support	☑
Clips	☑
Maps	☑

Apple Health

Apple Health and iCloud

- Apple Health data **can** be obtained from iCloud
- May contain significantly more information compared to what is available on device
- Technically, Apple Health belongs to “synced data” as opposed to “cloud backups”
    - This results in significantly more reliable extraction
    - Loose expiration rules of iCloud tokens compared to backups



13:08 LTE

< Apple ID iCloud

STORAGE

iCloud 358,8 GB of 2 TB Used

🟨 Photos 🟪 Backups 🟦 Others ⬜ Family

Manage Storage >

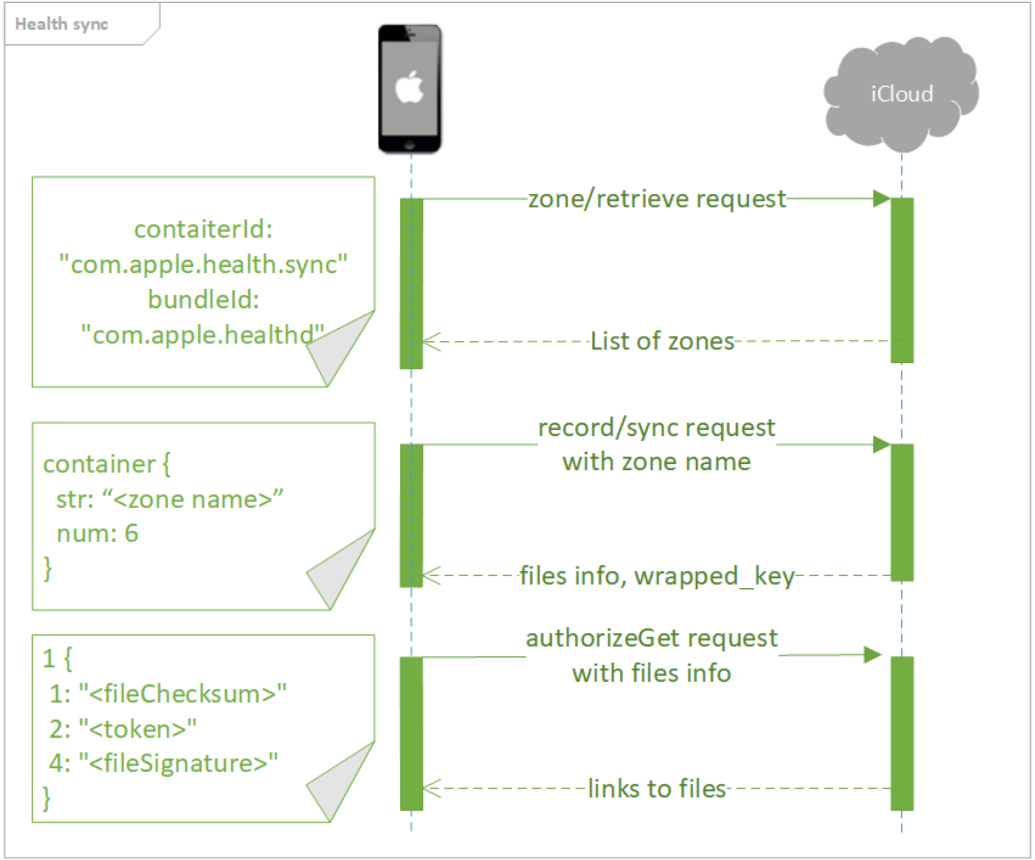
APPS USING ICLOUD

Photos	On >
Mail	●
Contacts	●
Calendars	●
Reminders	●
Notes	●
Safari	●
Home	●
Health	●
Wallet	●
Game Center	●
Siri	●
Keychain	On >
Find My iPhone	On >

Apple Health

Accessing Health Data

- Receive encrypted file chunks
- Request zone list
- Request zone sync
- Request file links
- Download files



```
containterId:
"com.apple.health.sync"
bundleId:
"com.apple.healthd"
```

```
container {
  str: "<zone name>"
  num: 6
}
```

```
1 {
 1: "<fileChecksum>"
 2: "<token>"
 4: "<fileSignature>"
}
```

Apple Health

```
contaiterId: "com.apple.health.sync"
bundleId: "com.apple.healthd"
```

Request Zone List

- All zones start with PrimarySyncCircle
- Followed by zone UUID, e.g. 1AA8B4D0-9B73-4D88-A740-BFE04DD8A5AC
- New zones created with logging in or on subsequent logins
- Zones are periodically merged

Apple Health

Request Zone Sync

- Request / Result:

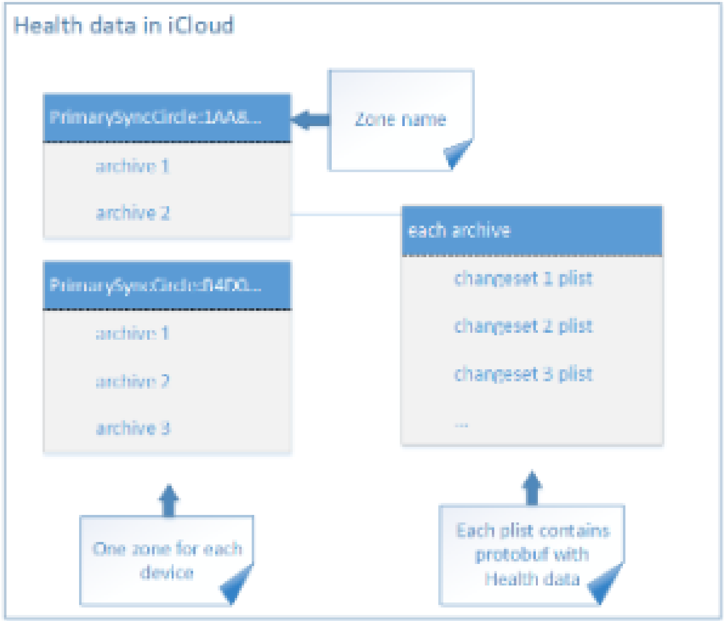
```
container {
 str: "PrimarySyncCircle:AF64D6
29-3688-4062-9503-BE97B45D5BC2"
 num: 6
}
```

```
propertyName {
 name: "ChangeSet"
}
propertyValue {
 valueType: 6
 authInfo {
  owner1Dsid: "8888888888"
  fileChecksum: "\001\233\254\2671GQ\316\324mM\243\031\254\322|\017\364\233N\
f"
  structSize: 13465
  token: "B3B9SvMwRNXBK6fGaX6vOuVLwfbWA1H5QwEAAAMR7kM"
  url: "https://p29-content.icloud.com:443"
  owner2Dsid: "8888888888"
  wrapped_key {
   name: "\003_\242\000\335\266\255\312\0304\226e\344\333\235\227\226a\266\32
3H\364\021DM3\341\020~B\337O\346\016\017\357\375C[\346\301\311\356\261"
  }
  fileSignature: "\001\310\273\331\332\326a\337\202Xd\035e`p\277\321\226\211\
222\312"
  downloadTokenExpiration: 1529588220
 }
}
```

Apple Health

Download Files

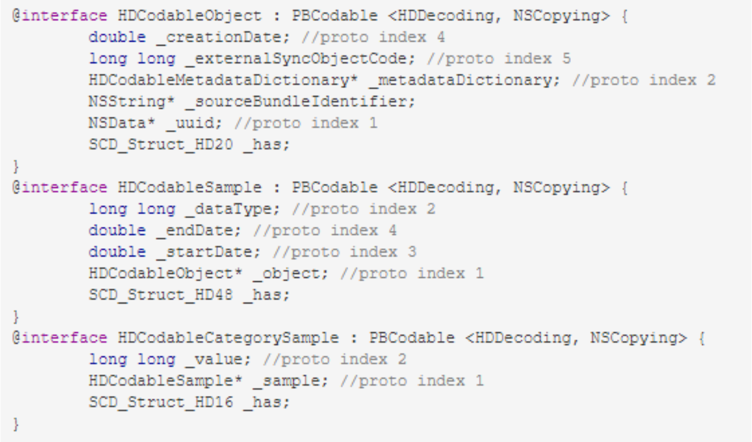
- Files from the list are downloaded by chunks
- Downloaded chunks must be decrypted
- record/sync request returns encrypted key (wrapped_key)
- Key is decrypted
- We’ve got a key for unwrapping encryption keys that accompany each chunk
- These keys are unwrapped with wrapped_key and are used to decrypt the chunks
- Decrypted chunks are merged into files



Apple Health

Sounds too simple?

- Synced data is received in protobuf structures
- Received structures are serialized objects described in HealthDaemon header files
- There are several types of Protobuf structures



```
@interface HDCodableObject : PBCodable <HDDecoding, NSCopying> {
        double _creationDate; //proto index 4
        long long _externalSyncObjectCode; //proto index 5
        HDCodableMetadataDictionary* _metadataDictionary; //proto index 2
        NSString* _sourceBundleIdentifier;
        NSData* _uuid; //proto index 1
        SCD_Struct_HD20 _has;
}
@interface HDCodableSample : PBCodable <HDDecoding, NSCopying> {
        long long _dataType; //proto index 2
        double _endDate; //proto index 4
        double _startDate; //proto index 3
        HDCodableObject* _object; //proto index 1
        SCD_Struct_HD48 _has;
}
@interface HDCodableCategorySample : PBCodable <HDDecoding, NSCopying> {
        long long _value; //proto index 2
        HDCodableSample* _sample; //proto index 1
        SCD_Struct_HD16 _has;
}
```

Apple Health

Accessing Health Data in iCloud

We can download **synced data**, which includes Apple Health

What can go wrong:

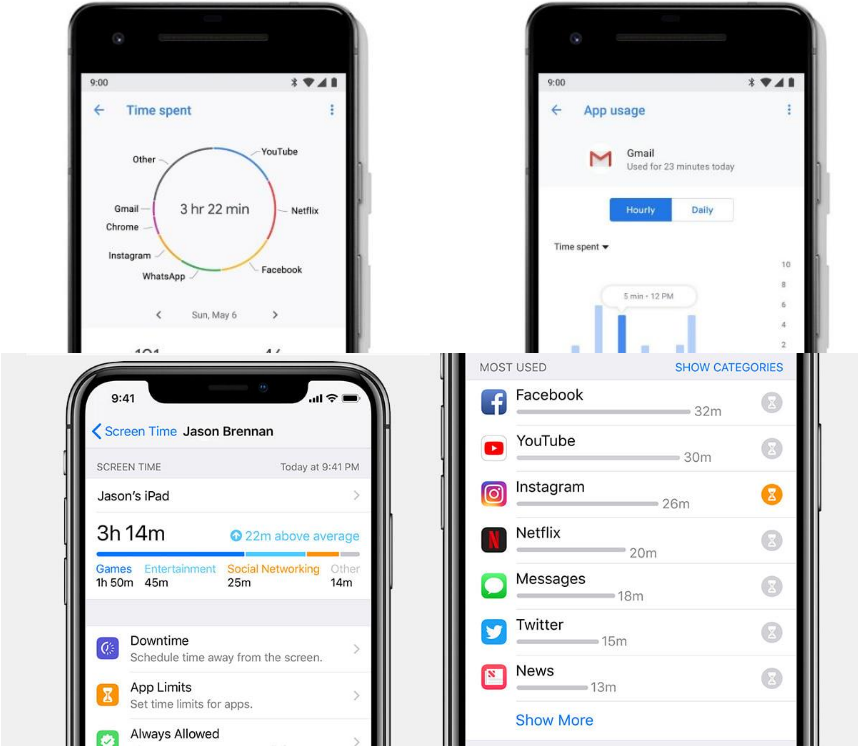
- Two-factor authentication may be an issue
- Access to secondary authentication factor is required (unless using authentication token)

Sign in to iCloud
Apple ID
Password
Keep me signed in
Forgot Apple ID or password?
Don't have an Apple ID? Create yours now.

Smartphone Privacy

Your Smartphone Knows More About Your Life

- Both Apple and Google introduced user-accessible usage stats
- Details application usage and categories
- Time spent in Games, Entertainment, Social Networking and other activities
- Daily, hourly and weekly statistics



9:00

Time spent

9:00

App usage

Gmail
Used for 23 minutes today

9:41

Screen Time Jason Brennan

SCREEN TIME Today at 9:41 PM

Jason's iPad

3h 14m 22m above average

Games	Entertainment	Social Networking	Other
1h 50m	45m	25m	14m

Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

Always Allowed

MOST USED SHOW CATEGORIES

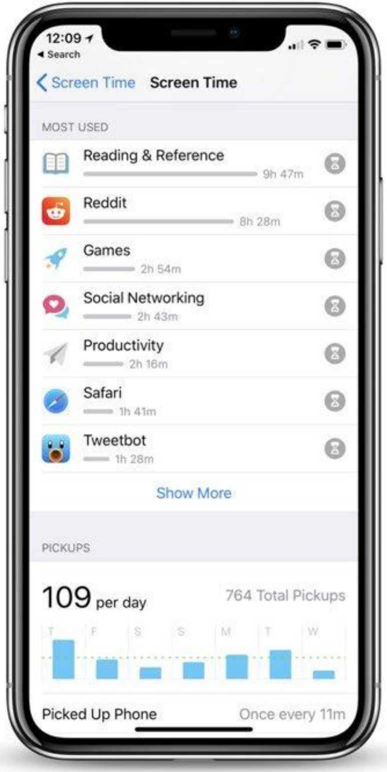
Facebook	32m
YouTube	30m
Instagram	26m
Netflix	20m
Messages	18m
Twitter	15m
News	13m

Show More

Smartphone Privacy

iOS 12 Screen Time: Statistics

- Daily and weekly reports
- Per category statistics and enforceable time limits
- Per app tracking
- Track how many times you picked up your phone



12:09
◂ Search

‹ Screen Time **Screen Time**

MOST USED

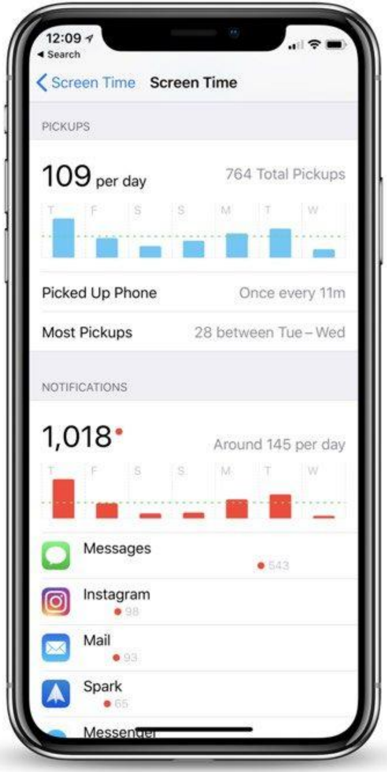
Reading & Reference	9h 47m
Reddit	8h 28m
Games	2h 54m
Social Networking	2h 43m
Productivity	2h 16m
Safari	1h 41m
Tweetbot	1h 28m

Show More

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m



12:09
◂ Search

‹ Screen Time **Screen Time**

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m

Most Pickups 28 between Tue – Wed

NOTIFICATIONS

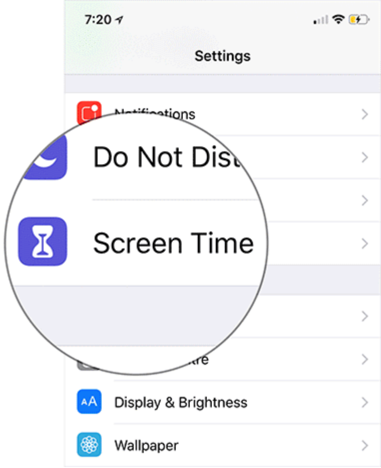
1,018 Around 145 per day

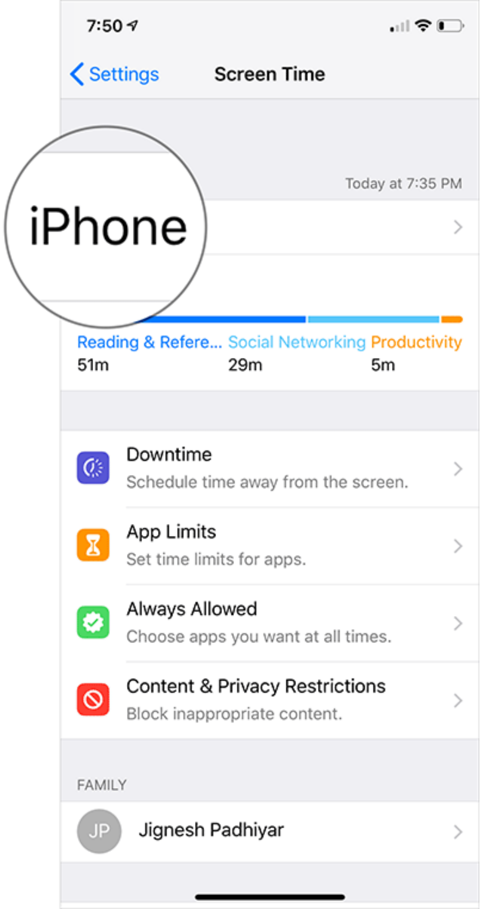
Messages	543
Instagram	98
Mail	93
Spark	65
Messenger	

Smartphone Privacy

iOS 12 Screen Time: Restrictions

- Track or restrict time spent on Gaming, Entertainment, Social Networking, Reading & Reference and other activities
- Track and restrict individual applications
- Set downtime and app limits
- Content and privacy restrictions
- Screen Time Passcode





Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

Always Allowed
Choose apps you want at all times.

Content & Privacy Restrictions
Block inappropriate content.

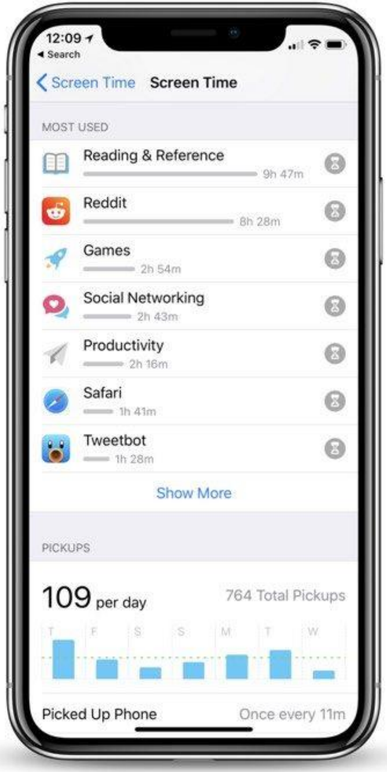
FAMILY

JP Jignesh Padhiyar

Smartphone Privacy

iOS 12 Screen Time: Statistics

- Daily and weekly reports
- Per category statistics and enforceable time limits
- Per app tracking
- Track how many times you picked up your phone



12:09

◂ Search

‹ Screen Time Screen Time

MOST USED

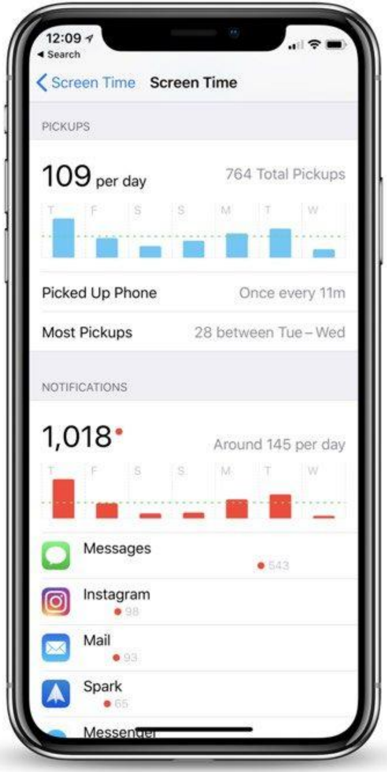
Reading & Reference	9h 47m
Reddit	8h 28m
Games	2h 54m
Social Networking	2h 43m
Productivity	2h 16m
Safari	1h 41m
Tweetbot	1h 28m

Show More

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m



12:09

◂ Search

‹ Screen Time Screen Time

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m

Most Pickups 28 between Tue – Wed

NOTIFICATIONS

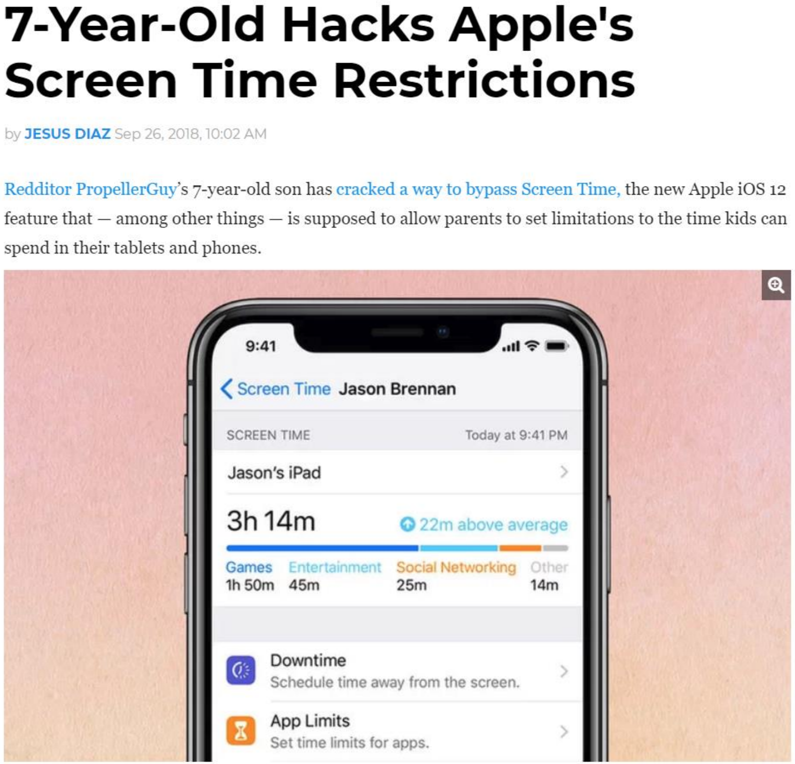
1,018 Around 145 per day

Messages	543
Instagram	98
Mail	93
Spark	65
Messenger	

Smartphone Privacy

iOS 12 Screen Time: iCloud Sync

- See how you use apps across multiple devices
- Downtime and App Limits sync through iCloud
- Restrictions and limits automatically applied to all devices
- Usage data syncs to all devices on the same Apple ID
  - So that you can't cheat the system
  - Unless you're 7 years old



7-Year-Old Hacks Apple's Screen Time Restrictions

by JESUS DIAZ Sep 26, 2018, 10:02 AM

Redditor PropellerGuy's 7-year-old son has cracked a way to bypass Screen Time, the new Apple iOS 12 feature that — among other things — is supposed to allow parents to set limitations to the time kids can spend in their tablets and phones.

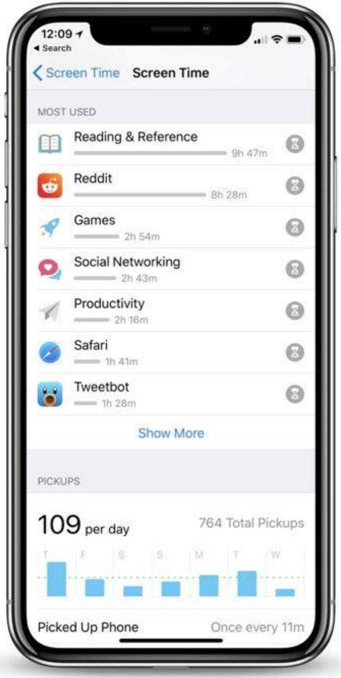
Smartphone Privacy

iOS 12 Screen Time: knowledge.db

- **Screen Time** is based on information collected in **knowledgeC.db** database

  /private/var/mobile/Library/CoreDuet/Knowledge/KnowledgeC.db

- **SQLite** format
- knowledgeC.db available since iOS 9



12:09
◂ Search

< Screen Time Screen Time

MOST USED

Reading & Reference 9h 47m

Reddit 8h 28m

Games 2h 54m

Social Networking 2h 43m

Productivity 2h 16m

Safari 1h 41m

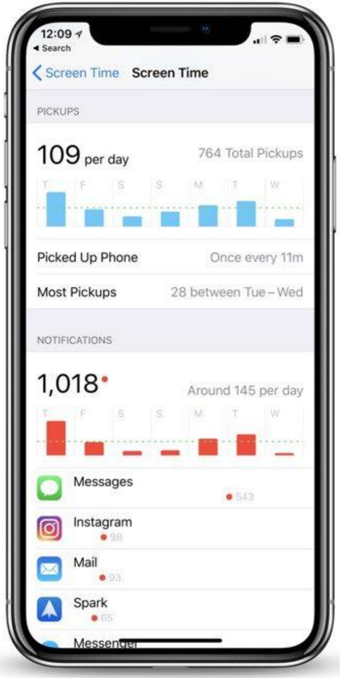
Tweetbot 1h 28m

Show More

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m



12:09
◂ Search

< Screen Time Screen Time

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m

Most Pickups 28 between Tue – Wed

NOTIFICATIONS

1,018 Around 145 per day

Messages 543

Instagram 98

Mail 93

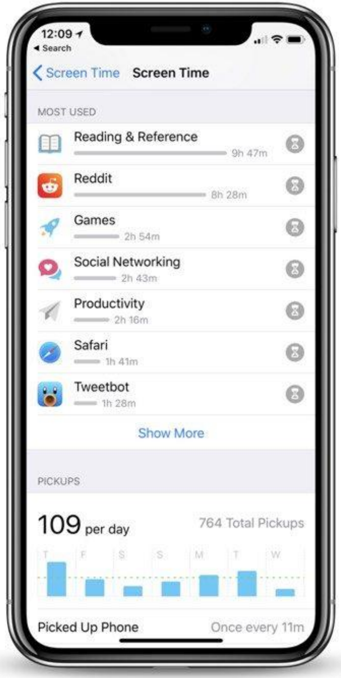
Spark 65

Messenger

Smartphone Privacy

iOS 12 Screen Time: Conclusion

- **Apple knows how you use your devices in great detail**
- **They store it on their servers:**
- Statistics and reporting
  - With iCloud sync
- Loosely enforceable restrictions
  - With iCloud sync



12:09
◂ Search

< Screen Time Screen Time

MOST USED

Reading & Reference 9h 47m

Reddit 8h 28m

Games 2h 54m

Social Networking 2h 43m

Productivity 2h 16m

Safari 1h 41m

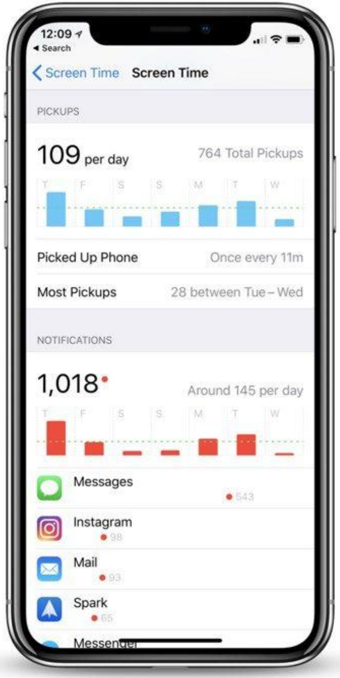
Tweetbot 1h 28m

Show More

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m



12:09
◂ Search

< Screen Time Screen Time

PICKUPS

109 per day 764 Total Pickups

Picked Up Phone Once every 11m

Most Pickups 28 between Tue – Wed

NOTIFICATIONS

1,018 Around 145 per day

Messages 543

Instagram 98

Mail 93

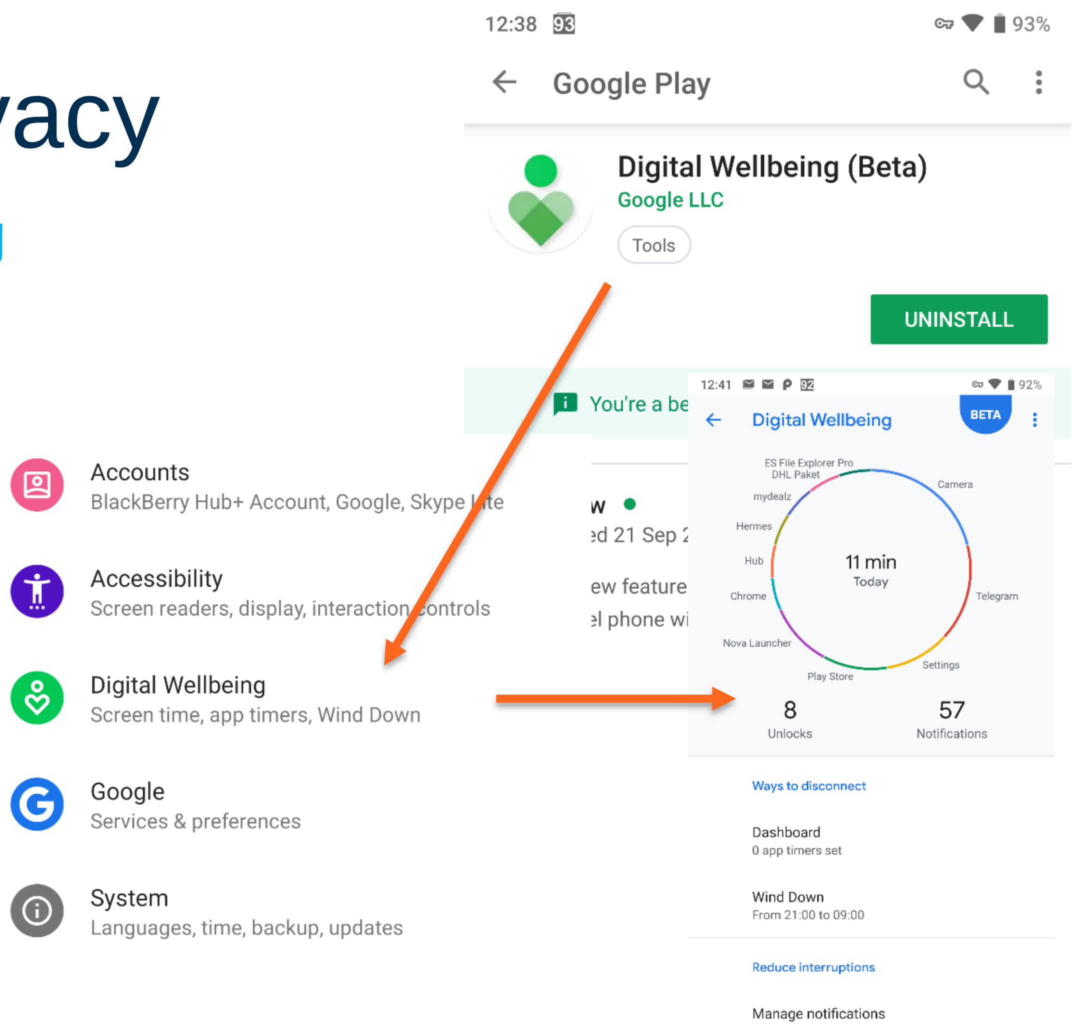
Spark 65

Messenger

Smartphone Privacy

Google: Digital Wellbeing

- Available in Android Pie
- Currently in beta, only on Pixels
- Must be downloaded from Google Play
- Accessible via Settings
- Daily overview
  - Unlocks
  - Notifications
  - Pie chart: app usage time



12:38 93 93%

Google Play

Digital Wellbeing (Beta)

Google LLC

Tools

UNINSTALL

You're a be

w ●

ed 21 Sep 2

ew feature

el phone wi

Accounts
BlackBerry Hub+ Account, Google, Skype Lite

Accessibility
Screen readers, display, interaction controls

Digital Wellbeing
Screen time, app timers, Wind Down

Google
Services & preferences

System
Languages, time, backup, updates

12:41 92 92%

Digital Wellbeing BETA

8 Unlocks

57 Notifications

Ways to disconnect

Dashboard
0 app timers set

Wind Down
From 21:00 to 09:00

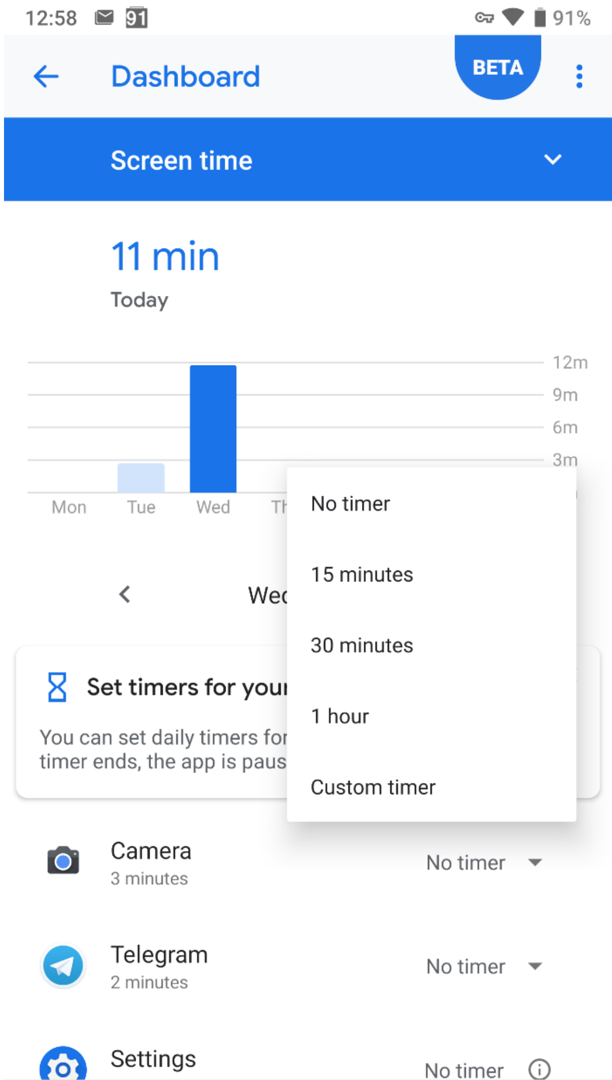
Reduce interruptions

Manage notifications

Smartphone Privacy

Digital Wellbeing: What’s Reported

- **Per app screen time**
  - How much time you spent in each app
- Daily reports
- Custom timers
  - Per app only
  - No categories!
  - Enforced on this device only
  - No cloud sync!



11 min
Today

Set timers for your

You can set daily timers for
timer ends, the app is paus

Camera
3 minutes
No timer

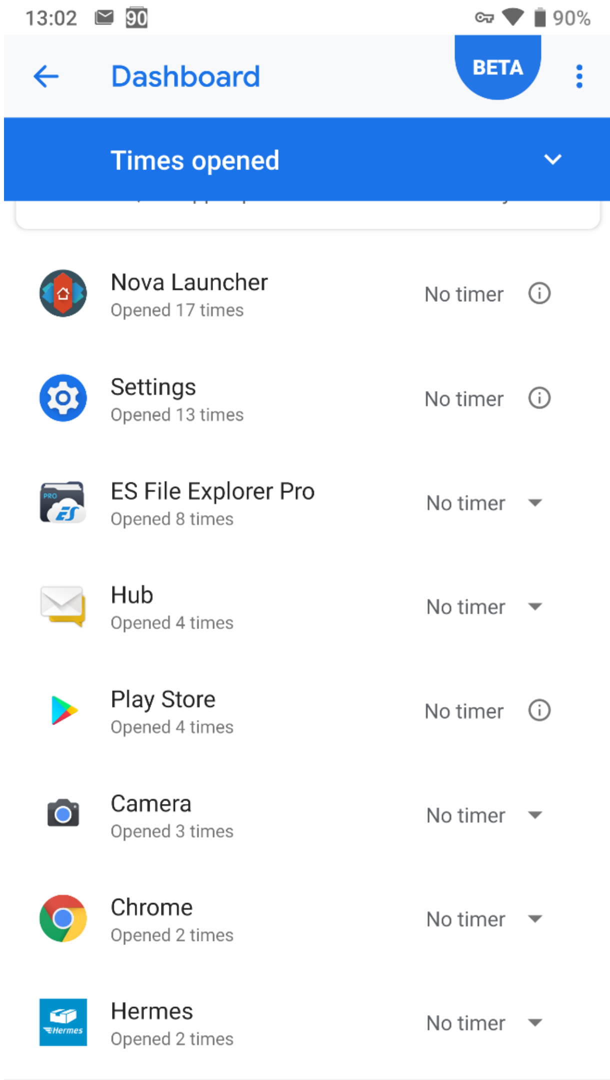
Telegram
2 minutes
No timer

Settings
No timer

Smartphone Privacy

Digital Wellbeing: What’s Reported

- Per app times opened
  - How frequently you used each app
- Daily reports
- Custom timers: screen time only (no limit on how many times the app can be launched)
  - Per app only
  - No categories!
  - Enforced on this device only
  - No cloud sync!



13:02 90%

Dashboard BETA

Times opened

Nova Launcher	Opened 17 times	No timer
Settings	Opened 13 times	No timer
ES File Explorer Pro	Opened 8 times	No timer
Hub	Opened 4 times	No timer
Play Store	Opened 4 times	No timer
Camera	Opened 3 times	No timer
Chrome	Opened 2 times	No timer
Hermes	Opened 2 times	No timer

Smartphone Privacy

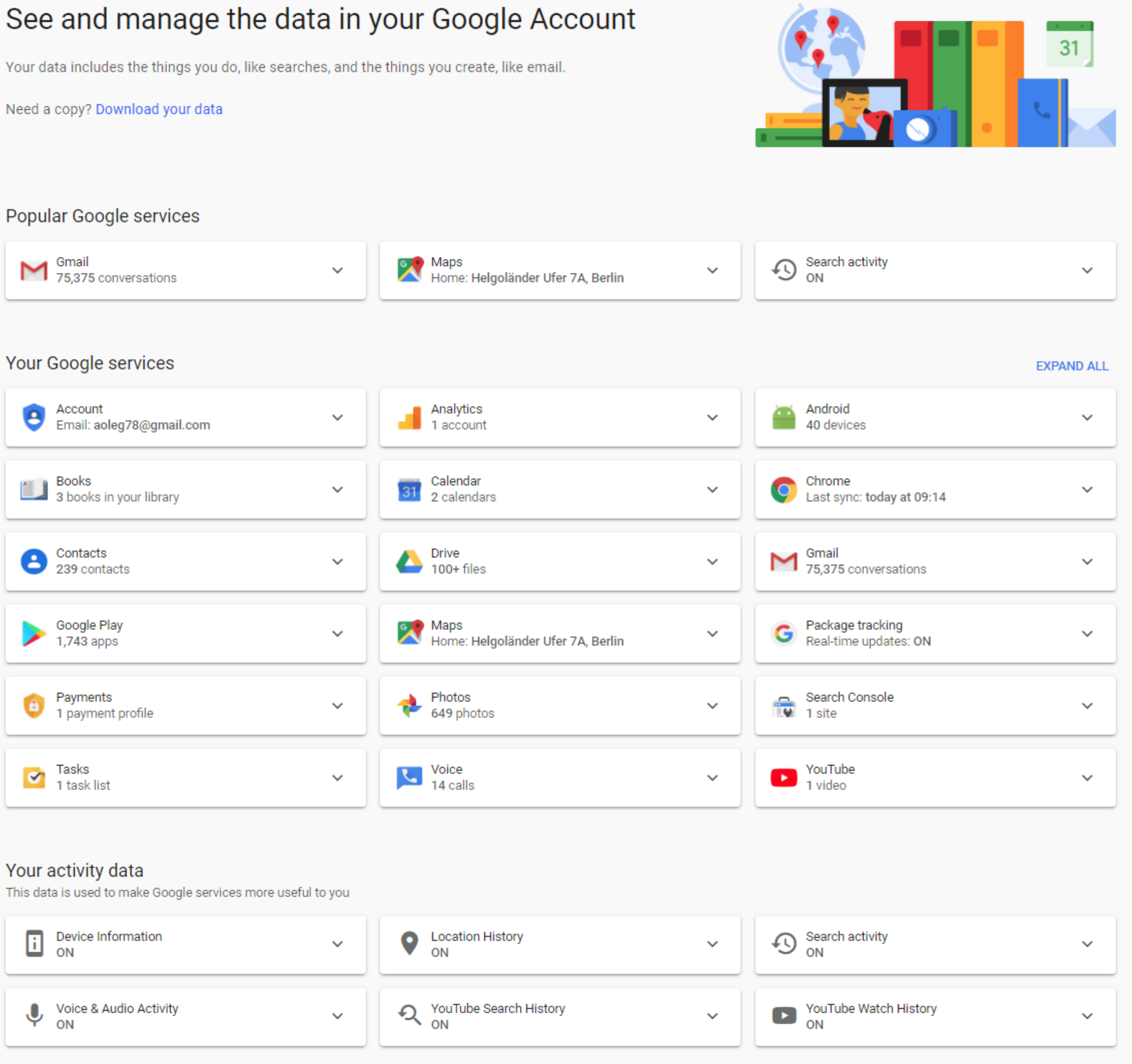
Apple Screen Time vs. Google Digital Wellbeing

- Apple Screen Time
  - Per app and per category statistics
  - Daily and weekly reports
  - iCloud sync to all user’s devices
    - Both usage and restrictions
  - Downtime
  - Restrictions passcode
  - No notification stats

- Google Digital Wellbeing
  - Per app statistics only
  - Daily reports
  - No sync with Google Account
    - Nothing gets synced
  - Wind Down
  - No restrictions passcode
  - Statistics on number of notifications

Google Dashboard

- Apple syncs Screen Time
- Google does not sync Digital Wellbeing
  - Android 9 runs in less than 0.1% of devices anyway
- Does Google know less about its users?
- *No!*
- **Google Dashboard** has significantly more information than Screen Time and Digital Wellbeing combined



See and manage the data in your Google Account

Your data includes the things you do, like searches, and the things you create, like email.

Need a copy? Download your data

Popular Google services

Gmail 75,375 conversations	Maps Home: Helgoländer Ufer 7A, Berlin	Search activity ON

Your Google services

EXPAND ALL

Account Email: aoleg78@gmail.com	Analytics 1 account	Android 40 devices
Books 3 books in your library	Calendar 2 calendars	Chrome Last sync: today at 09:14
Contacts 239 contacts	Drive 100+ files	Gmail 75,375 conversations
Google Play 1,743 apps	Maps Home: Helgoländer Ufer 7A, Berlin	Package tracking Real-time updates: ON
Payments 1 payment profile	Photos 649 photos	Search Console 1 site
Tasks 1 task list	Voice 14 calls	YouTube 1 video

Your activity data

This data is used to make Google services more useful to you

Device Information ON	Location History ON	Search activity ON
Voice & Audio Activity ON	YouTube Search History ON	YouTube Watch History ON

Smartphone Privacy

Your Smartphone Tracks Your Location

- Precise
- Energy-efficient
- Constantly running unless explicitly disabled
- Sometimes running even if explicitly disabled
  https://www.bbc.com/news/technology-45183041
  https://www.macrumors.com/2018/08/13/google-location-history-disabled-still-stores-data/

Smartphone Privacy

Who Tracks Your Location?

- Google (iOS, Android, desktop – Chrome, Google services in any browser)
- Apple (iOS, macOS)
- Facebook (on all platforms)
- Countless third-party apps and services
  - Even if location is disabled
  - Yes, it is possible

Smartphone Privacy

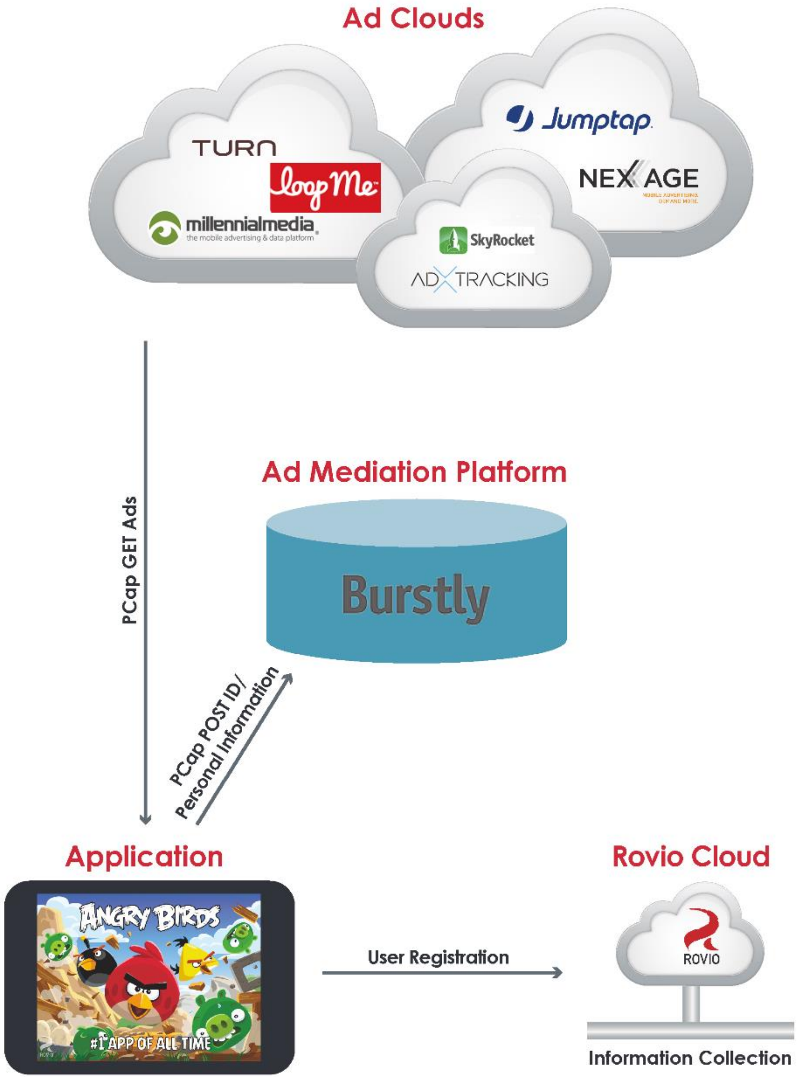
Why Google, Apple and FB track your Location?

- **To serve you better**
  - Google/Apple Maps, navigation
  - FB: local groups & events
  - Much more relevant search results
  - Find My Phone / Find My Device
  - Convenience: know how busy that restaurant is at this time of day or even **right now**
  - Indoor navigation (with beacons)
- **To sell ads**
  - Google’s main source of income
  - Location-based ads
  - Facebook: major advertisement network
- **To sell your data**
  - Apple & Google do not sell location data
  - Facebook does

Smartphone Privacy

Third-Party Apps Tracking

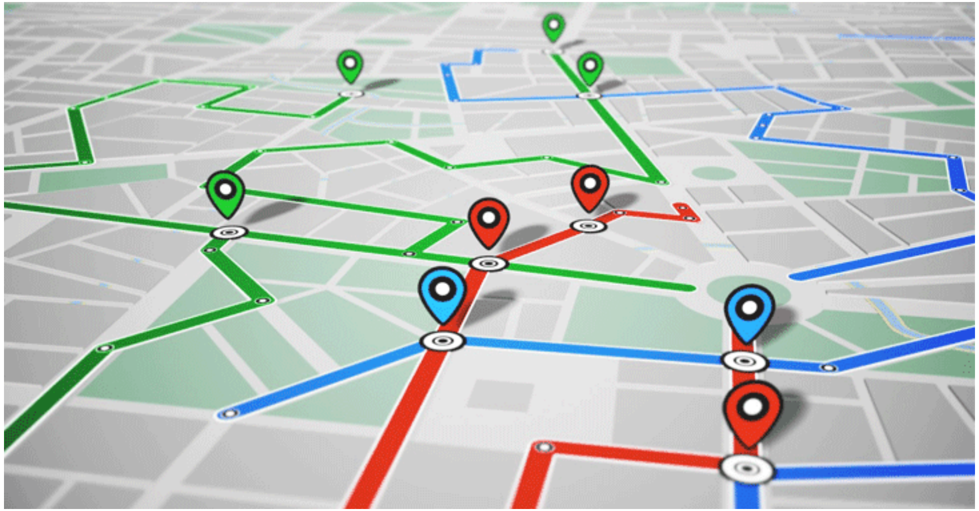
- **Collecting location, contacts, phone usage patterns and much more**
- To serve you better:
  - You really thought that game was free?
- To sell your data:
  - Multiple brokers buy this sort of data
  - Location data collected from everywhere
  - Including Wi-Fi networks and reverse BSSID lookup
  - Even IP address used as source of location data



Smartphone Privacy

Where location data is stored?

- Physical devices (iOS, Android, Windows, macOS X, other systems)
- Apple iCloud
- Google account
- Third-party cloud accounts
  - Social networks
  - Health & fitness applications
  - Instant messengers
  - Dating apps
  - Taxi apps
  - PoI/travel apps



Smartphone Privacy

How Apple Stores Location Data

- Location data is stored as:
  - Database records
  - PLIST values
  - JSON values
  - Mixed PLIST/JSON structures as database records
  - Log files (plain text)
- Where?
  - System databases (related to services/daemons)
  - Built-in apps data
  - Temporary/cached data
  - iCloud

Smartphone Privacy

What Apple Collects

- Collected data depends on the source and storage
- These items are always present:
  - **Latitude**
  - **Longitude**
  - **Timestamp** (mainly in UNIX Epoch format)
  - We've seen location records without timestamps
  - We have seen location names/IDs without lat/lon
- These items may be additionally available:
  - **Altitude**
  - **Accuracy** – how accurate the measurement is (can be represented as a circle with a given radius)
  - **Confidence** – how confident the system is about the stated accuracy
  - **Min/Max latitude and longitude** – yet another representation of accuracy. Can be represented as a rectangular area
  - **Speed**
  - **Course** – represents angle of turns in degrees
  - **End Date** – date when device left location
  - **Address** – street address; can be stored as a string or as multiple items

Smartphone Privacy

Routes

- Routes can be tracked on device or in the app
  - Can take speed, course, angle (magnetic compass) values into account
  - Routes stored on device
- Routes can be calculated in forensic software based on individual location records
  - Based on recorded locations
  - Can be calculated based on location records obtained from multiple sources (e.g. Maps, third-party apps, system logs etc.)

Smartphone Privacy

iTunes Backups: Sources of Location Data

- *Local (iTunes) backups are a major source of evidence*
- *Backups contain location data (not as much as stored on physical device)*

- Apple Maps
- Calendar
- Media (EXIF)
- Wallet
- Multiple third-party apps data and cache

- Location cache
- Frequent / Significant Locations
- Locations cached during media files analysis
- Apple Pay locations

Smartphone Privacy

Media (EXIF)

- Windows, macOS, iOS, Android
- Windows: File Properties > Details > GPS
- macOS: More Info > Latitude and Longitude
- Third-party software can map location data
- Forensic software extracts EXIF tags, parses location data, builds routes

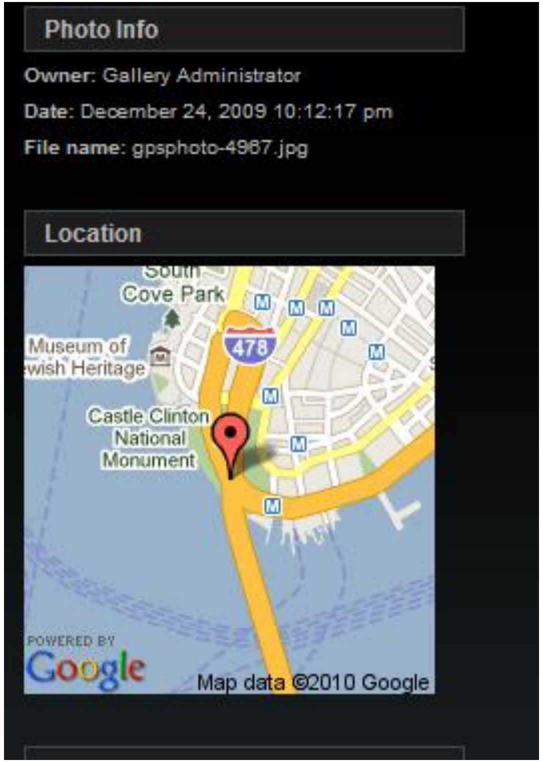


Photo Info

Owner: Gallery Administrator

Date: December 24, 2009 10:12:17 pm

File name: gpsphoto-4967.jpg

Location

Smartphone Privacy

Wallet

- Stored in folders:
- /HomeDomain/Library/Passes/Cards
- /HomeDomain/Library/Passes/BadUbiquitousPasses
- In .pkpass subfolders
- Look for pass.json files
- Some contain locations

```
{
  "description": "SOURCE to DESTINATION",
  "formatVersion": 1,
  "organizationName": "The Airlines",
  "relevantDate": "2013-02-20T20:40:00+01:00",
  "boardingPass": {
    "transitType": "PKTransitTypeAir"
  },
  "locations": [
    {
      "latitude": 12.11334800,
      "longitude": 13.56972200,
      "relevantText": "AirportName1"
    },
    {
      "latitude": 80.45861100,
      "longitude": 80.10611100,
      "relevantText": "AirportName2"
    }
  ]
}
```

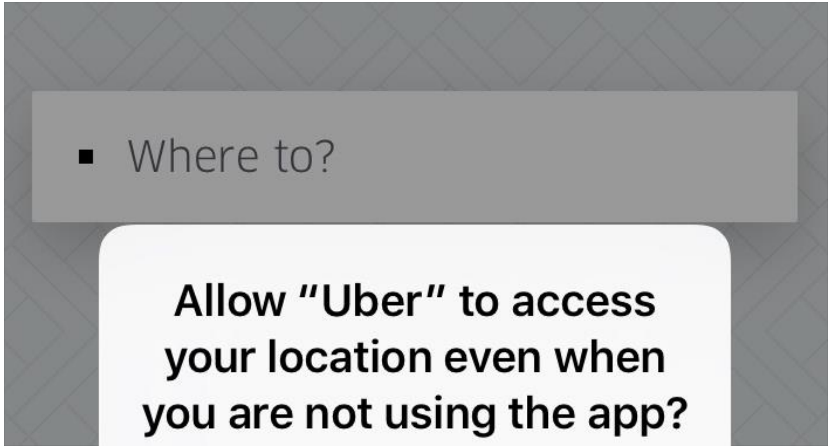
Smartphone Privacy

Third-Party Apps

- Multiple third-party apps and games collect location data
    - Even when you are not using the app
- This data may or may not be available in iTunes backups
- Apps may also cache thousands location points

  /private/var/mobile/Containers/Data/Application/<UUID>/Library/Caches/

  <UUID>: unique app identifier on this device



Where to?

Allow "Uber" to access your location even when you are not using the app?

```
{
    "jsonConformingObject":{
        "meta":{
            "location":{
                "course":-1,
                "city":"test",
                "speed":-1,
                "longitude":3.4,
                "gps_time_ms":1506351484216,
                "latitude":1.2,
                "horizontal_accuracy":65,
                "vertical_accuracy":10,
                "altitude":0.1
            }
        }
    }
}
```

Smartphone Privacy

Additional Location Data Exclusive to Physical Extraction

- Physical acquisition extracts full image of the file system
- Gains access to many files not in the backup
  - System logs, cache and temporary files
  - Protected app data
  - Apps with backups disabled
- Automatic sync with iCloud (if iCloud sync is enabled in the Settings)
  - Scheduled sync
  - On device reboot
  - On account change

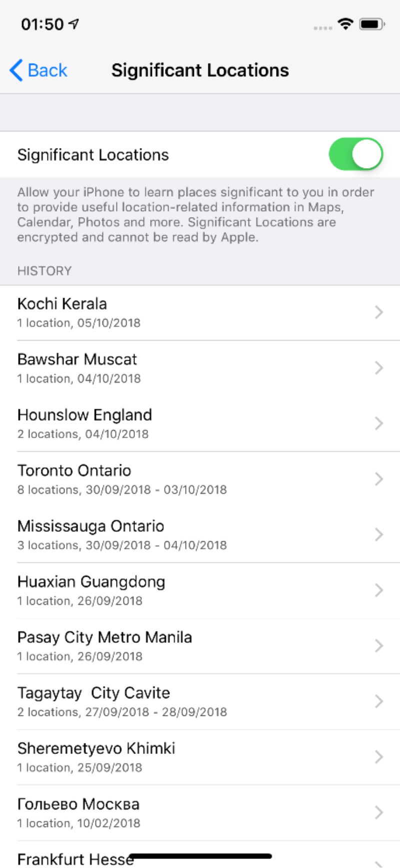
- Locations cache (3G/LTE, Wi-Fi)
- Frequent/Significant Locations
- Media file analysis cache
- Third-party cache
- Apple Pay locations

Smartphone Privacy

Location Cache (Physical Extraction Only)

- Databases:
  - /private/var/root/Library/Caches/locationd/cache_encryptedA.db
  - /private/var/root/Library/Caches/locationd/cache_encryptedB.db
  - /private/var/mobile/Library/Caches/com.apple.routined/cache_encryptedA.db
  - /private/var/mobile/Library/Caches/com.apple.routined/cache_encryptedB.db
- Tables:
  - Latitude, Longitude, Altitude, Timestamp, HorizontalAccuracy, VerticalAccuracy, Speed, Course, Confidence
  - MinimumLatitude, MinimumLongitude, MaximumLatitude, MaximumLongitude

Smartphone Privacy: significant locations



01:50

Back **Significant Locations**

Significant Locations ●

Allow your iPhone to learn places significant to you in order to provide useful location-related information in Maps, Calendar, Photos and more. Significant Locations are encrypted and cannot be read by Apple.

HISTORY

Kochi Kerala
1 location, 05/10/2018

Bawshar Muscat
1 location, 04/10/2018

Hounslow England
2 locations, 04/10/2018

Toronto Ontario
8 locations, 30/09/2018 - 03/10/2018

Mississauga Ontario
3 locations, 30/09/2018 - 04/10/2018

Huaxian Guangdong
1 location, 26/09/2018

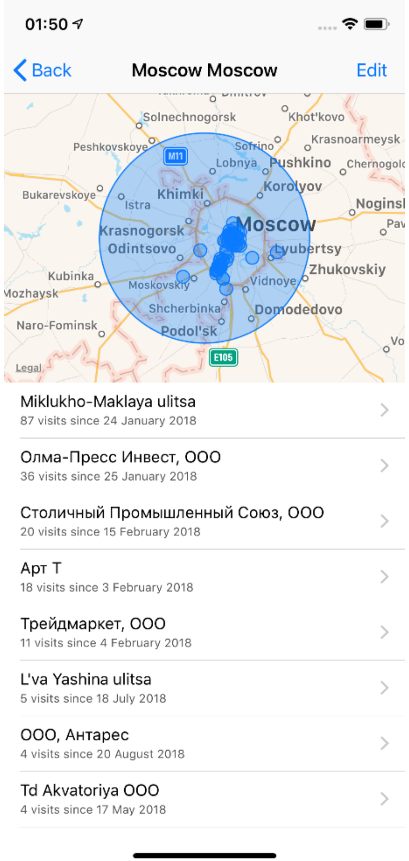
Pasay City Metro Manila
1 location, 26/09/2018

Tagaytay City Cavite
2 locations, 27/09/2018 - 28/09/2018

Sheremetyevo Khimki
1 location, 25/09/2018

Гольево Москва
1 location, 10/02/2018

Frankfurt Hesse



01:50

Back **Moscow Moscow** Edit

Miklukho-Maklaya ulitsa
87 visits since 24 January 2018

Олма-Пресс Инвест, ООО
36 visits since 25 January 2018

Столичный Промышленный Союз, ООО
20 visits since 15 February 2018

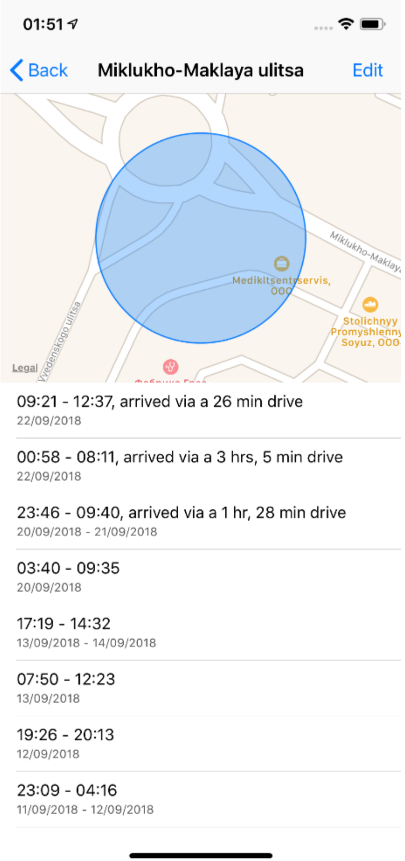
Арт Т
18 visits since 3 February 2018

Трейдмаркет, ООО
11 visits since 4 February 2018

L'va Yashina ulitsa
5 visits since 18 July 2018

ООО, Антарес
4 visits since 20 August 2018

Td Akvatoriya OOO
4 visits since 17 May 2018



01:51

Back **Miklukho-Maklaya ulitsa** Edit

09:21 - 12:37, arrived via a 26 min drive
22/09/2018

00:58 - 08:11, arrived via a 3 hrs, 5 min drive
22/09/2018

23:46 - 09:40, arrived via a 1 hr, 28 min drive
20/09/2018 - 21/09/2018

03:40 - 09:35
20/09/2018

17:19 - 14:32
13/09/2018 - 14/09/2018

07:50 - 12:23
13/09/2018

19:26 - 20:13
12/09/2018

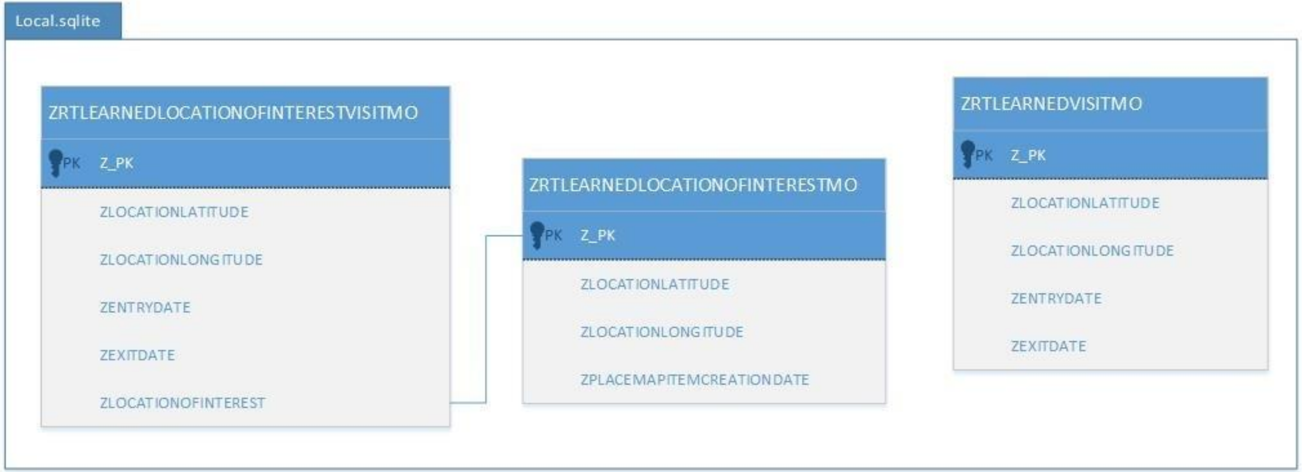
23:09 - 04:16
11/09/2018 - 12/09/2018

Smartphone Privacy

Significant Locations (Physical Extraction Only)

/private/var/mobile/Library/Caches/com.apple.routined/

- Local.sqlite: *data obtained on this device*
- Cloud.sqlite: *synced significant locations*
- Cache.sqlite: *temporary and unprocessed data*



Local.sqlite

ZRTLEARNEDLOCATIONOFINTERESTVISITMO

PK Z_PK

ZLOCATIONLATITUDE

ZLOCATIONLONGITUDE

ZENTRYDATE

ZEXITDATE

ZLOCATIONOFINTEREST

ZRTLEARNEDLOCATIONOFINTERESTMO

PK Z_PK

ZLOCATIONLATITUDE

ZLOCATIONLONGITUDE

ZPLACEMAPITEMCREATIONDATE

ZRTLEARNEDVISITMO

PK Z_PK

ZLOCATIONLATITUDE

ZLOCATIONLONGITUDE

ZENTRYDATE

ZEXITDATE

Smartphone Privacy

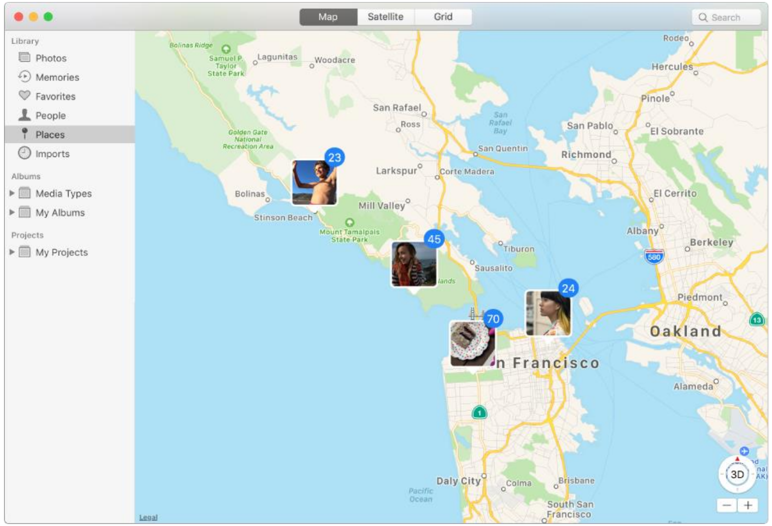
Synced Location Data (iCloud)

- System apps syncing location data via iCloud:
  - Apple Maps
  - Health
  - Calendar
  - Wallet
- Sensitive location data with direct sync:
  - Significant Locations: direct device-to-device sync only. Bypasses iCloud
- Wi-Fi connections
  - Reverse BSSID lookup reveals locations
  - Depending on the source, may not connect timestamps (first connect and last disconnect only)
  - Logs contain timestamps

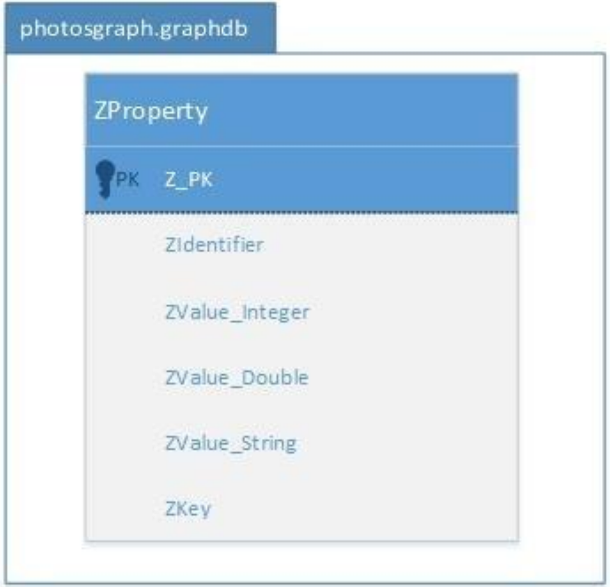
Smartphone Privacy

Locations Cached When Analyzing Media Files

- **photoanalysisd** process analyses media files; assigns tags, discovers faces, extracts EXIF etc
- **photosgraph** maps extracted EXIF locations



/private/var/mobile/Media/PhotoData/Caches/GraphService/PhotosGraph/photosgraph.graphdb



photosgraph.graphdb

ZProperty

PK Z_PK

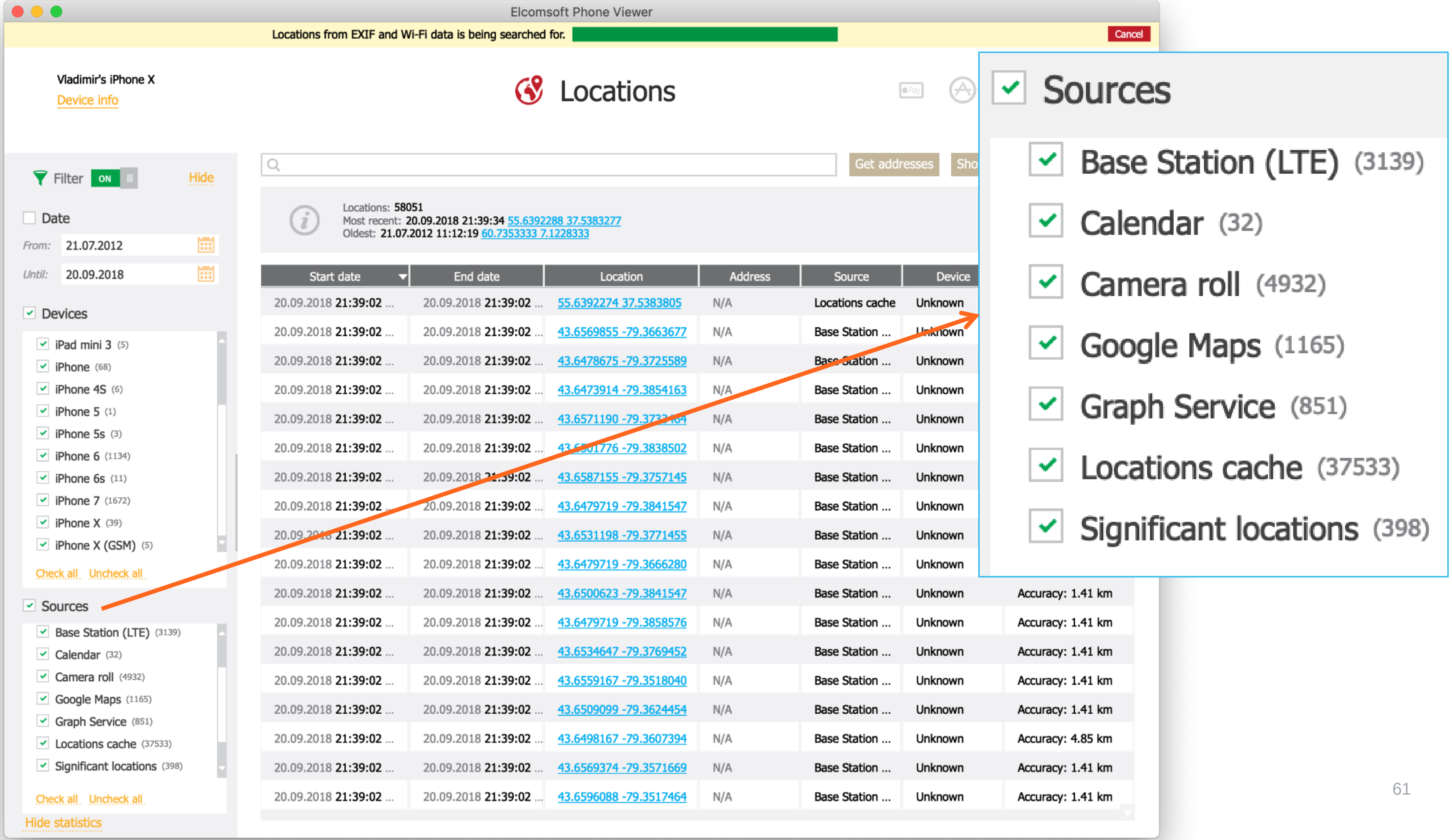
ZIdentifier

ZValue_Integer

ZValue_Double

ZValue_String

ZKey



Locations from EXIF and Wi-Fi data is being searched for.

Vladimir's iPhone X
Device info

Locations

Filter ON
Hide

□ Date
From: 21.07.2012
Until: 20.09.2018

☑ Devices
- ☑ iPad mini 3 (5)
- ☑ iPhone (68)
- ☑ iPhone 4S (6)
- ☑ iPhone 5 (1)
- ☑ iPhone 5s (3)
- ☑ iPhone 6 (1134)
- ☑ iPhone 6s (11)
- ☑ iPhone 7 (1672)
- ☑ iPhone X (39)
- ☑ iPhone X (GSM) (5)

Check all Uncheck all

☑ Sources
- ☑ Base Station (LTE) (3139)
- ☑ Calendar (32)
- ☑ Camera roll (4932)
- ☑ Google Maps (1165)
- ☑ Graph Service (851)
- ☑ Locations cache (37533)
- ☑ Significant locations (398)

Check all Uncheck all

Hide statistics

Locations: 58051
Most recent: 20.09.2018 21:39:34 55.6392288 37.5383277
Oldest: 21.07.2012 11:12:19 60.7353333 7.1228333

Start date	End date	Location	Address	Source	Device	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	55.6392274 37.5383805	N/A	Locations cache	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6569855 -79.3663677	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6478675 -79.3725589	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6473914 -79.3854163	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6571190 -79.3732464	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6501776 -79.3838502	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6587155 -79.3757145	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6479719 -79.3841547	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6531198 -79.3771455	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6479719 -79.3666280	N/A	Base Station ...	Unknown	
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6500623 -79.3841547	N/A	Base Station ...	Unknown	Accuracy: 1.41 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6479719 -79.3858576	N/A	Base Station ...	Unknown	Accuracy: 1.41 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6534647 -79.3769452	N/A	Base Station ...	Unknown	Accuracy: 1.41 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6559167 -79.3518040	N/A	Base Station ...	Unknown	Accuracy: 1.41 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6509099 -79.3624454	N/A	Base Station ...	Unknown	Accuracy: 1.41 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6498167 -79.3607394	N/A	Base Station ...	Unknown	Accuracy: 4.85 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6569374 -79.3571669	N/A	Base Station ...	Unknown	Accuracy: 1.41 km
20.09.2018 21:39:02 ...	20.09.2018 21:39:02 ...	43.6596088 -79.3517464	N/A	Base Station ...	Unknown	Accuracy: 1.41 km

☑ Sources
- ☑ Base Station (LTE) (3139)
- ☑ Calendar (32)
- ☑ Camera roll (4932)
- ☑ Google Maps (1165)
- ☑ Graph Service (851)
- ☑ Locations cache (37533)
- ☑ Significant locations (398)

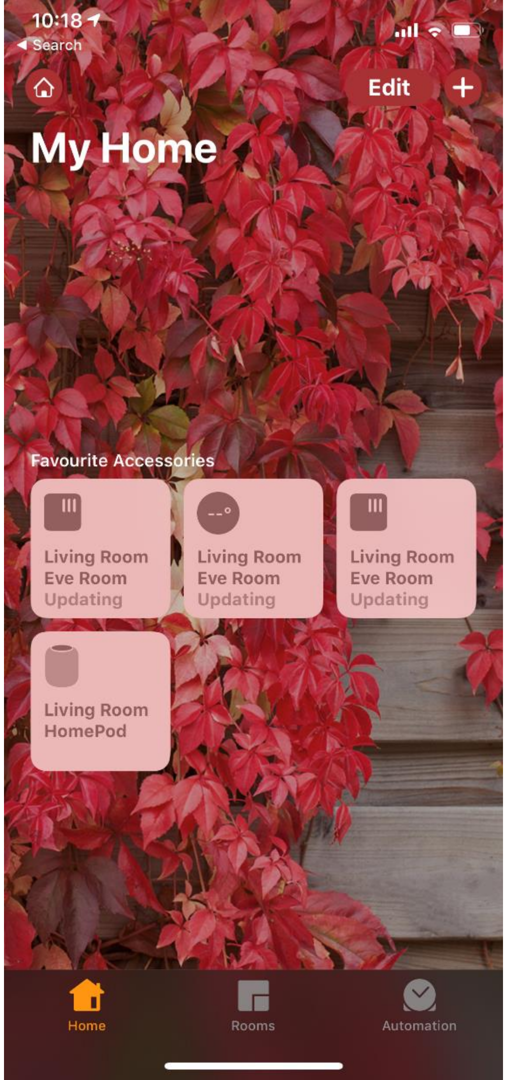
The Future Is…

iCloud: what’s next?

More synced data in iCloud

- Home data (HomePod, various sensors, lights, thermostats etc)
- Screen Time (app usage; previously available via full file system acquisition only)
- Voice memos
- Weather & Stocks

Remember Celebgate? ;)



10:18

◀ Search

Edit +

My Home

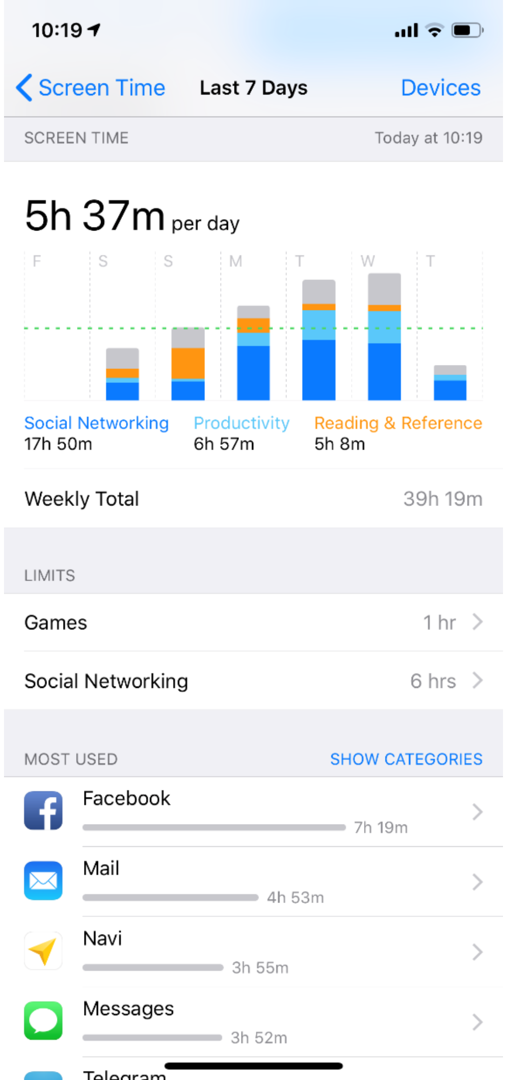
Favourite Accessories

Living Room
Eve Room
Updating

Living Room
Eve Room
Updating

Living Room
Eve Room
Updating

Living Room
HomePod



10:19

< Screen Time | Last 7 Days | Devices

SCREEN TIME — Today at 10:19

5h 37m per day

Social Networking	Productivity	Reading & Reference
17h 50m	6h 57m	5h 8m

Weekly Total 39h 19m

LIMITS

Games	1 hr >
Social Networking	6 hrs >

MOST USED — SHOW CATEGORIES

Facebook	7h 19m
Mail	4h 53m
Navi	3h 55m
Messages	3h 52m
Telegram	

Smartphone Privacy

Google Android

- Android collects significantly more data than iOS
- Google collects significantly more information than Apple
- These statements are not equivalent
  - Android ecosystem is seemingly built for tracking
  - Every other app in Google Play store tracks your location
  - Even with Location disabled
  - Even without Location permission
- All Android apps have Internet access
  - No special permission is needed
  - IP address determines approximate location
  - Allows scanning nearby Wi-Fi networks

Smartphone Privacy

Google Android

- All Android apps can access BSSID of currently connected Wi-Fi, and
- All Android apps can scan nearby Wi-Fi access points
  - Single BSSID reverse lookup determines current location within 20m radius
  - Triangulating multiple BSSID’s reveals precise location
  - Multiple free and commercial Wi-Fi Geo-Location databases exist
  - openwlanmap.org

Smartphone Privacy

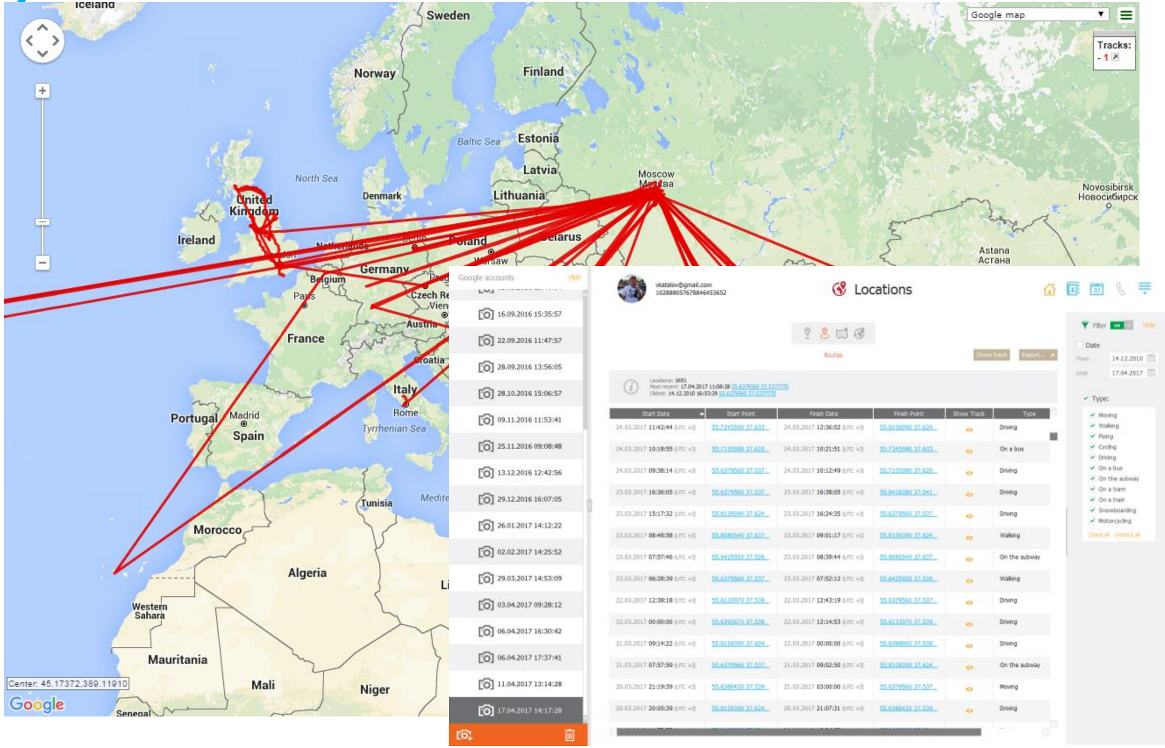
Google: Sources of Location Data

- Location History: Takeout, cloud extraction, online interface
  - Extremely comprehensive
  - **Stored in the cloud (Google Account)**
  - Cloud contains more information than device
- Google Maps and My Places
- Photos: local (extract from device), Takeout (Google Photos)
- System logs: local (root required)
- App data: local (root required), cloud backups (limited)

Smartphone Privacy

Google Location History

- Multiple data points
- Many years worth of data (you will be surprised)
- Collected from all devices on the same Google Account
- Android, iOS, Windows, Mac
- Google services in all Web browsers (if signed in)
- Location + date & time)



16.09.2016 15:35:57
22.09.2016 11:47:57
28.09.2016 13:56:05
28.10.2016 15:06:57
09.11.2016 11:53:41
25.11.2016 09:08:48
13.12.2016 12:42:56
29.12.2016 16:07:05
26.01.2017 14:12:22
02.02.2017 14:25:52
29.03.2017 14:53:09
03.04.2017 09:28:12
06.04.2017 16:30:42
06.04.2017 17:37:41
11.04.2017 13:14:28
17.04.2017 14:17:28

vkatalov@gmail.com
102888057678846453652

Locations

Routes

Show track   Export...

Locations: 1651
Most recent: 17.04.2017 11:08:28 55.6379560 37.5377770
Oldest: 14.12.2010 16:53:29 55.6379560 37.5377770

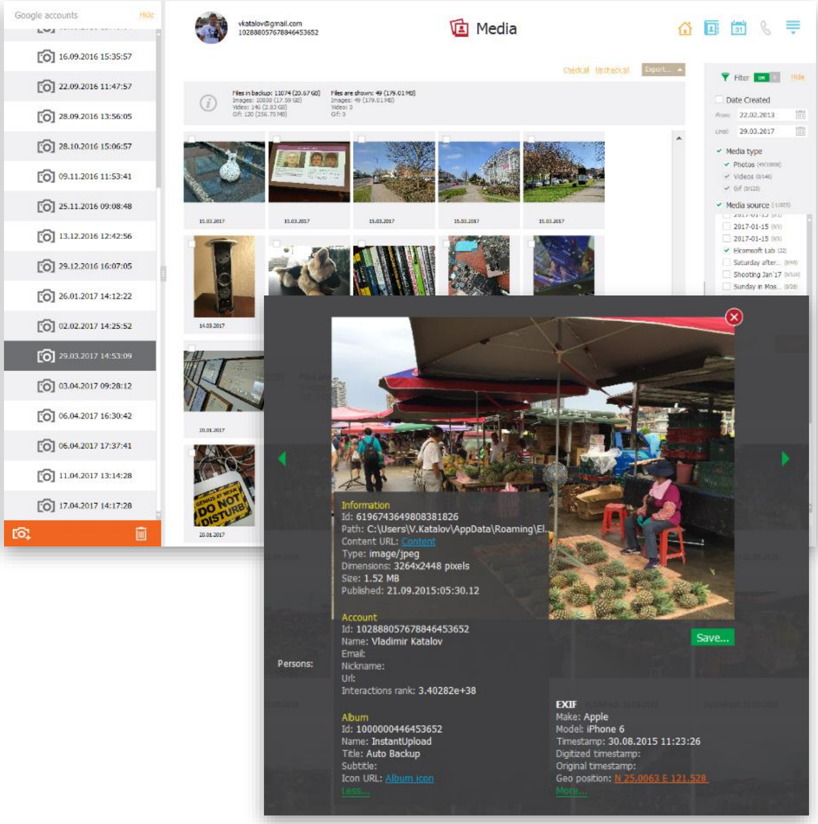
Start Date	Start Point	Finish Date	Finish Point	Show Track	Type
24.03.2017 11:42:44 (UTC +3)	55.7245590 37.633...	24.03.2017 12:36:02 (UTC +3)	55.8109390 37.624...	👁	Driving
24.03.2017 10:18:55 (UTC +3)	55.7105080 37.620...	24.03.2017 10:21:51 (UTC +3)	55.7245590 37.633...	👁	On a bus
24.03.2017 09:38:14 (UTC +3)	55.6379560 37.537...	24.03.2017 10:12:49 (UTC +3)	55.7105080 37.620...	👁	Driving
23.03.2017 16:36:05 (UTC +3)	55.6379560 37.537...	23.03.2017 16:38:05 (UTC +3)	55.6416280 37.541...	👁	Driving
23.03.2017 15:17:32 (UTC +3)	55.8109390 37.624...	23.03.2017 16:24:35 (UTC +3)	55.6379560 37.537...	👁	Driving
23.03.2017 08:48:58 (UTC +3)	55.8080540 37.637...	23.03.2017 09:01:17 (UTC +3)	55.8109390 37.624...	👁	Walking
23.03.2017 07:57:46 (UTC +3)	55.6425920 37.526...	23.03.2017 08:39:44 (UTC +3)	55.8080540 37.637...	👁	On the subway
23.03.2017 06:28:39 (UTC +3)	55.6379560 37.537...	23.03.2017 07:52:12 (UTC +3)	55.6425920 37.526...	👁	Walking
22.03.2017 12:38:18 (UTC +3)	55.6133970 37.539...	22.03.2017 12:43:19 (UTC +3)	55.6379560 37.537...	👁	Driving
22.03.2017 00:00:00 (UTC +3)	55.6392670 37.538...	22.03.2017 12:14:53 (UTC +3)	55.6133970 37.539...	👁	Driving
21.03.2017 09:14:22 (UTC +3)	55.8109390 37.624...	22.03.2017 00:00:00 (UTC +3)	55.6388900 37.538...	👁	Driving
21.03.2017 07:57:59 (UTC +3)	55.6379560 37.537...	21.03.2017 09:02:50 (UTC +3)	55.8109390 37.624...	👁	On the subway
20.03.2017 21:19:39 (UTC +3)	55.6386430 37.539...	21.03.2017 03:00:00 (UTC +3)	55.6379560 37.537...	👁	Moving
20.03.2017 20:05:39 (UTC +3)	55.8109390 37.624...	20.03.2017 21:07:31 (UTC +3)	55.6386430 37.539...	👁	Driving

Filter ON Hide
□ Date
From 14.12.2010
Until 17.04.2017
✓ Type:
✓ Moving
✓ Walking
✓ Flying
✓ Cycling
✓ Driving
✓ On a bus
✓ On the subway
✓ On a tram
✓ On a train
✓ Snowboarding
✓ Motorcycling
Check all Uncheck all

Smartphone Privacy

Media

- Photos from all user’s devices can be uploaded to Google Photos
- Google Photos **not the same as** Google Drive!
- Location data via EXIF



vkatalov@gmail.com
102888057678846453652

Files in backup: 11074 (20.67 GB)
Images: 10808 (17.59 GB)
Video: 146 (2.83 GB)
Gif: 120 (256.75 MB)

Files are shown: 49 (179.01 MB)
Images: 49 (179.01 MB)
Video: 0
Gif: 0

From: 22.02.2013
Until: 29.03.2017

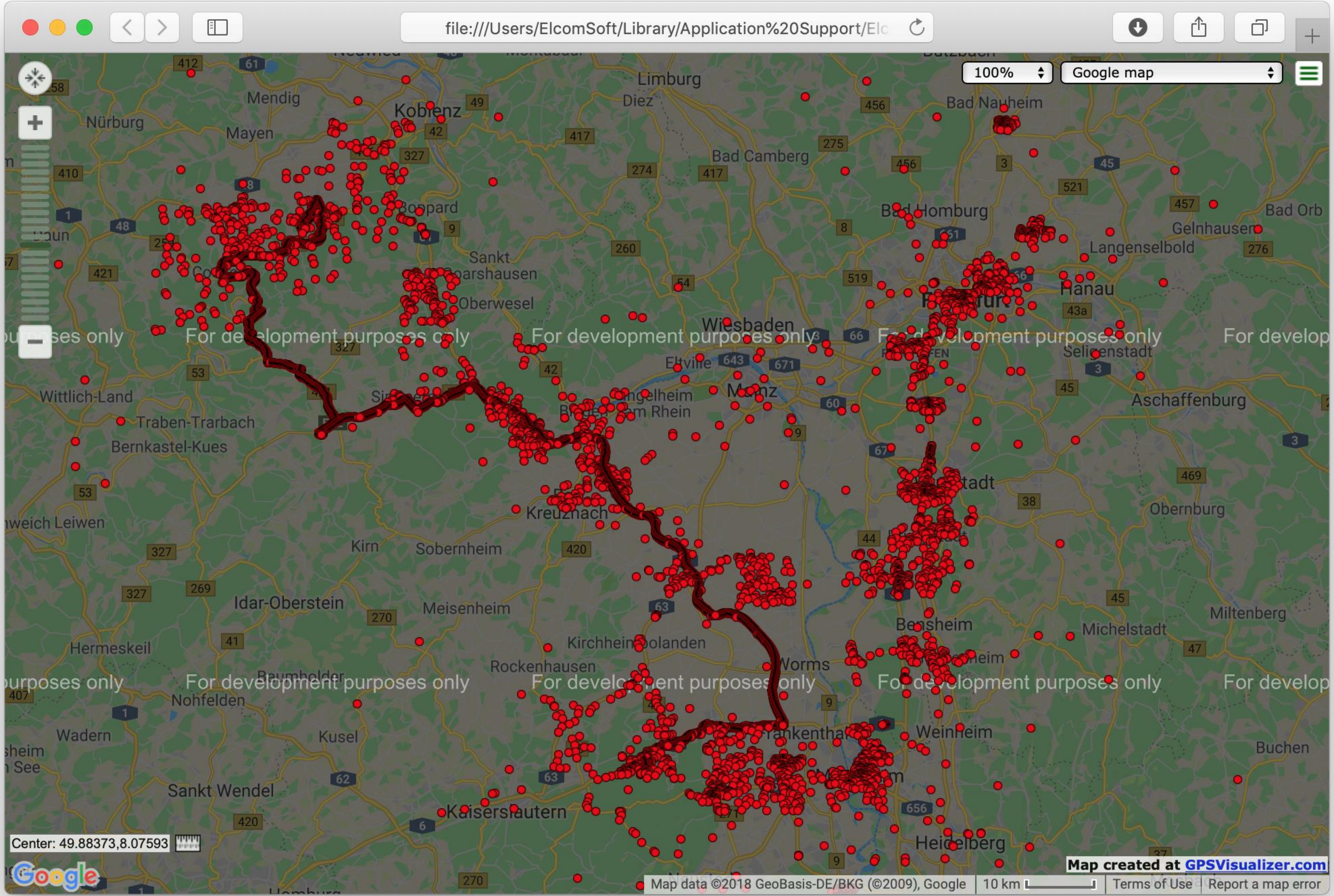
☐ 2017-01-15
☐ 2017-01-15
☑ Elcomsoft Lab (22)

Information
Id: 6196743649808381826
Path: C:\Users\V.Katalov\AppData\Roaming\El...
Content URL: Content
Type: image/jpeg
Dimensions: 3264x2448 pixels
Size: 1.52 MB
Published: 21.09.2015:05:30.12

Account
Id: 102888057678846453652
Name: Vladimir Katalov
Email:
Nickname:
Url:
Interactions rank: 3.40282e+38

Album
Id: 1000000446453652
Name: InstantUpload
Title: Auto Backup
Subtitle:
Icon URL: Album icon

EXIF
Make: Apple
Model: iPhone 6
Timestamp: 30.08.2015 11:23:26
Digitized timestamp:
Original timestamp:
Geo position: N 25.0063 E 121.528



file:///Users/ElcomSoft/Library/Application%20Support/Elc

100%

Google map

Center: 49.88373,8.07593

Map created at GPSVisualizer.com

Map data ©2018 GeoBasis-DE/BKG (©2009), Google

10 km

Terms of Use

Report a map error

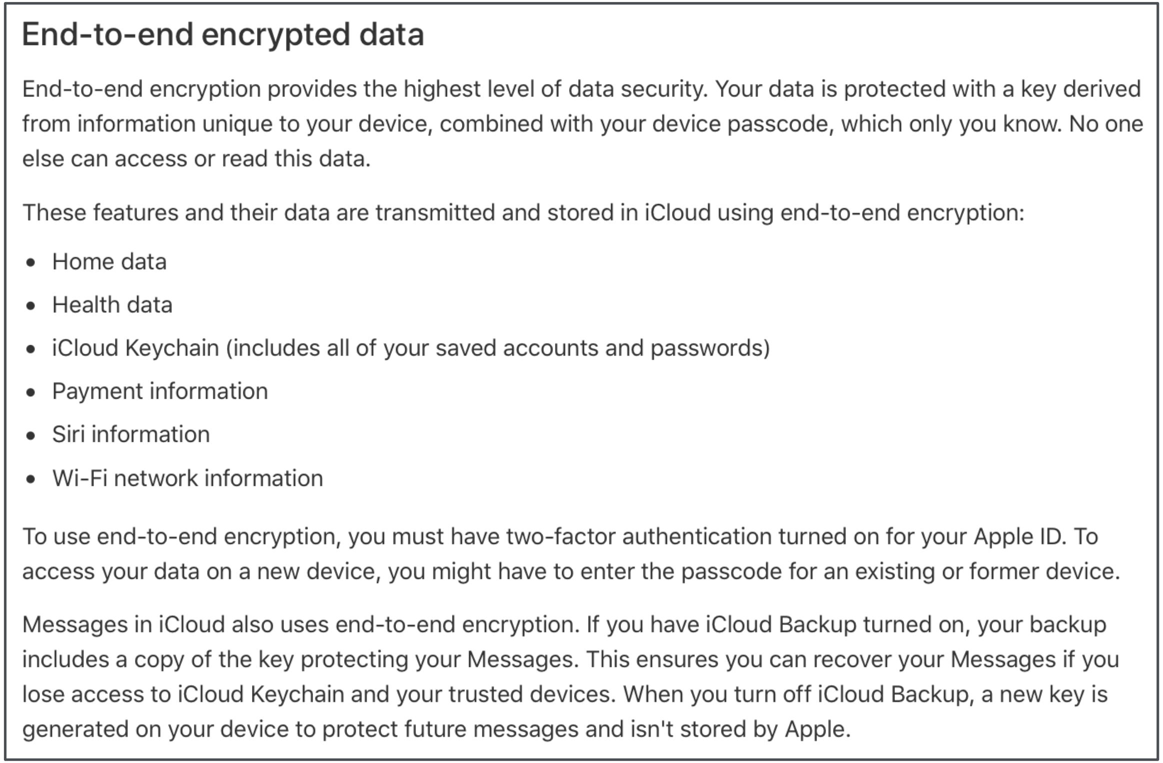
Smartphone Privacy

Where to get the data from?

- Device (local backup)
- Device (cloud backup) // credentials required!
- Device (physical acquisition) // requires jailbreaking/rooting
- Cloud (synced data) // credentials required!
- Cloud (location services like Apple Find My Phone, Apple Find Friends. Google Find My Device) // credentials required!
- Third-party [cloud] services // credentials required!

Smartphone Privacy

iCloud security overview (HT202303)



End-to-end encrypted data

End-to-end encryption provides the highest level of data security. Your data is protected with a key derived from information unique to your device, combined with your device passcode, which only you know. No one else can access or read this data.

These features and their data are transmitted and stored in iCloud using end-to-end encryption:

- Home data
- Health data
- iCloud Keychain (includes all of your saved accounts and passwords)
- Payment information
- Siri information
- Wi-Fi network information

To use end-to-end encryption, you must have two-factor authentication turned on for your Apple ID. To access your data on a new device, you might have to enter the passcode for an existing or former device.

Messages in iCloud also uses end-to-end encryption. If you have iCloud Backup turned on, your backup includes a copy of the key protecting your Messages. This ensures you can recover your Messages if you lose access to iCloud Keychain and your trusted devices. When you turn off iCloud Backup, a new key is generated on your device to protect future messages and isn't stored by Apple.

Reality

- *Home data: have not checked yet, but seems that not*
- *Health: not always (only if all devices on the account use macOS 11.4 / iOS 12*
- *iCloud Keychain: yes*
- *Payment information: yes*
- *Siri information: yes*
- *Wi-Fi network information: password only*

Still, most of that data can be downloaded and decrypted with proper tokens

Obtaining the Credentials

How to get cloud password or token?

- Legally (court order)
- Social engineering
- From computer (cached browser passwords)
- From computer (saved token from system or apps)
- Extract macOS keychain
- From other account that was easier to break (Apple / Google / Microsoft)
- Extract from local iTunes backup (with password)
- From password manager (need to crack master password first)
- Password re-use often helps
- From the sticker on monitor or note under the keyboard
- Rubberhose cryptanalysis

Smartphone Privacy

Vladimir Katalov, ElcomSoft

Questions?