December 2019

Breaking Health Clouds

Fitbit and other health trackers: obtaining vital evidence for your investigation

Vladimir Katalov, ElcomSoft

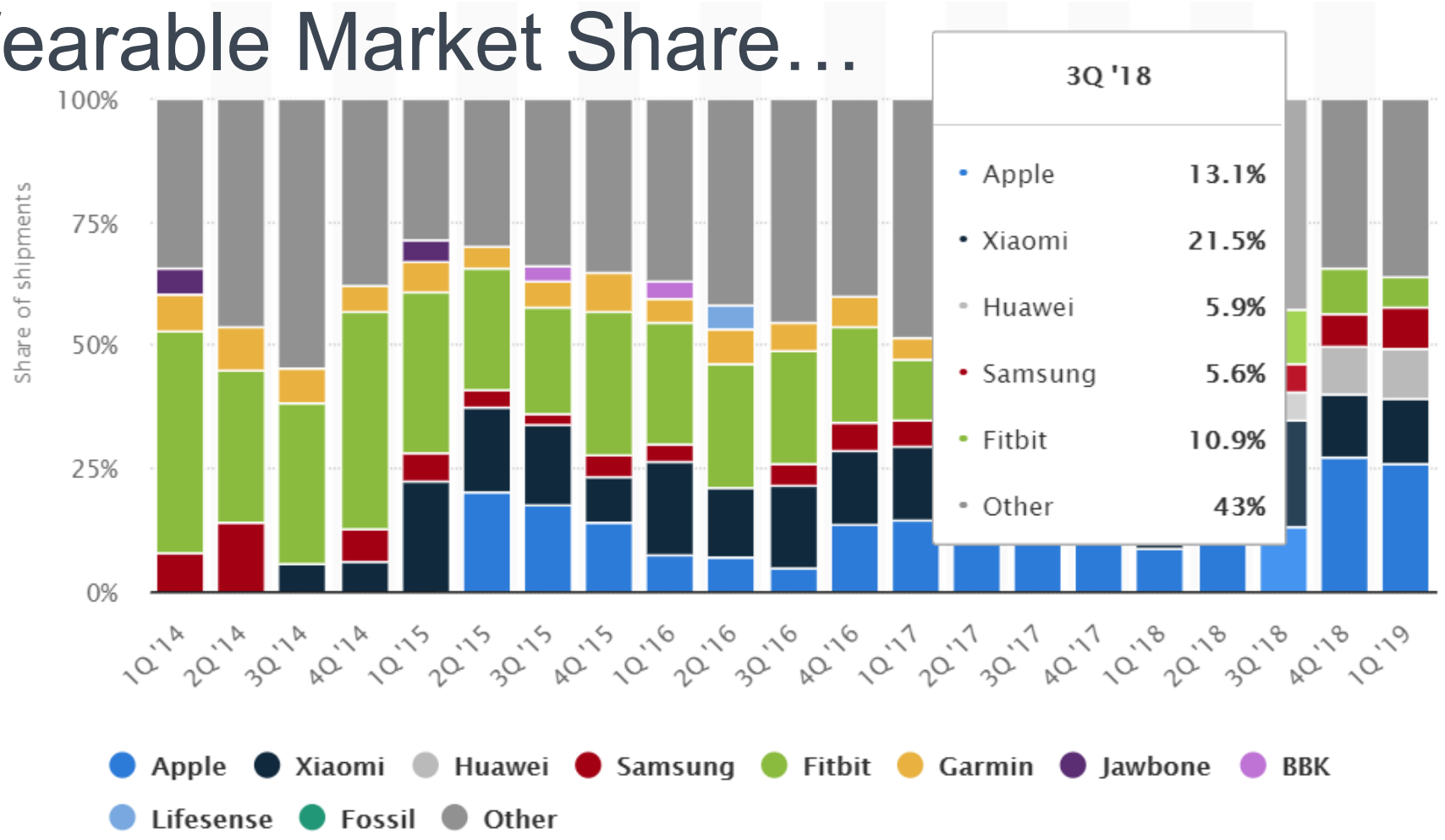

ELCOMSOFT
Fitbit
and Other Health Trackers
Obtaining vital evidence
for your investigation
Vladimir Katalov, ElcomSoft

Introduction to Mobile Forensics

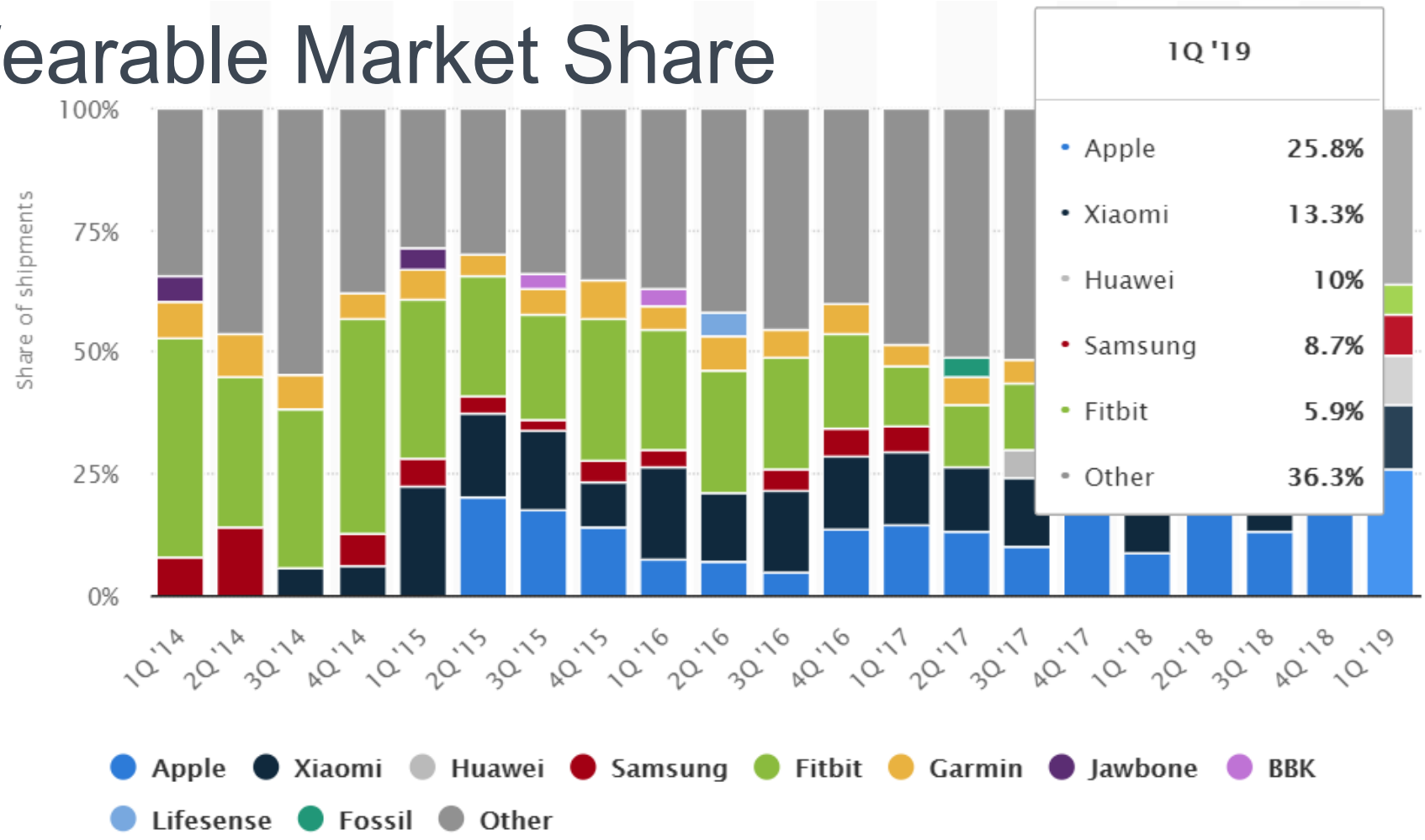
How to access the evidence?

- **Off the phone extraction**
  - Logical acquisition: backups, photos, shared files, some logs
  - Physical (file system) imaging: everything sans deleted files, might be complex or unavailable
- **Cloud (over-the-air) acquisition**
  - No device required
  - Remote access to a lot of data
  - Sometimes, extracts more data than stored on a single device

Wearable Market Share…



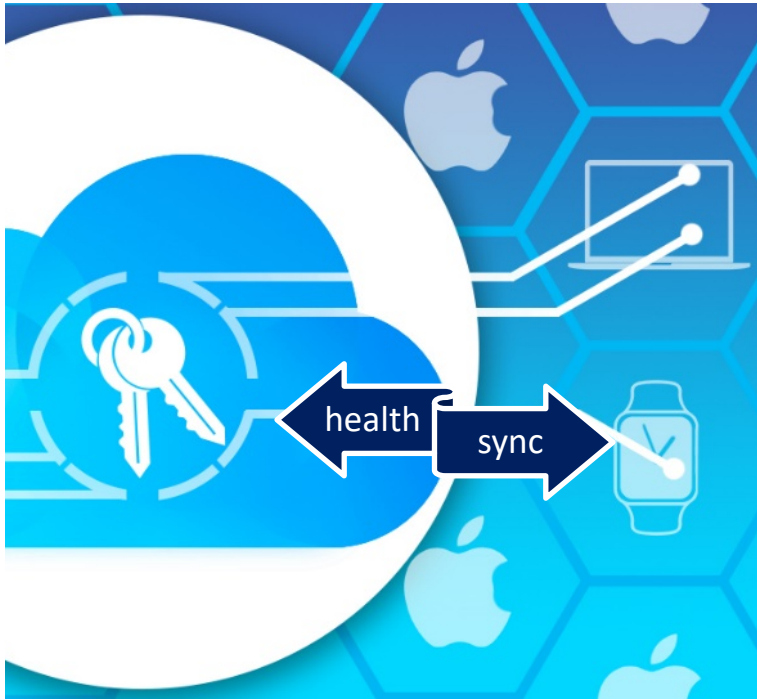
Wearable Market Share



Health Evidence

Health evidence is stored in the cloud

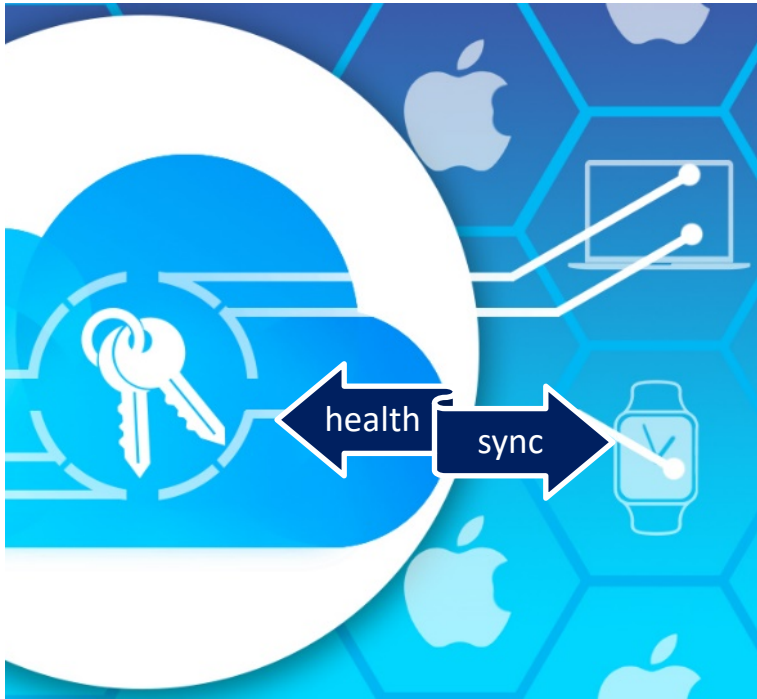
- **Apple and Google cloud platforms**
- Single point access to all health data is very tempting
- Some manufacturers sync Health data, and some don’t
- Apple requires sharing data with Apple Health to approve manufacturer’s HealthKit integration
  - Some manufacturers ignore HealthKit altogether
- Google does not have any requirements
  - Most manufacturers ignore Google Fit



Health Evidence

Apple Watch, Google WearOS (ex- Android Wear)

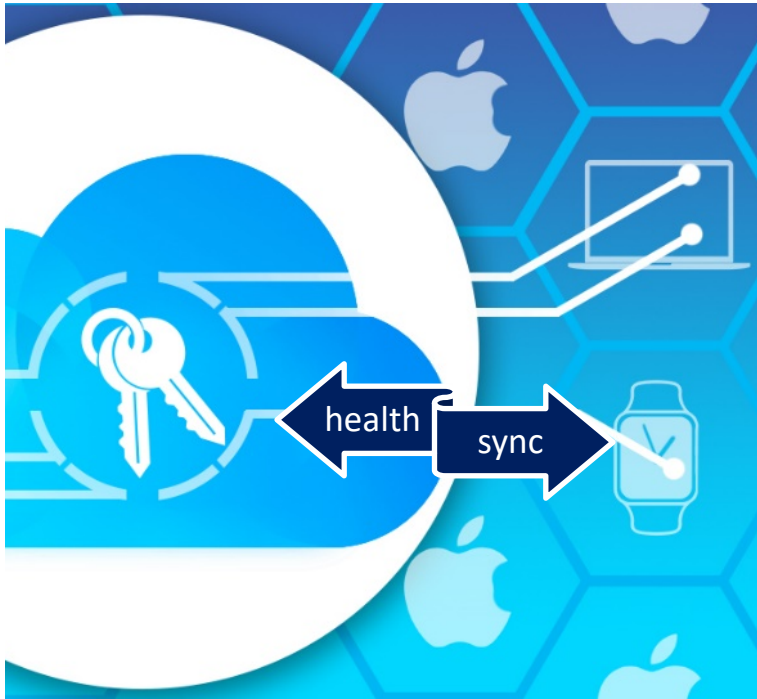
- **Apple Watch:** iCloud only
  - Exclusively works through Apple HealthKit
  - **No** integration with Google or Android
- **Google WearOS watches** (all models)
  - Works on iOS devices, but…
  - **No** integration with Apple HealthKit (Google's decision)
  - Full integration with Google Fit



Health Evidence

Fitness trackers with proprietary cloud services

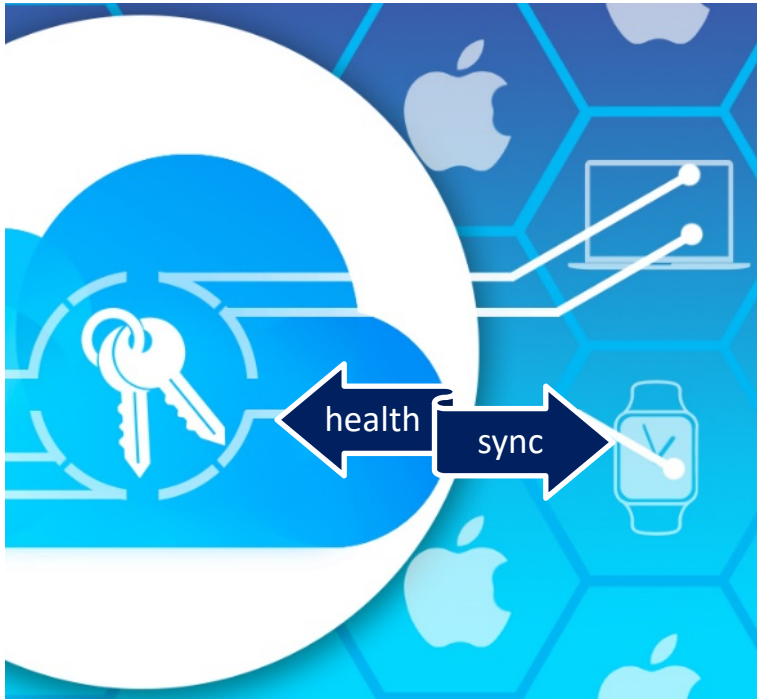
- **Samsung Health: proprietary Samsung Cloud**
  - Ignores Apple HealthKit and Google Fit
- **Xiaomi, Amazfit**: Mi Cloud, proprietary cloud
  - Integration with Apple HealthKit
  - Google Fit: limited (steps only) integration



Health Evidence

Fitness trackers with proprietary cloud services

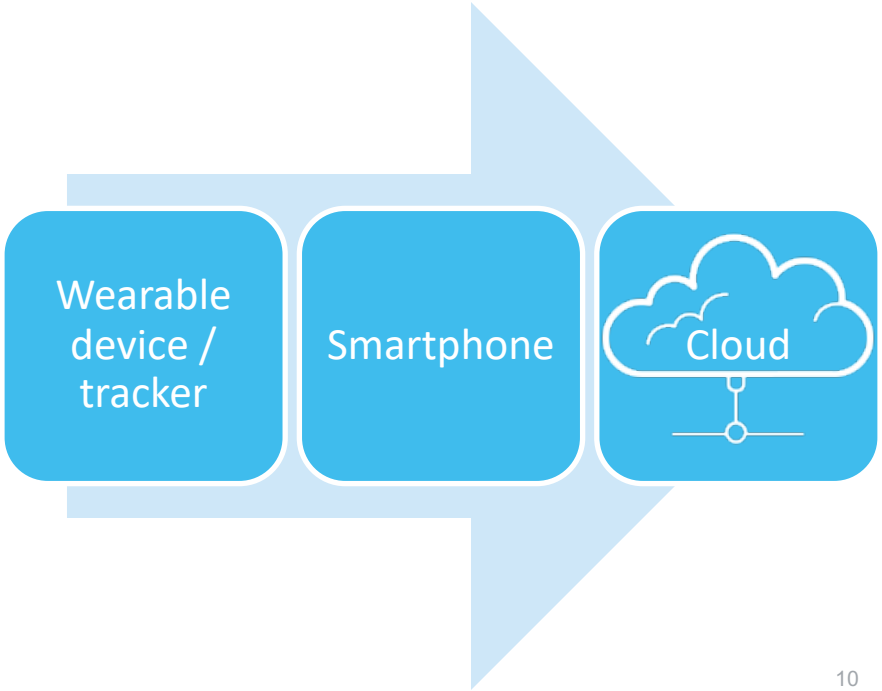
- **Garmin**: Garmin Connect, proprietary cloud
  - One-way sync > to Apple HealthKit
  - Google Fit: no integration
- **Fitbit: proprietary cloud only**
  - Ignores Apple HealthKit and Google Fit



Wearables Data Flow

Wearable device > Phone > Cloud

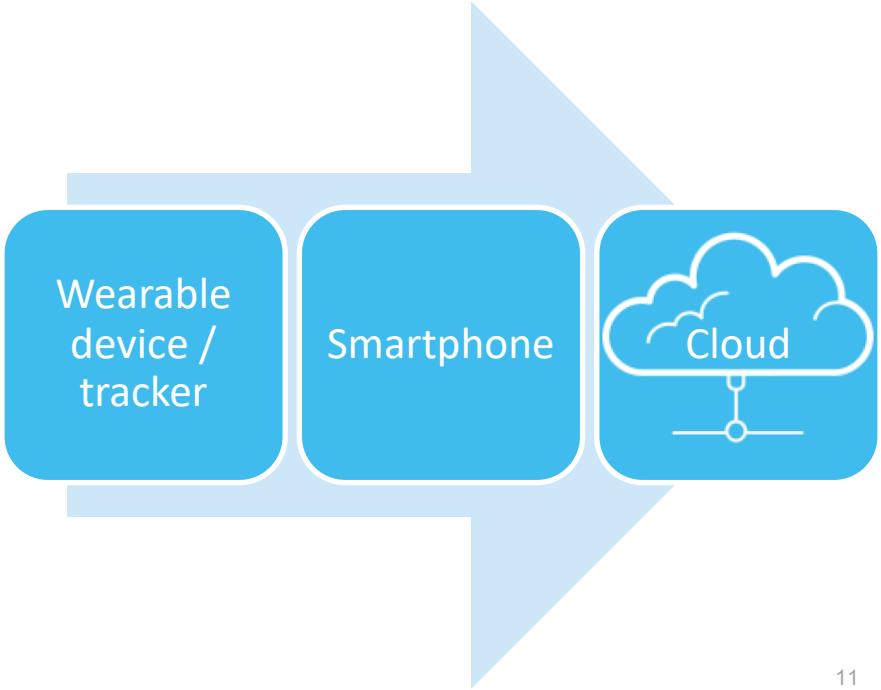
- The wearable device collects information (steps, heart rate, GPS, activity, screen time etc.)
- The data is synchronized with an app on the phone via a low-energy connection (e.g. Bluetooth LE, Wi-Fi and LTE sync available on some models)
- The app (Apple Health, Google Fit, Samsung Health, Mi Fit etc.) processes the data and (optionally) syncs with Apple Health Kit (or Google Fit on Android)
- And then…



Wearables Data Flow

Wearable device > Phone > Cloud

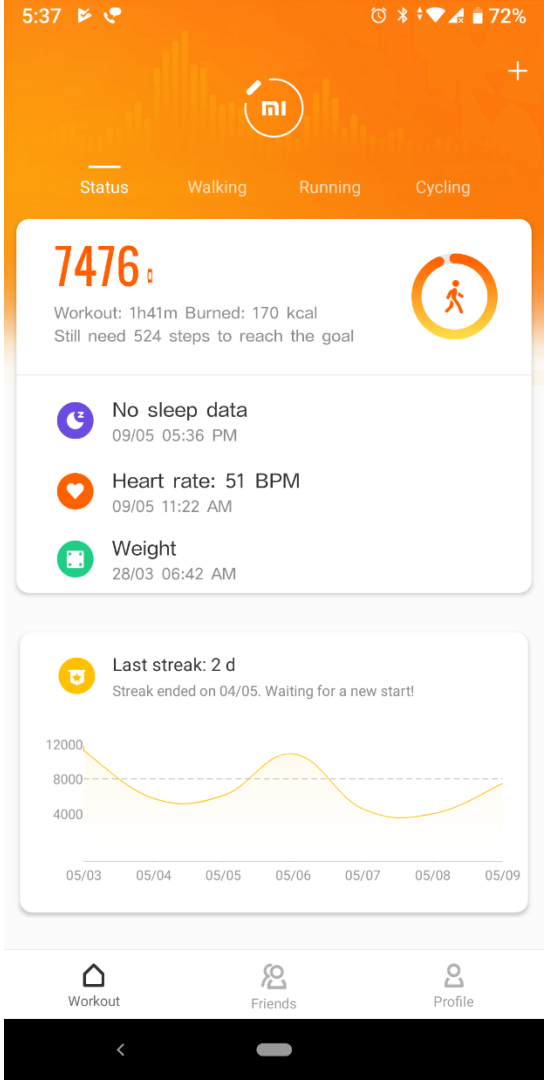
- The data ends up in the cloud
- If the data is synced with Apple HealthKit, the Health app aggregates the data and syncs with iCloud
- If the data is synced with Google Fit, then Google takes care of the sync
- More often than not, manufacturers employ their very own, proprietary cloud service
- **Such as Fitbit**



Data collected by vendors

Mi Fit

Data	Description
User profile	Information provided by the user such as age, height and weight
Device list	List of devices registered for Mi Fit
Running history	Detailed information about running workouts
Band data	Service information from the tracker device
Hearth rate	Raw hearth rate data
Event reminders	Events and reminders
Manual data	Any information the user added manually
Health settings	Settings of the Health app
ETE and THA events	ETE and THA rhythm events
Weight records	Timestamped weighing data



Data collected by vendors

Samsung Health

- As one can expect, Samsung collects lots of finely detailed information
- More than 100 distinct data categories
- As an example, ALP, albumin, amylase, blood pressure, blood glucose, caffeine intake, creatinine, CPK and bilirubin data fields are available for the blood
- Unsurprisingly, Samsung does not sync with Apple HealthKit or Google Fit, which define a much smaller (and less detailed) subset of health data

Data collected by vendors

Fitbit

- Fitbit collects, stores and processes data to estimate a variety of metrics
- The data is stored in Fitbit cloud
  - Step count and distance traveled
  - Calories burned
  - Weight
  - Heart rate
  - Sleep stages and active minutes
  - Location

Data collected by vendors

Where Fitbit stores data

- Fitbit stores data in the proprietary cloud service
- Fitbit offers a Web API to access data: https://dev.fitbit.com/build/reference/web-api/
- Web API gives access to all of the following:
  - Activity
  - Body & weight
  - Devices and alarms
  - Food logging
  - Friends
  - Heart rate
  - Sleep
  - User profile

Data collected by vendors

Data in Fitbit cloud

- **Activity**
  - **Daily activity summary** including:
  - **Daily goals for elevation (elevation, floors), steps, calories burned, and distance**
  - **Activity time series:** time series data in the specified range
  - **Activity logging:** the same data in user's local language
  - **Activity types:** a tree of all valid Fitbit public activities as well as private custom activities the user created
  - **Activity goals:** a user's current daily or weekly activity goals
  - **Lifetime stats:** the user's activity statistics

Data collected by vendors

Data in Fitbit cloud

- **Body & Weight**
  - **Body fat:** the list of all user's **body fat log entries** for a given day
  - **Body time series:** time series data in the specified range
  - **Goals:** a user's current body fat percentage or weight goal
  - **Weight:** a list of all user's body weight log entries for a given day

Data collected by vendors

Data in Fitbit cloud

- **Devices and alarms**
  - Data provided through the Fitbit API does not necessarily represent a single tracker
  - Data can change frequently, as trackers sync at different intervals and the unified data is recalculated at each sync
  - Distance and number of steps are correlated when GPS data is available

Data collected by vendors

Data in Fitbit cloud

- **Food logging**
  - Public and private food logs
  - Nutrition information
  - Hydration logs
  - Including goals and time series

Data collected by vendors

Data in Fitbit cloud

- **Friends**
  - List of user's friends
  - Links to friends profiles
  - Friends data (e.g. number of steps)
  - Invitations
  - Invitation responses

Data collected by vendors

Data in Fitbit cloud

- **Sleep logs**
  - Detailed information on the user's sleeping sessions
  - Sleep and awake minutes, time in bed, minutes to fall asleep
  - **Summaries**: minutes after wakeup, minutes asleep, minutes awake, minutes to fall asleep, start time, time in bed, sleep phase
  - Sleep phase ("level"): wake, rem, awake, restless, asleep etc.

Data collected by vendors

Data in Fitbit cloud

- **User profile**
  - Detailed information on authenticated user
  - Basic information about user's friends
  - No access to other users profiles

Fitbit Acquisition

Will Google acquisition of Fitbit affect the cloud?

- Most definitely, it will
- Fitbit acquisition gives Google access to a trove of data from sleep tracking to heart rates
- “Fitbit and Google Announce Collaboration to Accelerate Innovation in Digital Health and Wearables”
- “Fitbit to leverage Google Cloud to increase operational efficiency, agility and speed to mark
- “Fitbit intends to use Google’s new Cloud Healt API to help the company integrate further into t healthcare system”
- Source: Fitbit press release

Fitbit Acquisition

Does Fitbit acquisition affect users and/or forensics?

- No, at least not immediately
- The changes, if any, will occur slowly
- Most probably to new products only
- Most probably not before Q3’ 2020 anyway because of development pipeline
- Existing products will be likely grandfathered, keep using existing Fitbit services

Apple HealthKit

What is Apple HealthKit?

- Introduced in Sep 2014 with iOS 8
- Health app pre-installed on all iPhones
- Always active, always collecting information
- Supported by Apple Watch, additional data collected
- Integrates data supplied by third-party fitness trackers
- **Fitbit does not support HealthKit**

Apple HealthKit

Who integrates with Apple HealthKit

- Apple Watch (all models)
- Many third-party fitness trackers
  - Xiaomi, Amazfit
  - Garmin
  - Withings
  - Huawei (own OS only)

Apple HealthKit

Who integrates with Apple HealthKit

- Dozens of health and tracking apps
  - **Workouts++**
  - **Strava**
  - **Endomondo**
- They have proprietary cloud services, too
- From time to time,
  these cloud services leak data

Apple HealthKit

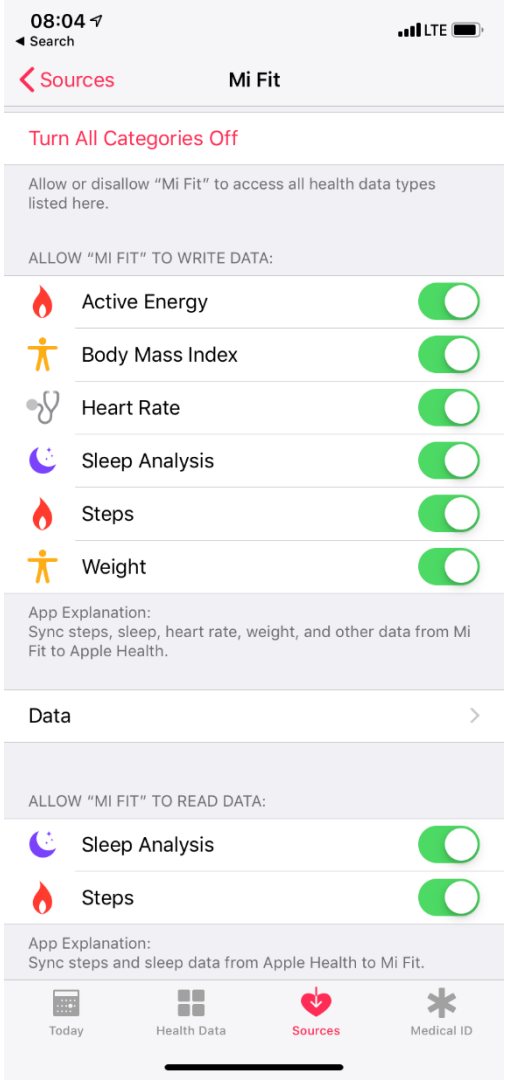
Who does not integrate with Apple HealthKit

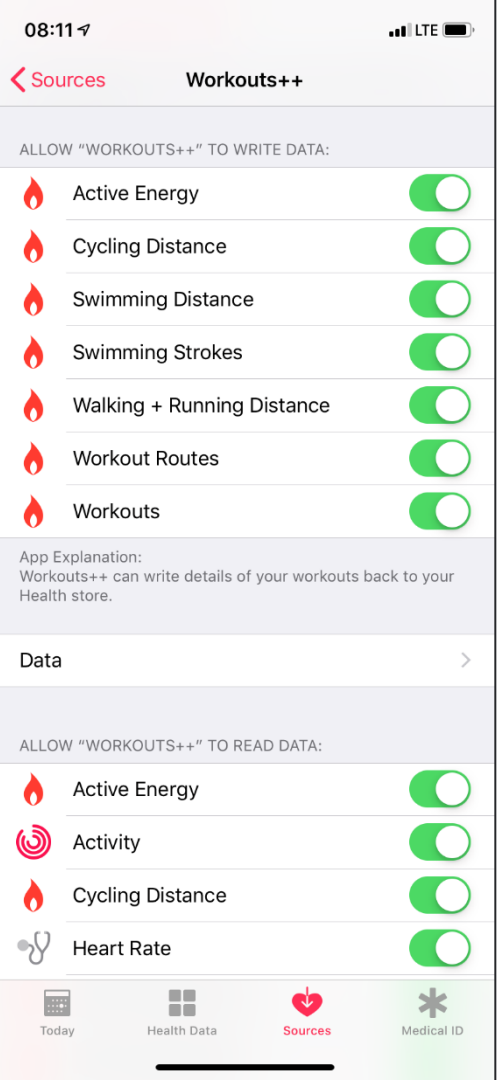
- Samsung
- Google (WearOS watches)
  - Dozens of manufacturers
- **Fitbit**

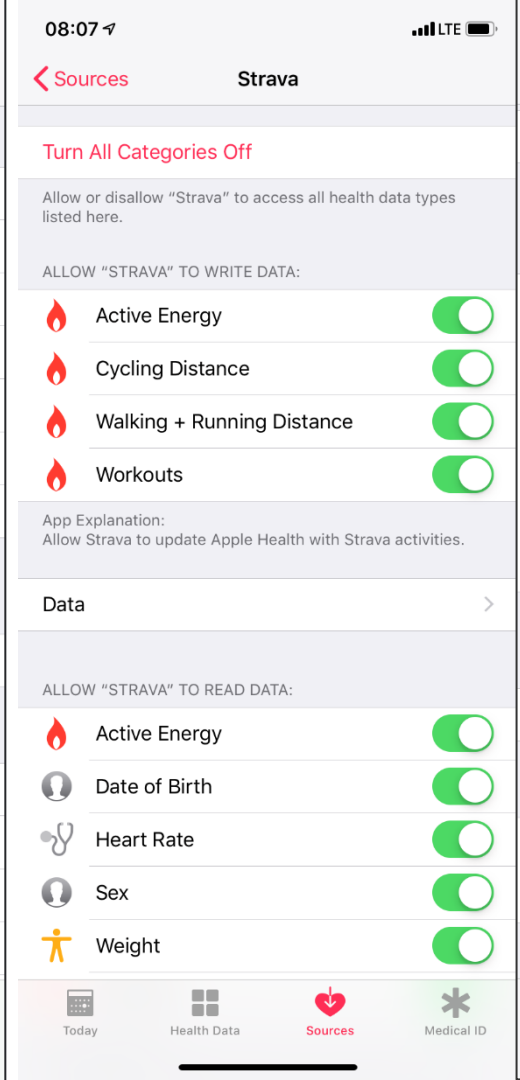
What apps contribute

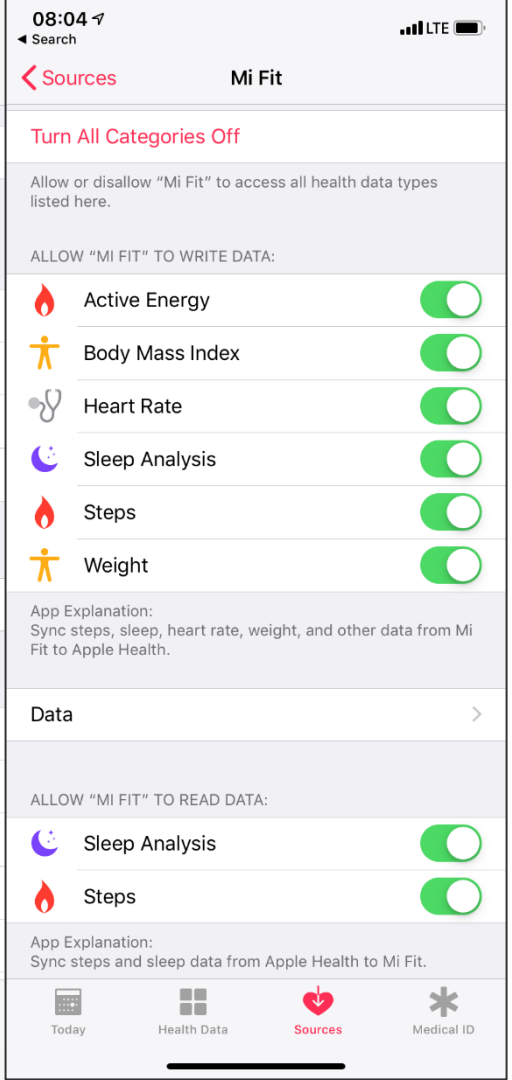
Apps contribute a lot to Health data

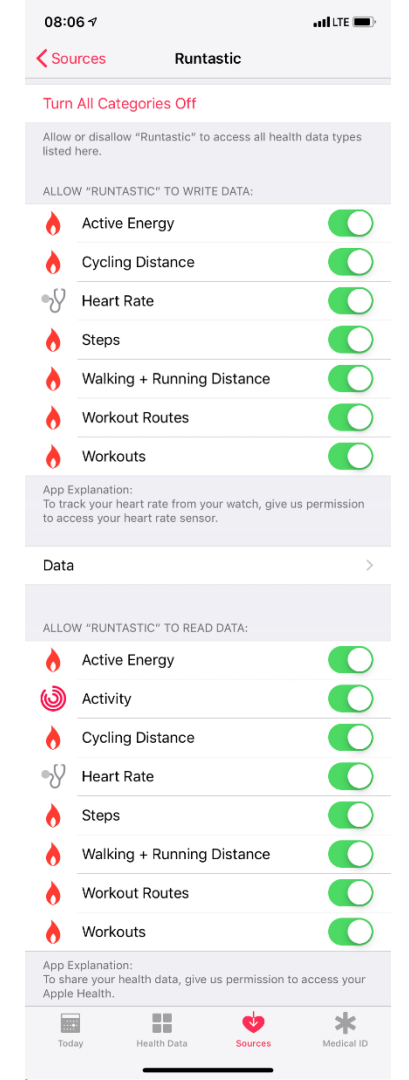
- Steps, detailed heart rate, calories burned
- GPS track, automatic workout detection
- Cycling, swimming, walking, wheelchair distances
- Weight and body mass index
- Sleep analysis
- Active energy
- And a lot more

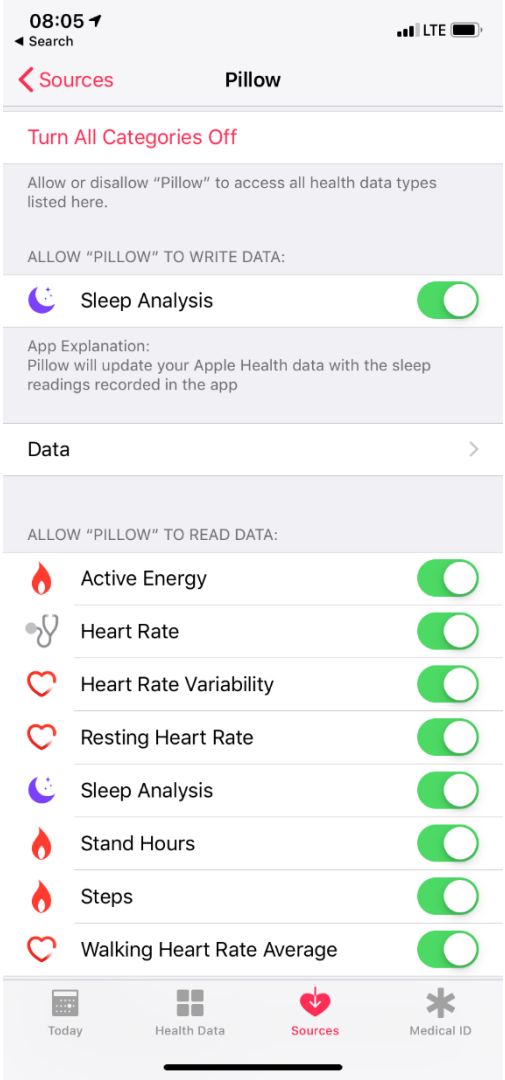


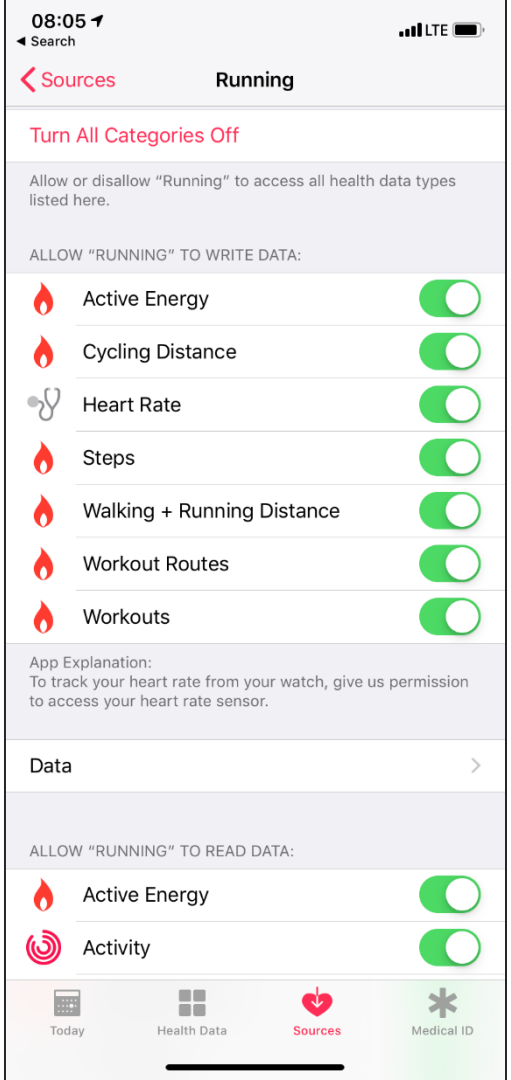

08:11
LTE
Sources
Workouts++
ALLOW "WORKOUTS++" TO WRITE DATA:
Active Energy
Cycling Distance
Swimming Distance
Swimming Strokes
Walking + Running Distance
Workout Routes
Workouts
App Explanation:
Workouts++ can write details of your workouts back to your Health store.
Data
ALLOW "WORKOUTS++" TO READ DATA:
Active Energy
Activity
Cycling Distance
Heart Rate
Today
Health Data
Sources
Medical ID

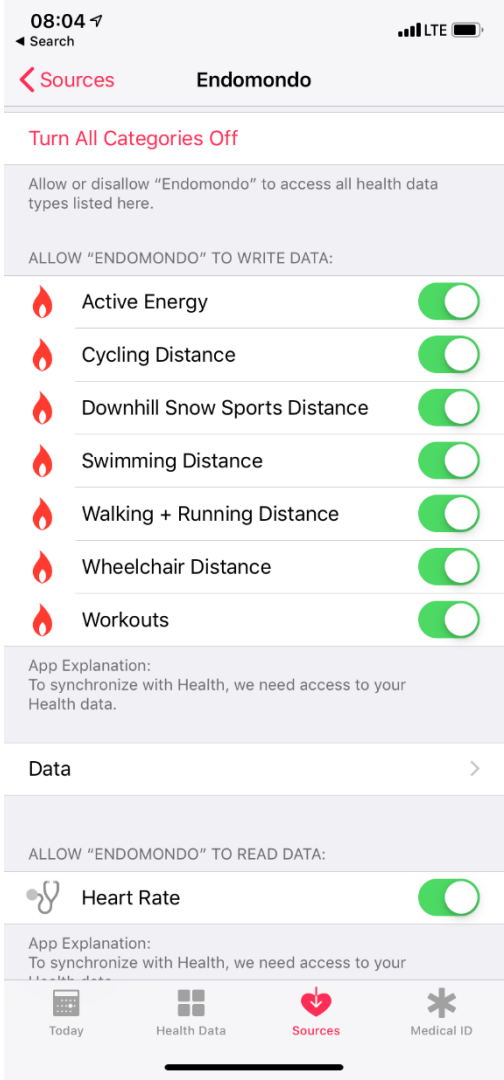

08:07
LTE
Sources
Strava
Turn All Categories Off
Allow or disallow "Strava" to access all health data types listed here.
ALLOW "STRAVA" TO WRITE DATA:
Active Energy
Cycling Distance
Walking + Running Distance
Workouts
App Explanation:
Allow Strava to update Apple Health with Strava activities.
Data
ALLOW "STRAVA" TO READ DATA:
Active Energy
Date of Birth
Heart Rate
Sex
Weight
Today
Health Data
Sources
Medical ID


08:04
Search
LTE
Sources
Mi Fit
Turn All Categories Off
Allow or disallow "Mi Fit" to access all health data types listed here.
ALLOW "MI FIT" TO WRITE DATA:
Active Energy
Body Mass Index
Heart Rate
Sleep Analysis
Steps
Weight
App Explanation:
Sync steps, sleep, heart rate, weight, and other data from Mi Fit to Apple Health.
Data
ALLOW "MI FIT" TO READ DATA:
Sleep Analysis
Steps
App Explanation:
Sync steps and sleep data from Apple Health to Mi Fit.
Today
Health Data
Sources
Medical ID


08:06
LTE
Sources
Runtastic
Turn All Categories Off
Allow or disallow "Runtastic" to access all health data types listed here.
ALLOW "RUNTASTIC" TO WRITE DATA:
Active Energy
Cycling Distance
Heart Rate
Steps
Walking + Running Distance
Workout Routes
Workouts
App Explanation:
To track your heart rate from your watch, give us permission to access your heart rate sensor.
Data
ALLOW "RUNTASTIC" TO READ DATA:
Active Energy
Activity
Cycling Distance
Heart Rate
Steps
Walking + Running Distance
Workout Routes
Workouts
App Explanation:
To share your health data, give us permission to access your Apple Health.
Today
Health Data
Sources
Medical ID


08:05
Search
LTE
Sources
Pillow
Turn All Categories Off
Allow or disallow "Pillow" to access all health data types listed here.
ALLOW "PILLOW" TO WRITE DATA:
Sleep Analysis
App Explanation:
Pillow will update your Apple Health data with the sleep readings recorded in the app
Data
ALLOW "PILLOW" TO READ DATA:
Active Energy
Heart Rate
Heart Rate Variability
Resting Heart Rate
Sleep Analysis
Stand Hours
Steps
Walking Heart Rate Average
Today
Health Data
Sources
Medical ID


08:05
Search
LTE
Sources
Running
Turn All Categories Off
Allow or disallow "Running" to access all health data types listed here.
ALLOW "RUNNING" TO WRITE DATA:
Active Energy
Cycling Distance
Heart Rate
Steps
Walking + Running Distance
Workout Routes
Workouts
App Explanation:
To track your heart rate from your watch, give us permission to access your heart rate sensor.
Data
ALLOW "RUNNING" TO READ DATA:
Active Energy
Activity
Today
Health Data
Sources
Medical ID


08:04
Search
LTE
Sources
Endomondo
Turn All Categories Off
Allow or disallow "Endomondo" to access all health data types listed here.
ALLOW "ENDOMONDO" TO WRITE DATA:
Active Energy
Cycling Distance
Downhill Snow Sports Distance
Swimming Distance
Walking + Running Distance
Wheelchair Distance
Workouts
App Explanation:
To synchronize with Health, we need access to your Health data.
Data
ALLOW "ENDOMONDO" TO READ DATA:
Heart Rate
App Explanation:
To synchronize with Health, we need access to your
Today
Health Data
Sources
Medical ID

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
- Unlike iCloud Keychain or Messages, iCloud Health data has no additional protection
  - No need to enter device passcode, no additional encryption

Apple Health

Accessing Health Data in iCloud

Use Elcomsoft Phone Breaker to download **synced data**, which includes Apple Health

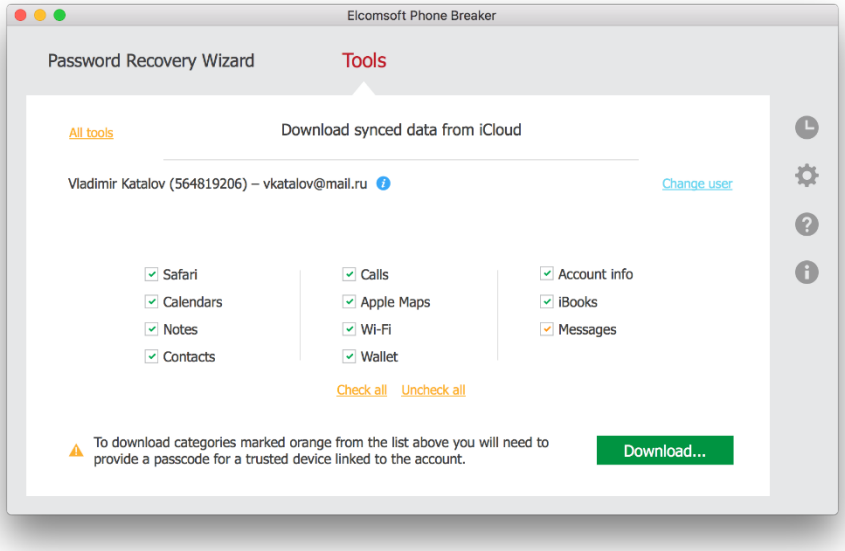
What can go wrong:

- Two-factor authentication may be an issue
- Access to secondary authentication factor is required (unless using authentication token)
- Passcode of one of the trusted devices is needed (iPhone or Mac)

Apple HealthKit

Extracting Synced Data

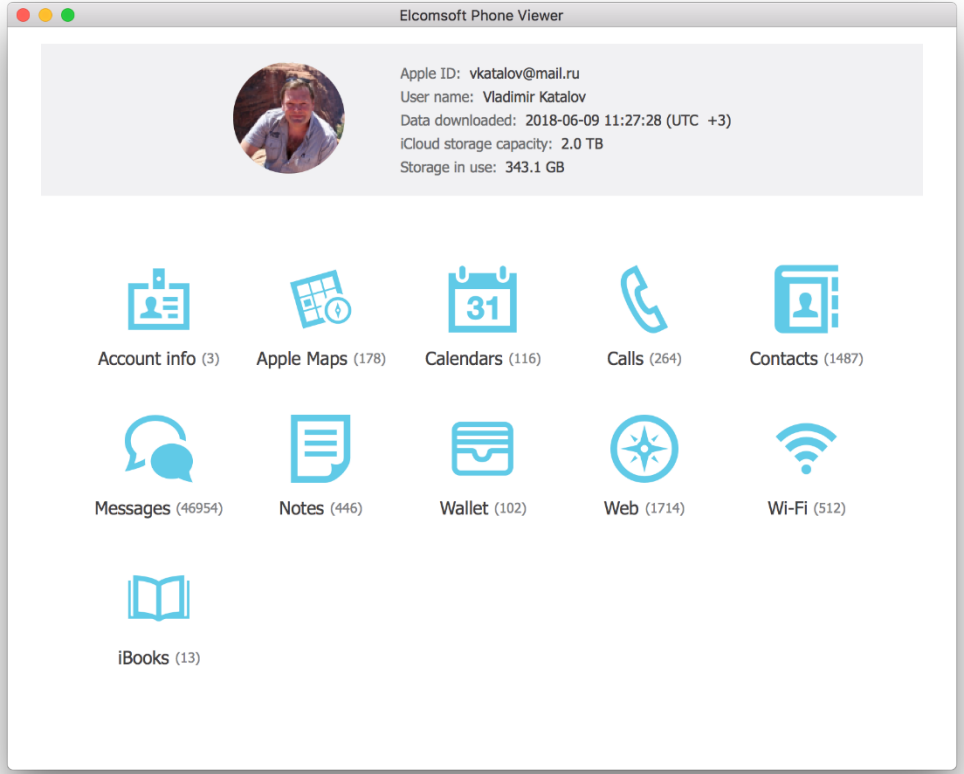
- Start Elcomsoft Phone Breaker
- Select Tools > Apple > Synced Data
- Authenticate with Apple ID and password + 2FA, or…
- Use authentication token
- Select categories to download



Apple HealthKit

Viewing Health Data

- Use Elcomsoft Phone Viewer



Google Fit

Data collected by Google Fit

- **Activity**: active minutes, activity segments, heart points, sessions (workouts), walking and running, steps, Location
- **Body Measurements**: height and weight
- **Heart**: heart rate and blood pressure
- **Nutrition**: carbohydrates, cholesterol, dietary energy, dietary fiber, protein, saturated fat, sodium, total fat, caffeine, calcium, monounsaturated fat, polyunsaturated fat, potassium, sugar, etc.
- **Sleep**: sleep data
- **Sensors**: raw timestamped sensor data

Google Fit

Where Google Fit data is stored

- Google collects Fit data only if the **optional** Google Fit app is installed from Google Play store
- The app collects and syncs Fit data with Google Drive
- Health data is stored in Google Drive with no additional protection
- Can be exported via Google Takeout, extracted with Elcomsoft Cloud Explorer or requested by LE
- Can be downloaded with updated Elcomsoft Cloud eXplorer (ETA: Q1’2020)

Google Fit vs. Apple Health

The two systems compared

- A third-party fitness tracker or smart watch device supporting both Android and iOS is more likely to share data with **Apple Health** rather than **Google Fit**
- Apple Health standardizes data. HealthKit compliant apps cannot supply types of data that are not defined by Apple.
- Google Fit will accept data of any type including unknown. Unknown types of data will not be displayed but will be synced in the cloud.

Google Fit vs. Apple Health

Security of health data in the cloud

- **Apple Health**
  - iOS 12 and 13 protect Health data with the user's device passcode
  - To extract, need all of the following: Apple ID, password, 2FA code, device screen lock passcode
  - Cannot be extracted from the cloud via GDPR requests; not provided to LE
- **Google Fit**
  - Stored in the cloud with no additional protection
  - Can be easily exported, extracted or requested from Google by LE

December 2019

Breaking Health Clouds

Fitbit and other health trackers: obtaining vital evidence for your investigation

Vladimir Katalov, ElcomSoft