HACK IN BO
Spring 2018 Edition

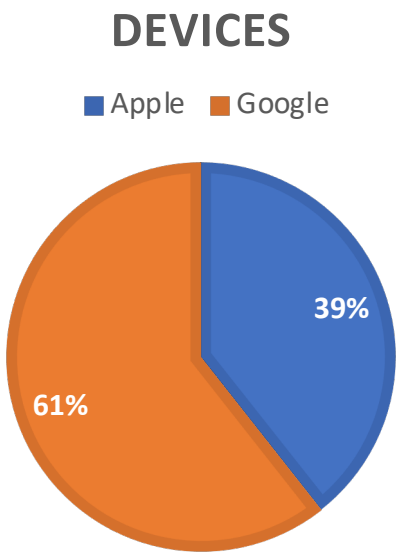
Google and Apple cloud services: real time surveillance.

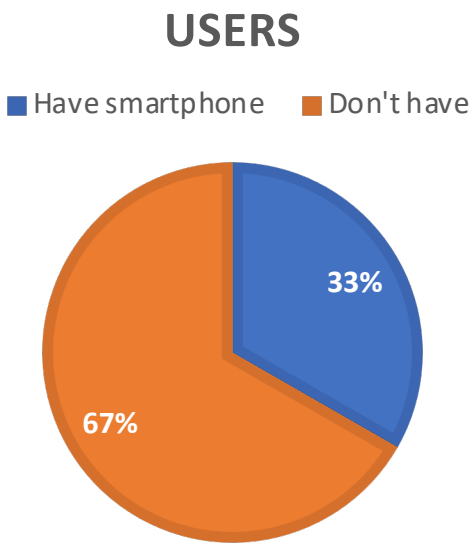
Andrey Malyshev

Elcomsoft

Smartphone usage over the world

- Apple: 1.3 billion iOS devices (2018)
- Google: over 2 billion Android devices (2017)
- 2.53 billion smartphone users in 2018 (according to Statista)





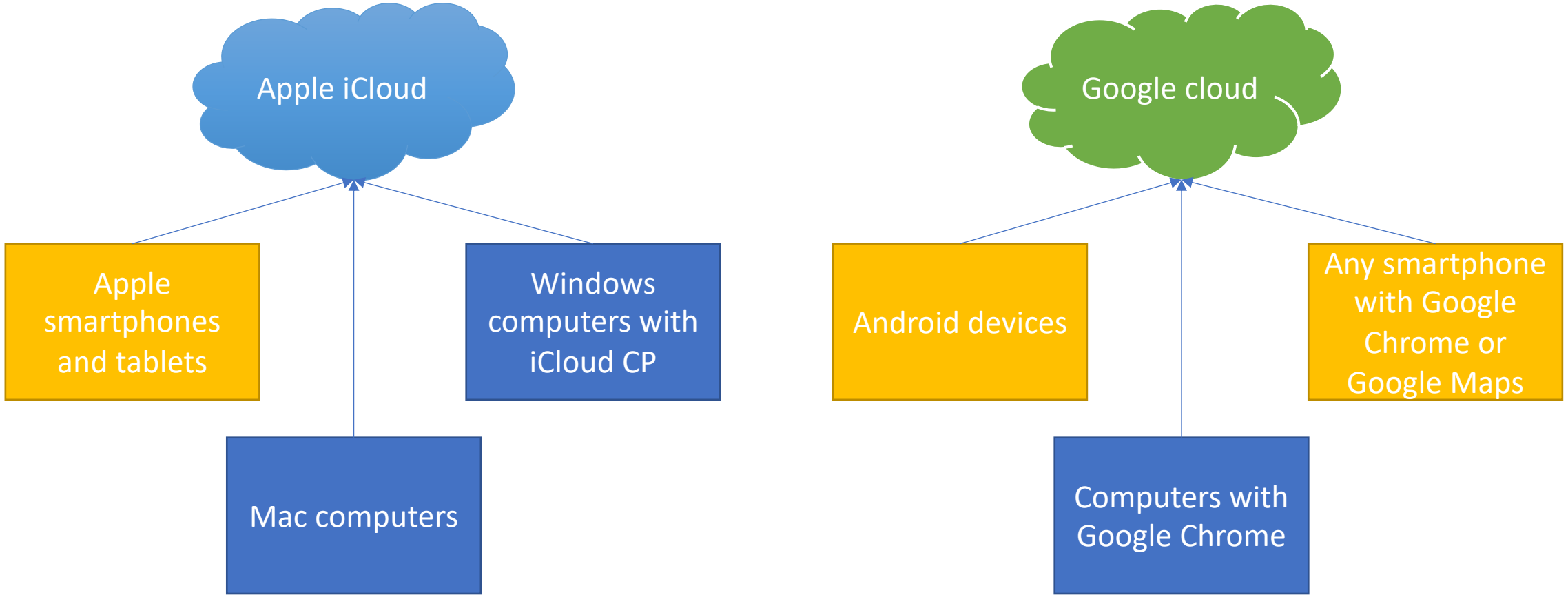
What's inside the smartphone?

- Contacts & calendars
- Call logs and text messages
- Emails and chats
- **Account and application passwords**
- **Web and Wi-Fi passwords**
- Documents, settings and databases
- Web history & searches
- Pictures and videos
- Geolocation history, routes and places
- 3rd party app data
- Cached internet data
- System and application logs
- Social network activities

What's in the Cloud?

- Apple
  - iOS device backups: 3 snapshots of each device
  - Synchronized data
- Google
  - Android device backups
  - Synchronized data

Cloud data: not only smartphones



Google and Apple cloud services: real time surveillance.

What data is synced?

Apple iOS: iCloud

- Account info
- Calendars, Contacts, Notes
- Call logs (phone, Skype, other apps)
- iOS 11.4 beta: iMessage/SMS
- Safari history, bookmarks, opened tabs
- Health data, Home, News
- Apple Maps: searches, favorites
- Wi-Fi networks
- iBooks
- iCloud Photo Library
- **iCloud Keychain**
- **FileVault2 recovery token**
- ***Some deleted data***

Google Account

- Dashboard: devices, stats and personal data
- Location and POI-based mapping data
- Google search history
- Mail, calendars, notes
- Calls
- SMS messages
- Chrome history, bookmarks, auto-fill, **passwords**
- Wi-Fi networks
- Photo library

Synced data by platform

	Apple	Google
Contacts/calendars/tasks	+	+
Call log	+	It depends
Notes	+	+
Messages	iOS 11.4 beta + 2FA	8.0+
Mail	iCloud mail	Gmail
Internet	Safari	Chrome
Media	iCloud Photo Library	Google Photos
Documents	iCloud Drive	Google Docs
Location	Current/last	Current, history
3rd party apps data	iCloud Drive	Google Drive
Other	Health, Wallet, Maps etc	Dashboard and more

Secrets stored in the cloud

	Apple	Google
Wi-Fi passwords	+	+
Web site passwords	+	+
Credit cards (autofill)	CVC/CVV is not stored	CVC/CVV is not stored
Credit cards (payment systems)	*Apple Pay (Wallet): last 4 digits only*	*Google Pay (?)*
App-specific	*It depends*	*Sometimes*
Authentication tokens	+	+
Encryption keys	+	-
Certificates	+	-
Autocomplete	+	+

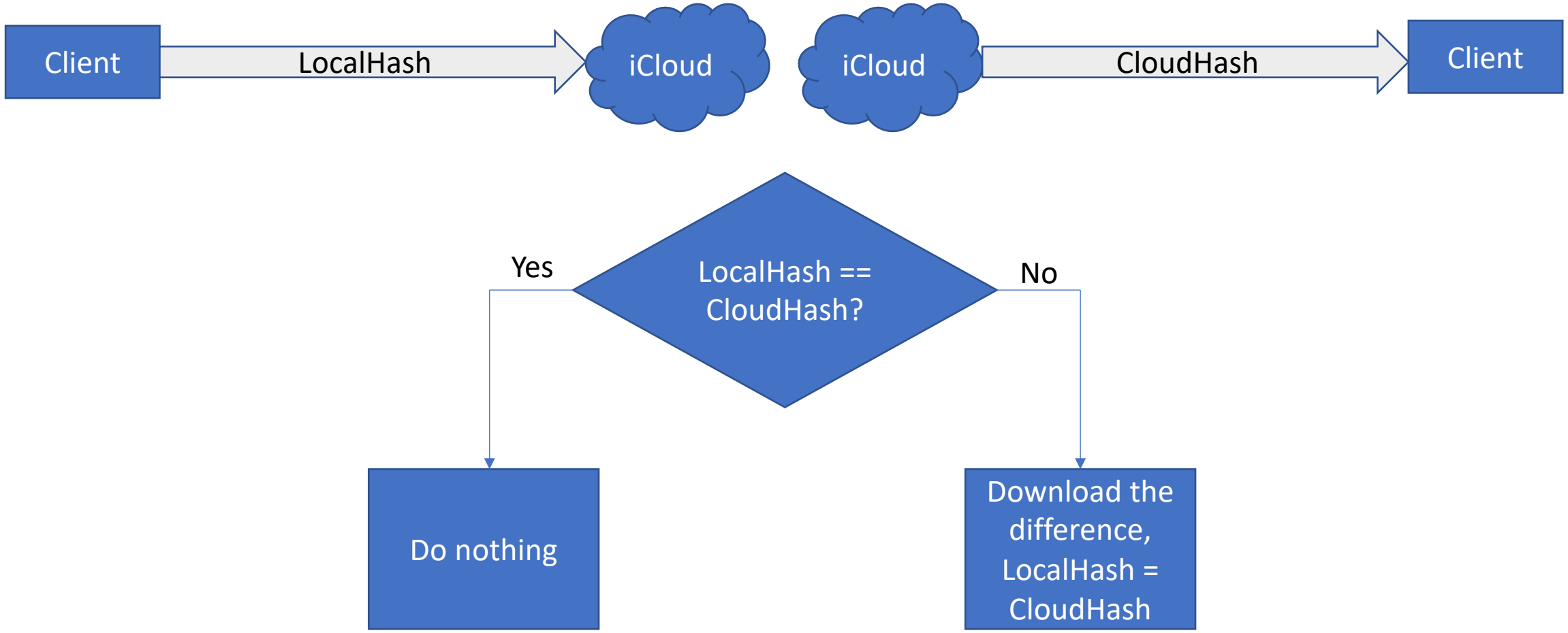
Synced data vs backups

- **Real-time synchronization**, data appears in the Cloud in several minutes.
- Backups are huge, hard to download, contain many useless information
- **Apple detects backup downloads by third-party apps and locks account**
- Some types of synced data not included in iCloud backups if sync is enabled:
  - Photos (if iCloud Photo Library is enabled)
  - Text messages and iMessages (iOS 11.4 beta, if synced)

Advantages of obtaining synced data

- Usually enabled by default
- Little known, rarely disabled
  - **Challenge**: try making your iPhone to NOT sync call logs via cloud
- **Real-time data and real-time availability**
- Deleted data is available for many categories (documents, call logs, pictures: up to 30 days)
- Weaker protection compared to cloud backups
- Current location

iCloud synced data: some technical details

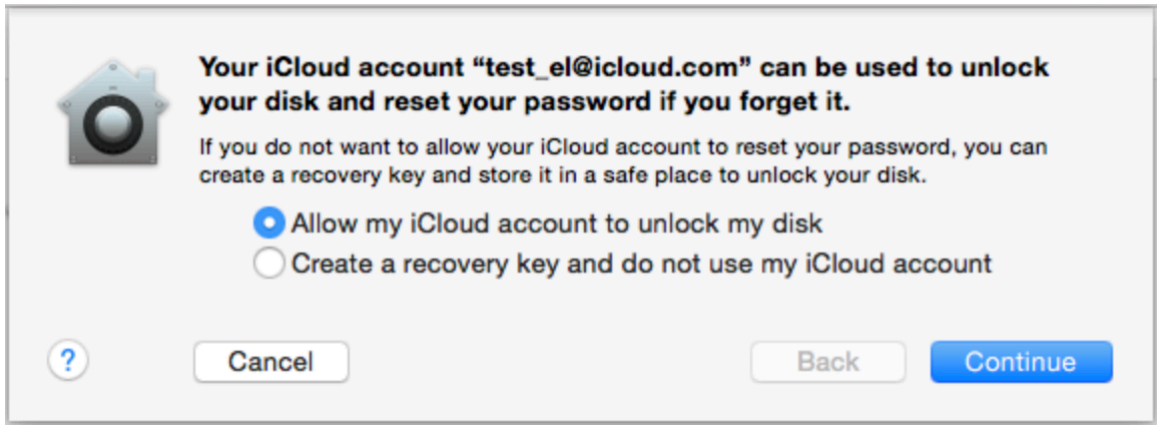


iCloud Keychain

- Synchronized over all connected devices
- Supports 2FA or iCloud security code
- Contains:
  - Apple IDs with passwords
  - Wi-Fi passwords
  - E-Mail account passwords
  - Passwords stored in browser
  - Credit cards (no CVC/CVV)
  - Authentication tokens

Apple FileVault key in iCloud

- FileVault is a disk encryption feature, introduced in OS X 10.7.
- Several methods to access encrypted volume
  - Password
  - Recovery passphrase
  - Recovery certificate
  - **Recovery key stored in iCloud**



Apple Wallet

- Stored in iCloud
- Synchronized between devices in real-time
- Contains:
  - Discount cards and coupons
  - Event tickets
  - Frequent flyer cards
  - Boarding passes

Apple iCloud: authentication tokens

- Tokens are binary files
- Do not contain account password or password hash
- Are saved to desktop computers to access iCloud from iTunes or iCloud CP
- Allow users to bypass entering login-password
- **Allow investigators to bypass 2FA**

Apple iCloud: Anisette data

- Anisette data is a set of binary data stored on PC or Mac
- It’s random data, generated by Apple servers
- It’s downloaded when user logged into iCloud and completely passed 2FA
- When we have Anisette data, second step of 2FA is not needed
- But we still need login and password

Apple authentication token limitations

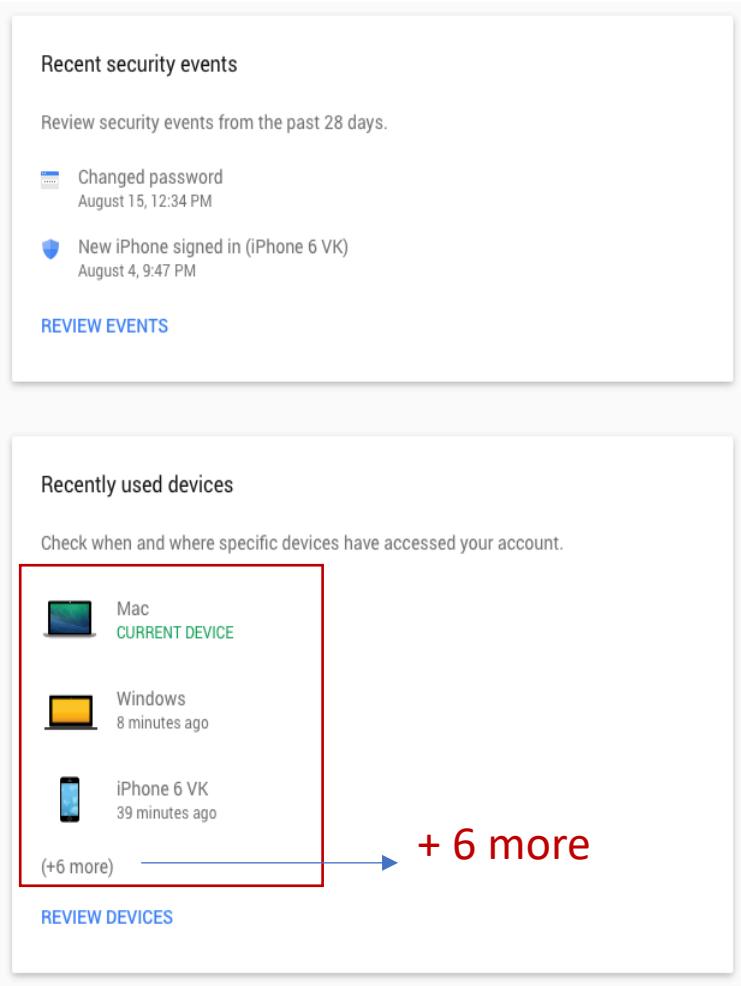
- **iOS 8**: Authentication tokens are short-lived
  - iCloud backups can only be downloaded within a limited timeframe
  - Exact expiry timeframe not known

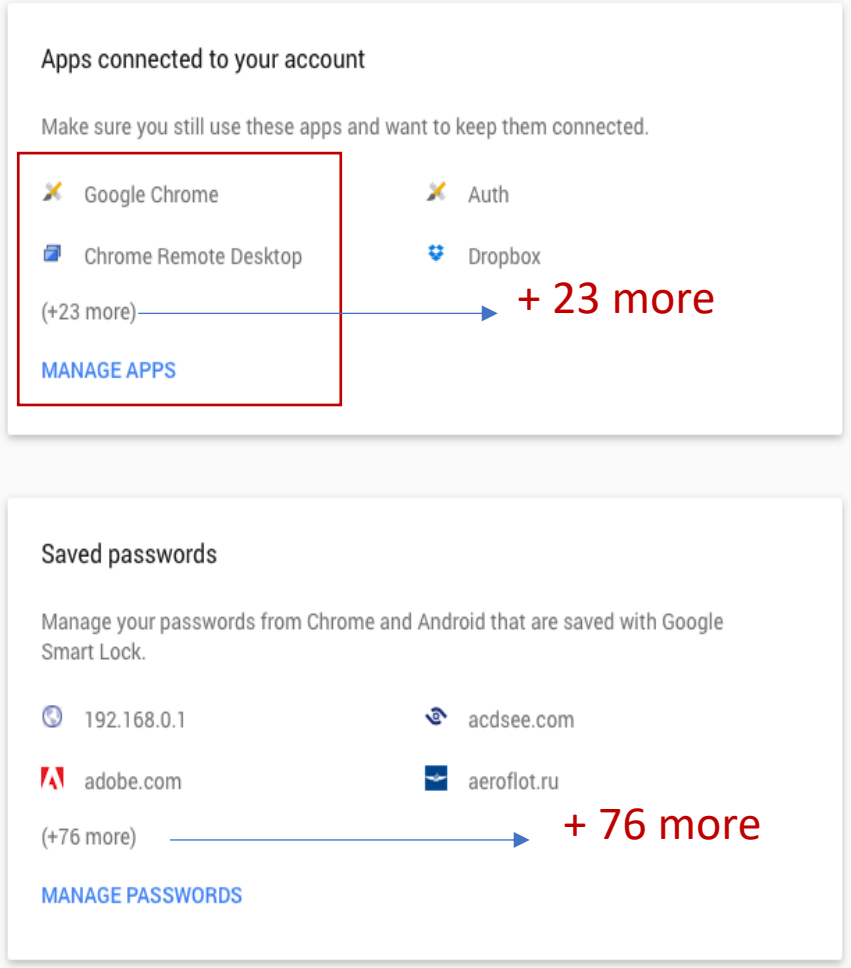
- **iOS 9, 10**: Backups stored in iCloud Drive, authentication tokens do not expire

- **iOS 11**: authentication tokens expire again; after expiration, allow to get everything but iCloud backups (so only files at iCloud Drive, synced data, iCloud Photo Library)
- **iCloud keychain**: the other token (+anisette data); heavily obfuscated private APIs in macOS X

Google: collecting data from multiple sources

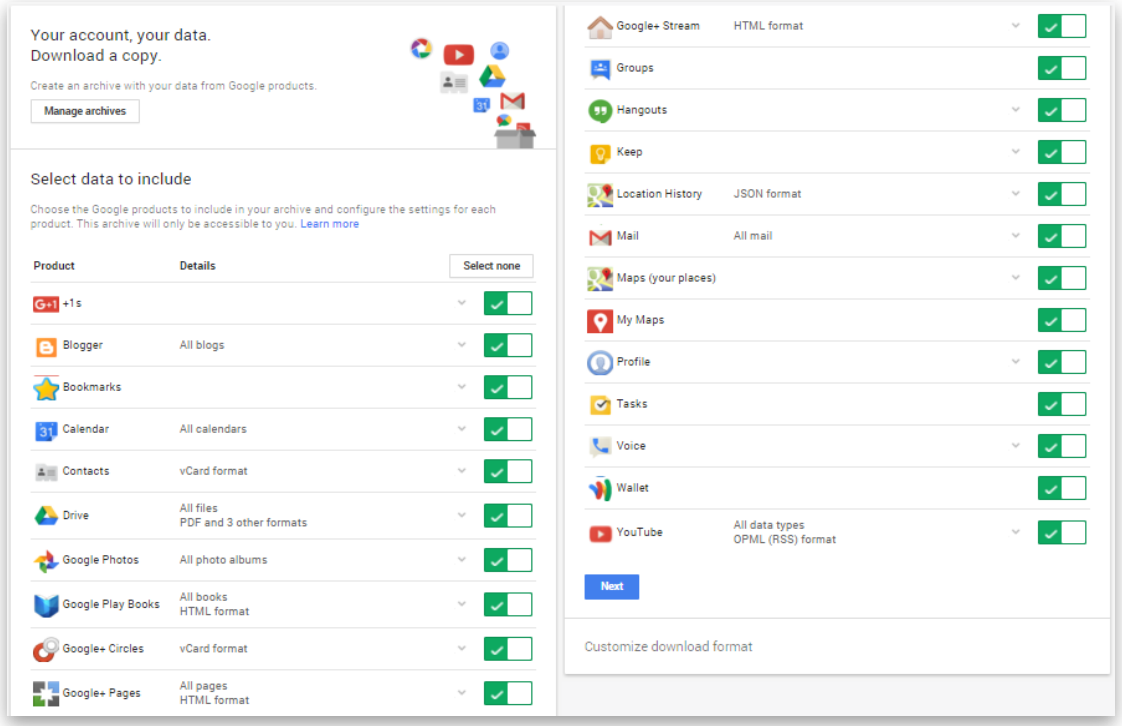
- Multiple devices
  - Mac
  - Windows
  - iPhone
  - iPad
  - …and Android
- Apps
  - Dropbox
  - Auth
  - Chrome
  - Remote desktop
  - Many more





Google Takeout

- Leaves many traces
- Not everything is exported
- Limited flexibility
- Numerous awkward formats
- User alerted via email



Google Dashboard – not available in Google Takeout

Account
- email
- number of Google API clients (sites and apps)
- account time: personal, work, both
- Activities in last 28 days
    - browsers and OSs that had access
    - locations
    - new apps and sites

YouTube
- number of videos and playlists loaded
- user name
- sex
- last video rating (+video name and date)
- activities for last 28 days
    - number of views, by day
    - total views
    - searches
    - likes and dislikes

Search history (query + date)
- last Web search
- last image search
- last news search
- last video search
- last maps search
- last books search
- activities for last 28 days
    - top 10 searches
    - percentage of searches by category (web, image etc.)
    - activity (by day)

Google Sync. (non-Android devices)
- number of bookmarks
- last sync date
- number of passwords
- number of Chrome extensions

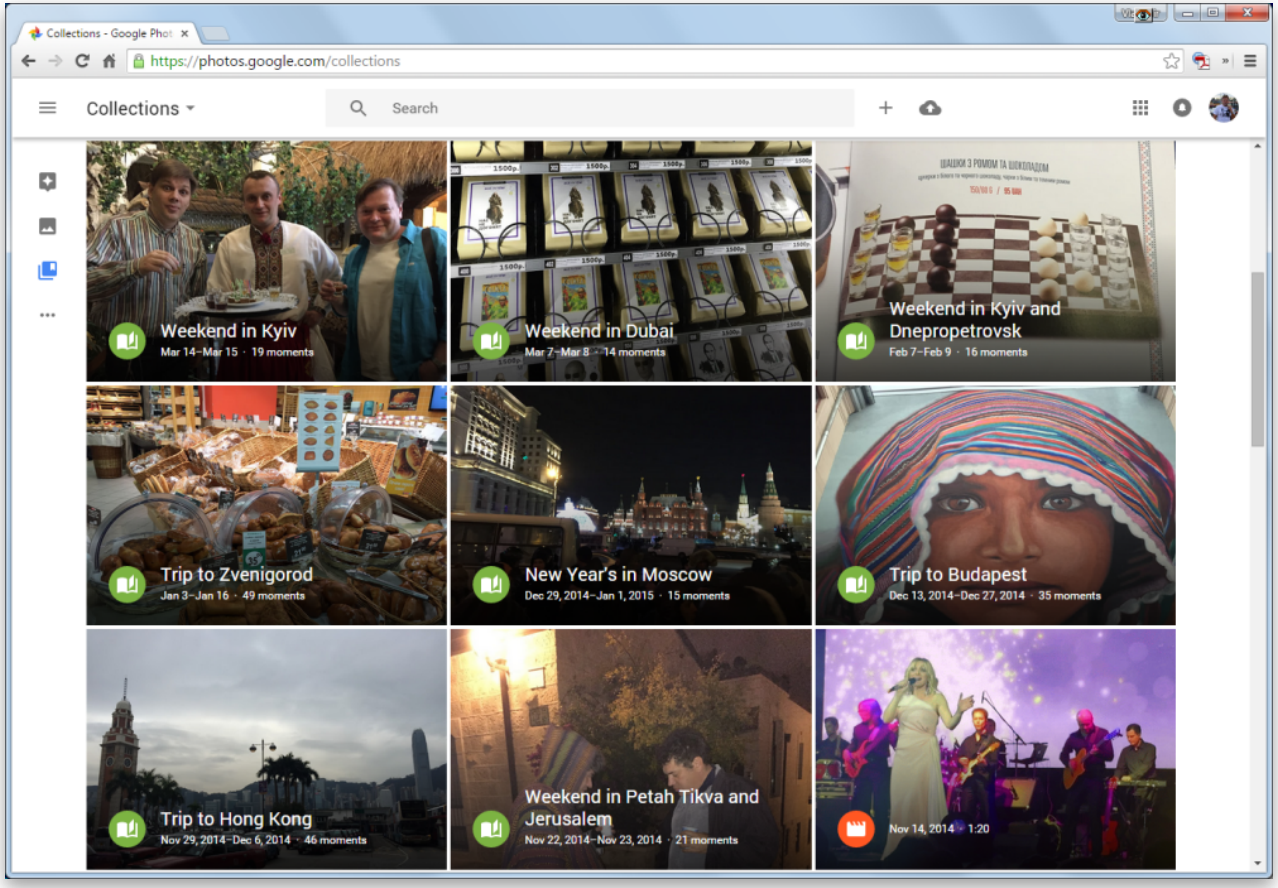
Profile info
- Google+ name
- profile URL
- number of phone numbers
- number of "+1"

Gmail
- number of mail threads
- last thread subject
- number of messages in inbox
- last incoming message subject
- number of sent mails
- last sent mail subject

Android
- make, model
- first auth date/time
- last activity date/time
- apps that backup their data (name, date, size)

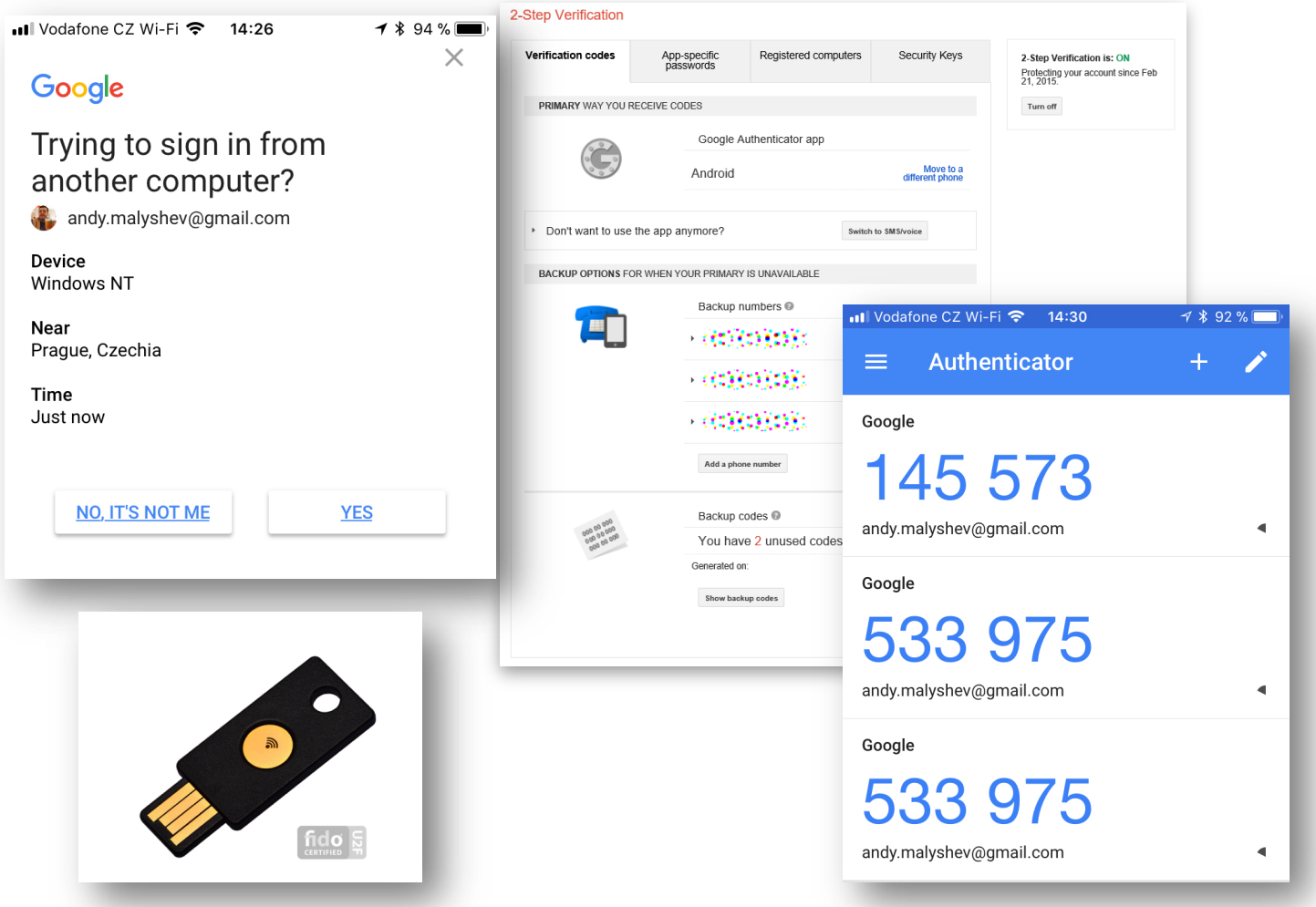
Google Photos

- Albums/events
- Comments
- EXIF
- Geo tags
- Subscriptions
- View counters
- People



Google account: 5 different 2FA types

- Google prompt: application on mobile device
- Authenticator app: time limited codes
- Single-use backup codes
- SMS codes
- FIDO hardware security key (Yubico etc)
- **All 2FA types can be bypassed using authentication token from Google Chrome or Google Drive**

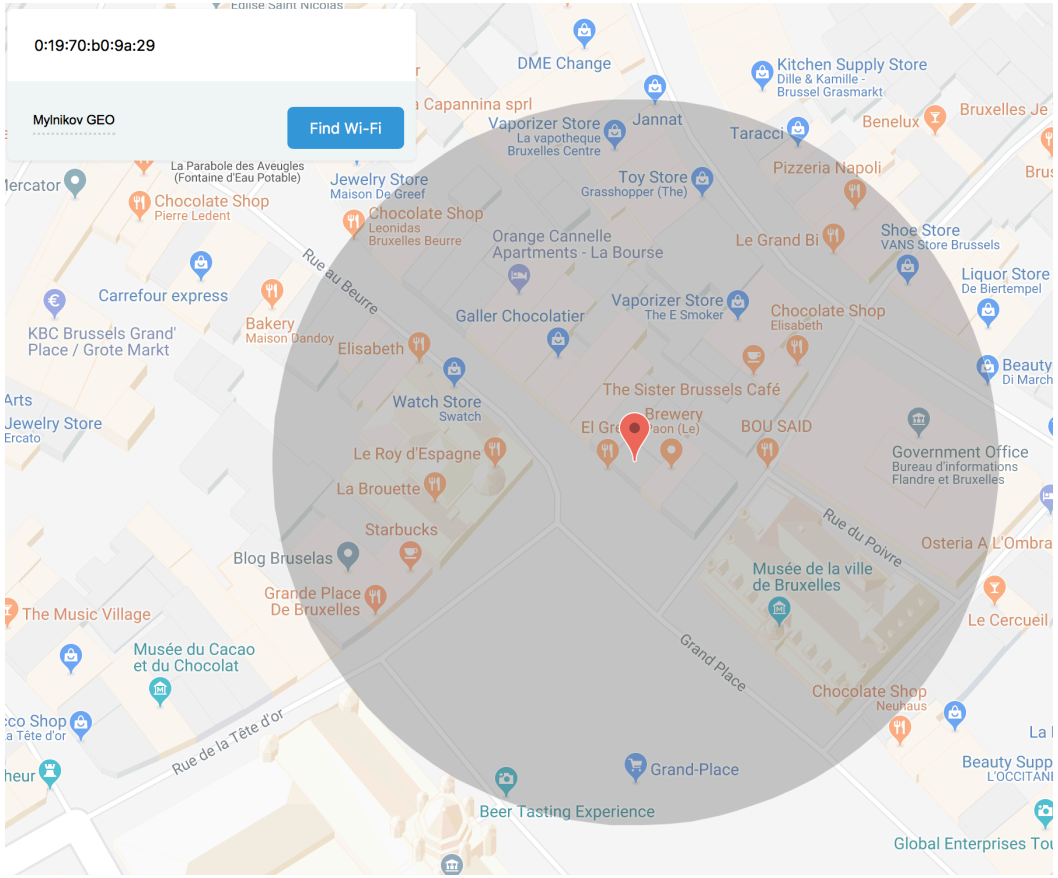


Locations by devices and applications

Source	On device	Apple iCloud	Google cloud
Apple device: last location	+	+	-
Apple device: location history	+	-	-
Apple Maps: searches and favorites	+	+	-
Apple: significant locations	+	-	-
Google Maps: Android devices	+	-	+
Google Maps: iOS and WM devices	+	-	+
Uber	+	Backups	-
Other taxi services	It depends	?	?

Wi-Fi hotspots: getting locations

- Both Google and Apple clouds store wi-fi hotspot BSSID
- BSSID can be used to determine hotspot location
- Databases of hotspot locations:
  - Google
  - Mylnikov GEO
  - Wigle.net
  - openBMAP



Synchronized data: conclusion

- Apple and Google collect as much data as possible
- Most of data is synchronized in real-time
- Both Apple and Google use 2FA to secure cloud access
- In certain cases 2FA can be bypassed using authentication tokens

HACK IN BO®
Spring 2018 Edition

Thank you!

Andrey Malyshev

Elcomsoft s.r.o.

www.elcomsoft.com

andy@elcomsoft.com