AVANSIC®

E-Discovery & Digital Forensics

evidence at your fingertips.

Mobile Device Forensics and User Tracking

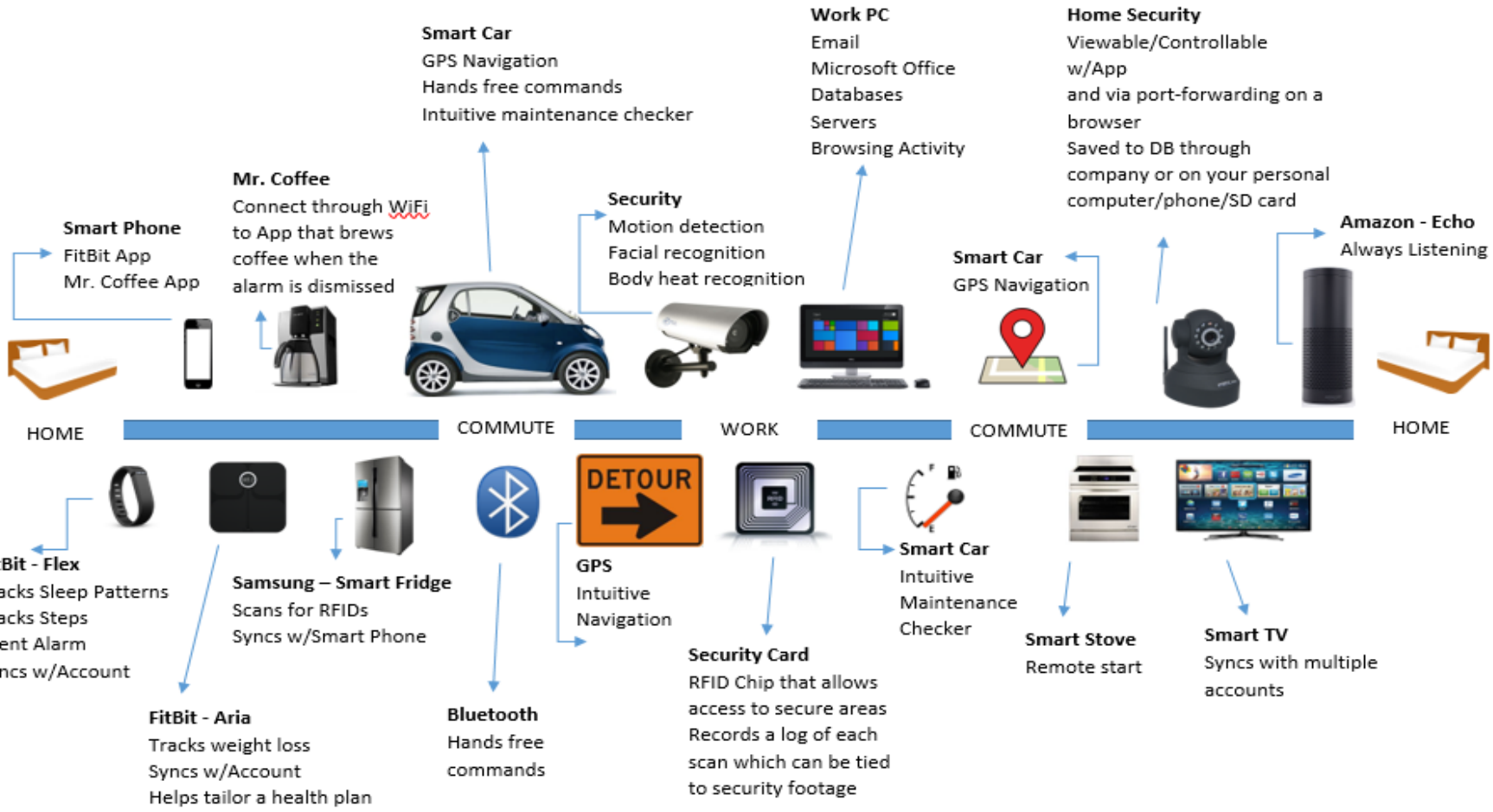
Lance Watson, Chief Operating Officer

George Patterson, Manager of Research & Development

Agenda

- Mobile Device Forensics
  - What can be found
  - Does device type matter?
  - Is possession the same thing as authorization?
  - BYOD
  - What needs to be in an agreement to investigate a phone
  - Does my agreement allow me to access additional platforms (ie, Facebook, corporate email) through the phone?
- User Tracking
  - Mobility Usage Reports
  - Google Maps
  - Other location information

Connected Devices



Storage Capacity

- Devices can store data themselves
- Most data is in the cloud
  - Temporary cache on the phone
- Historically, data was easily and quickly overwritten
  - Most modern phones will have, for example, the entire call history

Connected Data

Cell Phone Forensics

- Challenges
  - iPhone vs. Android
  - Large number of operating system versions
  - Cables
- What can be retrieved (but not always)
  - Call times and durations
  - Text messages
  - Contacts
  - Photos & videos
  - Calendar
  - List of installed apps
  - Device ID capture
- Can sometimes retrieve deleted information

Locked Devices

- Need the access to retrieve the maximum amount of information
- May be able to get some data without the passcode
  - More devices are now encrypted – the data may be available but isn't useable without the passcode

Collection Types

- Physical
  - Forensic bit-by-bit acquisition
  - Most comprehensive extraction of data
  - Allows for data carving
  - Limited to Android or older (4 and before) iPhones
  - May require rooting
- Logical
  - Active data
  - For iPhones, similar to backup process through iTunes
  - Won't find deleted data the OS doesn't know about
- File System
  - Performed by interacting with the operating system

Syncing

- Email
  - Forensic collection can retrieve some email header information
  - Won't retrieve the body of the email
- Social Media
  - Need to have the username and password
  - Otherwise, search warrants and law enforcement may be necessary
- Phone Backups
  - iCloud, Google, LG Backup, Samsung Kies, etc.

External Data and Preservation

- Time is of the essence
  - Must preserve key data soonest
  - Must be handled as evidence in order to ensure admissibility
  - Some sites have a "self-preserve" feature (Facebook)
- Not easy
  - Some service providers are cooperative, most are not
  - Cloud/synced data can be difficult to locate
  - May actually be on a local computer or server

Mobility Usage Reports

- From the telephone carrier
  - By subpoena or court order
- Call, text and data usage over time
  - Be specific in what you request
  - May not include cell tower location data unless requested
- Call information
  - Who contacted who
  - When and for how long
- SMS/MMS information
  - Who contacted who and when
  - WILL NOT CONTAIN CONTENT OF MESSAGE
- Data Usage
  - How much data up and down
  - Aggregate Only – NOT ASSOCIATED WITH A GIVEN APPLICATION

Location Tracking

- Google Maps
  - If location services are on, can provide a map indicating data sources contacted and general direction of travel.
  - Accessing History will show a blue line for general direction of travel
    - Not 100% accurate as to actual roads used.
  - Turning on Raw Data will show data sources used to calculate the blue line

Case Studies and Legal Discussion

- Geolocation
  - Driver of an 18-wheeler hits a sedan, determining where the accident happened
  - Determining whether the driver was on the phone and what they were doing
  - Right to monitor employees via GPS on their mobile devices

Conclusion

- Information available for retrieval depends on the device
- Devices and their operating systems are very rapidly changing
- Devices have a large number of configurations
- User tracking information can be available in data sources outside the device
- Mobile devices are a goldmine of information