PROGRAM MATERIALS
Program #32242
October 27, 2022

Your Home is Spying on You: A Look at Internet of Things Forensics

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Your Home is Spying on You: A Look at Internet of Things Forensics

Brian M. Chase, Esq.
Managing Director, Digital Forensics

ARCHERHALL
AIM HIGH

BChase@ArcherHall.com
855.839.9084

Digital Forensics & eDiscovery experts serving attorneys in all 50 states

- Cellphones
- Computers & Tablets
- External Hard Drives
- Smart Devices
- Emails & SMS
- Social Media Accounts
- Cloud Data
- Electronic Medical Records

BUSINESS LITIGATION

EMPLOYMENT LAW

SCHOOLS AND HIGHER-ED

MEDICAL MALPRACTICE

IP THEFT

BANKRUPTCY

About Brian Chase

- Undergraduate Degree in MIS from the University of Arizona
- Law Degree from the University of Arizona
- Licensed to practice law in Arizona and New York
- Director of Digital Forensics at ArcherHall
- Adjunct Professor of Law at the University of Arizona
- Numerous digital forensics certifications
- Testimony in State and Federal Court, Civil and Criminal Cases
- Misdemeanor and Felony trials as an attorney

INTERNET OF THINGS AND THE SMART HOME

ARCHERHALL
AIM HIGH

Internet of Things (IoT)

The Internet of Things is the term given to devices other than traditional computers, laptops, and tablets that connect to the Internet.

Examples include:

- Refrigerators
- Thermostats
- Lightbulbs
- Echo/Google Home
- Ovens
- Smart Locks

The “Smart Home”

Smart Home is the term used to describe homes full of IoT devices that control various aspects of your home.

Think of an Amazon Echo combined with a Nest Thermostat, Hue Lightbulbs, and a Ring Video Doorbell.

All of these devices can communicate together and you can control them with your voice through the Echo.

But all of these devices also record data…

“Alexa, did you hear a murder”

ARCHERHALL
AIM HIGH

“Alexa, did you hear a murder?”

- Murder in 2015 in Arkansas
- James Bates had work friends over to watch football and agreed to let two of them crash at his house.
- The next morning he wakes up to find his friend, Victor Collins, dead in his hot tub
- He calls 911
- Police investigate and find broken knobs and bottles, as well as blood spots near the hot tub
- Medical Examiner rules the death a homicide, police get a search warrant for the house

“Alexa, did you hear a murder?”

- During the search, police discover an Amazon Echo
- They seize the device and send a warrant to Amazon
- In the warrant affidavit they write that they have:
  - “reason to believe that Amazon.com is in possession of records related to a homicide investigation being conducted by the Bentonville Police Department.”

How The Echo Works

- Connects to your home WiFi
- Listens for the wake word of “Alexa” (Can be changed)
- After it hears the wake word, it records your request and sends it to Amazon
- Amazon servers process the request and the Echo provides a response
- Amazon saves the recording

Amazon Fights the Warrant

- Amazon refuses to turn over the data
- They assert the First Amendment protects speech gathered by the device
- They say police must prove a compelling need for the data and that it must be specific and integral to the investigation

- The Result?

- None. Bates agrees to the release of the data and Amazon complies. No ruling from the court

But the police had more

The Echo was not the only smart device in Bates' home

There was a smart water meter, which measured water usage down to the hour

Between the hours of 1:00 and 3:00 am, Bates used 140 gallons of water

Earlier that evening when all the men were together watching football, they never used more than 10 gallons of water within an hour

But the police were wrong

Bates had a step counting app on his iPhone

The iPhone showed that once he went to bed, he didn't get up again

FITBIT DATA

ARCHERHALL
AIM HIGH

Fitbit solves a murder

- On December 23, 2015, Connecticut police respond to the home of Richard Dabate
- Mr. Dabate describe their fight with a home intruder who zip tied him to a chair, cut him with a knife, demanded his wallet and credit cards, and shot his wife in the basement
- Mr. Dabate's story started falling apart and police looked to digital devices for evidence

Fitbit solves a murder

- Dabate's wife was wearing a Fitbit.
- Examination of the data revealed she logged 1,200 steps after the time Dabate said the intruder shot her
- Police looked at other data including home alarm sensors, Facebook activity, and cellphone records

Crying Wolf with a Fitbit

- In Pennsylvania, a woman called 911 and said she was raped
- Said she woke up at midnight to the assailant on top of her
- Claim she lost her Fitbit while struggling with him
- Cops found the Fitbit and examined the data – showed she was up all night walking around.
- Cops used this evidence along with other signs that there was no rape and charged her with false reporting.

IoT Frees an Innocent Man

- On May 21, 2016, Nicole Vander Heyden was found beaten and strangled to death
- The night before she was at a concert with her boyfriend, Doug Detrie
- Text messages show she accused him of cheating on him
- Blood found in the garage of their home
- Cord used to strangle her found across the street
- Police arrest Detrie, believing he killed her at home, disposed of the body in a field

IoT Frees an Innocent Man

- Detrie was wearing a Fitbit
- It showed he had one a few steps at night – going to the bathroom, checking on their baby
- Had Progressive Snapshot for his car – showed the car didn't move that night
- DNA evidence pointed to another man, George Burch
- Google Location data put Burch at all of the locations as Heyden, including her house and field were she was found

Strava maps out military bases

- Strava is an app that works with devices like Fitbit to track location
- Strava released data as a type of fitness social networking
- People were quick to find paths at military installations and even CIA Black Sites
- The data could even be filtered down to the individual level to track specific people

Tell-Tale Heart

- Ross Compton in Ohio claimed his house went up in flames
- Before it burned down, he was able to pack several bags and a suitcase
- He had an artificial heart implant and a pacemaker
- Police got a warrant for data from the pacemaker
- A cardiologist reviewed the data and said the story was highly improbable
- Mr. Compton was charged with arson

Echo calls a friend

- A Portland couple were talking about hardwood floors in their house
- They receive a call from the husband's employee telling them to disconnect their Echo
- Their Echo sent their conversation about the floors to the employee
- Amazon investigated and confirmed the Echo sent the conversation due to mishearing key words in the conversation

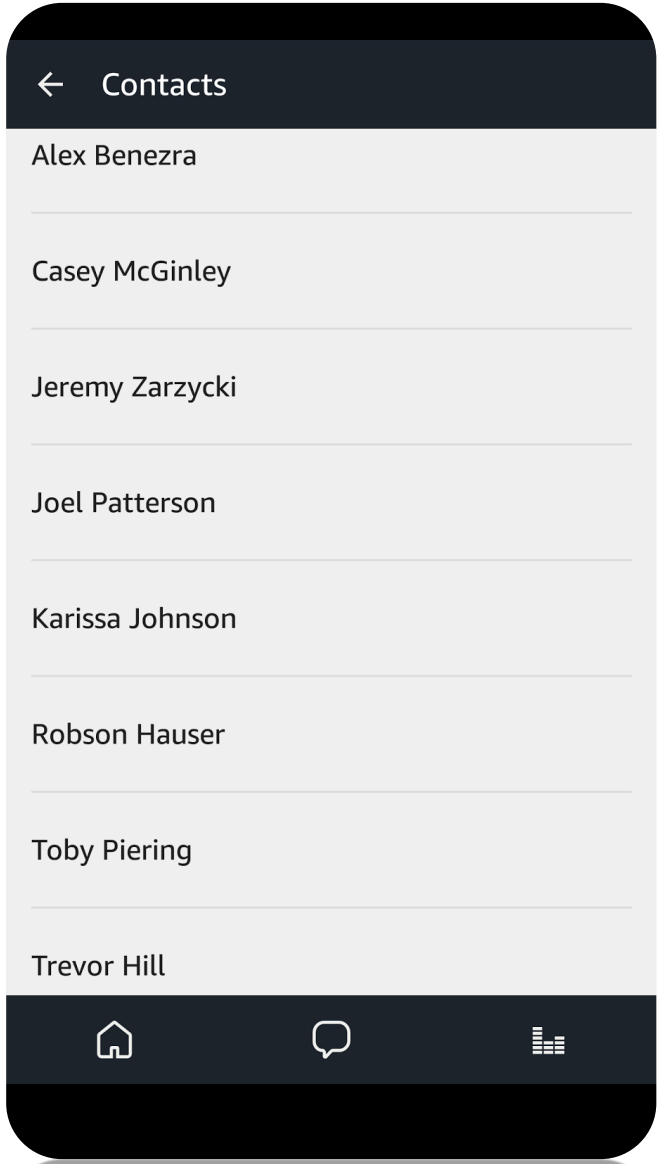
Smart Device Calls the Cops

- A smart device called police in New Mexico in the middle of a domestic violence incident
- Eduardo Barros was housesitting with his girlfriend and their daughter
- A fight ensued and Barros drew his gun
- He yelled “Did you call the sheriffs”
- This triggered the smart device, which heard “call the sheriffs” and it did
- Police arrived and arrested Barros

Smart Device Calls the Cops

One Problem:

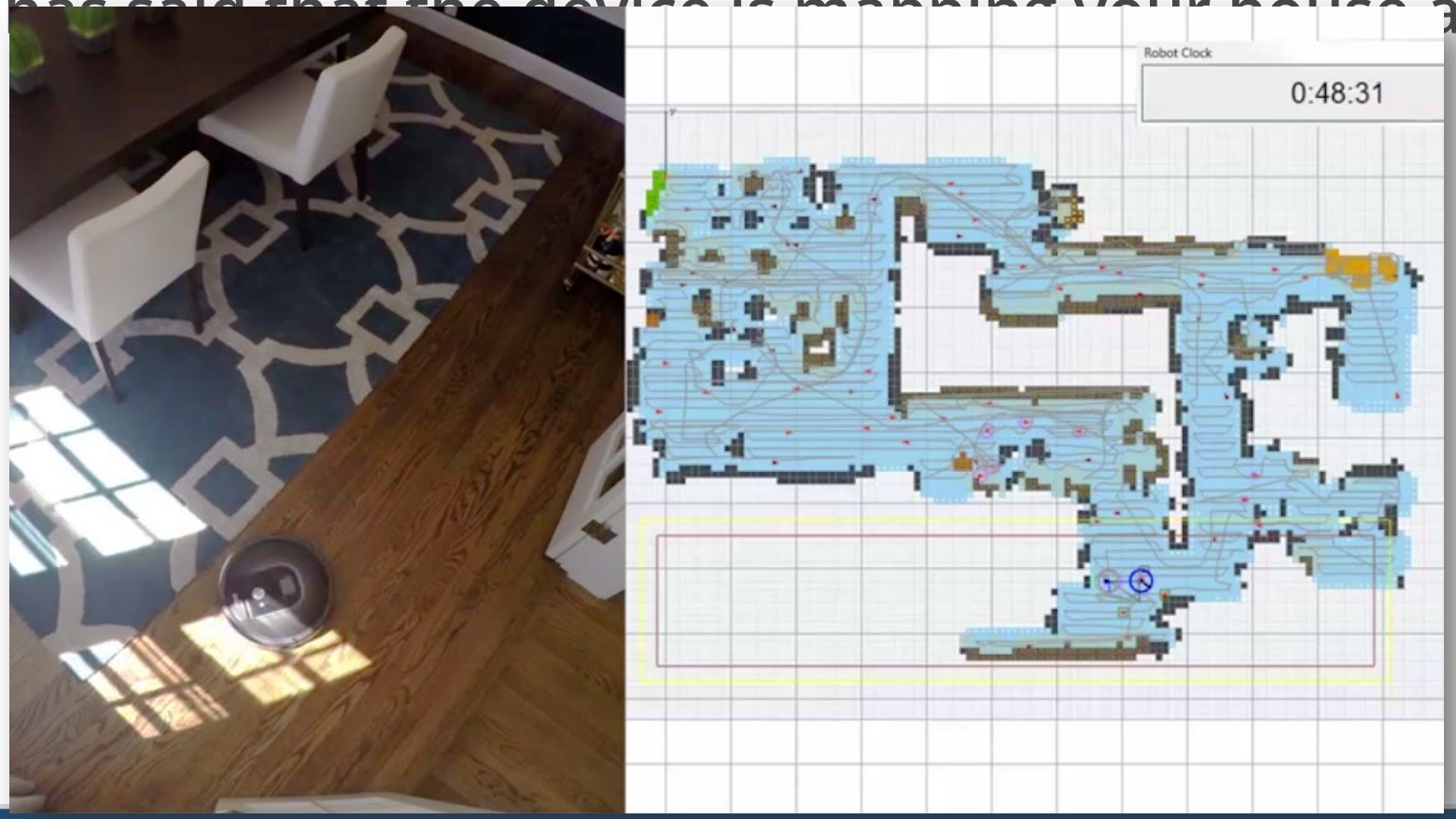
- This is was not possible



But it can call a Judge (or a Lawyer)

Roomba Mapping Your House

- New WiFi enabled Roombas can be controlled remotely and by the Echo
- Roomba has said that the device is mapping your house as it moves



Wifi enabled creepy toys

How about sex toys?

- “Qiui Cellmante is a connected sex toy with a companion app to control its locking/unlocking via Bluetooth that is typically managed by someone else than the person wearing the device.”
- Researchers found they could use a six-digit "friend code" and receive "a huge amount of information about that user," such as location, phone number, plain text password.
- Following the disclosure, an attacker started targeting Qiui Cellmate mobile app users who controlled the smart toy and locked the chastity device. Victims were asked to pay 0.02 bitcoins, around $270 at the time of the attacks.

Smart Locks

Nest

When it all goes wrong

WHERE TO GET THE DATA

ARCHERHALL
AIM HIGH

Where to get the data?

Device

Within the device itself

Phone

In the associated app

Cloud

From the cloud provider, or using authentication data from phone

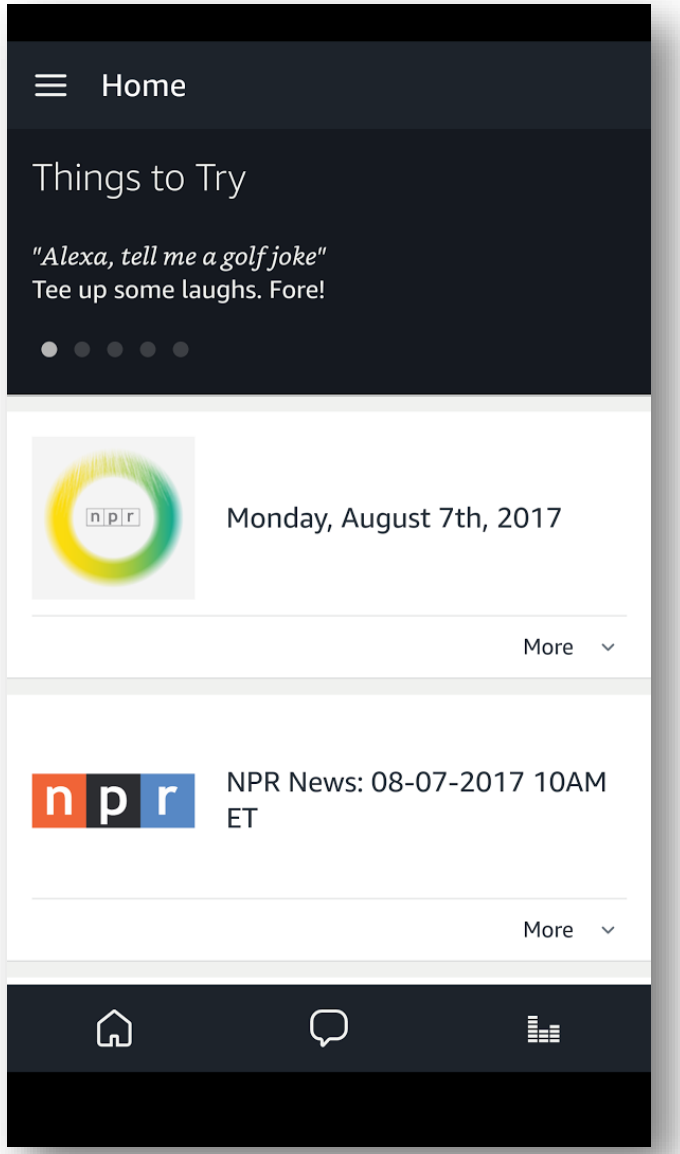
Device Forensics

Some of the data resides directly on the IoT device

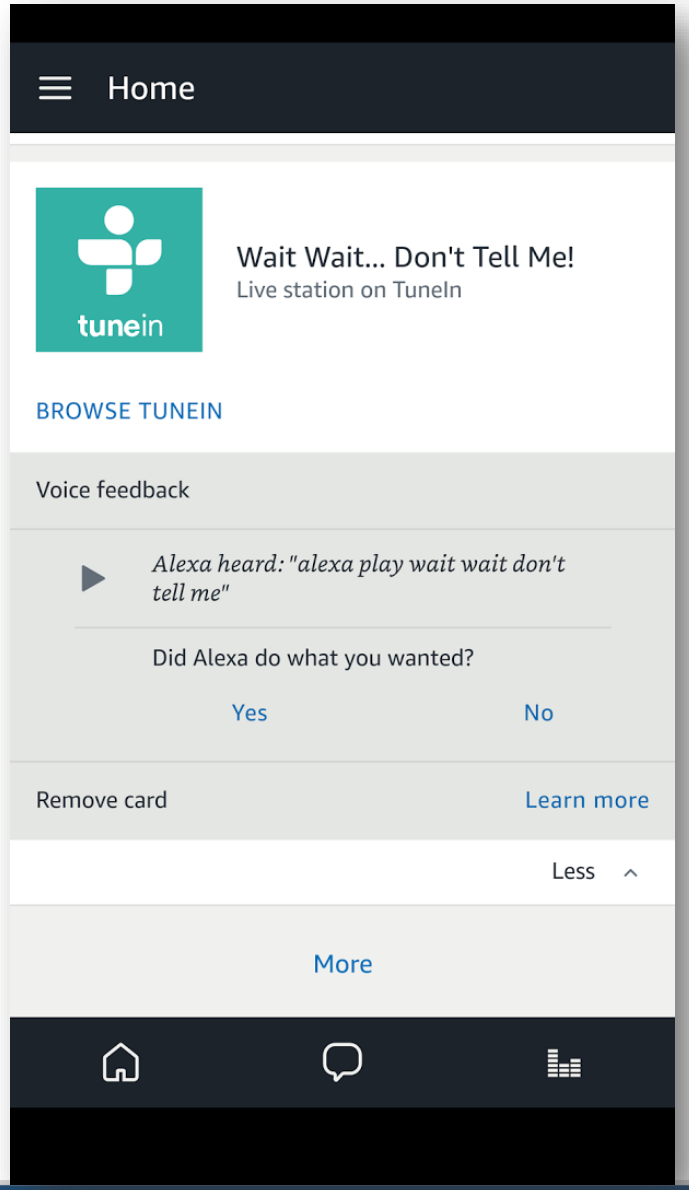
Investigators are learning how to dissemble the devices and find the data

This is time-consuming and expensive – don't expect to see it often

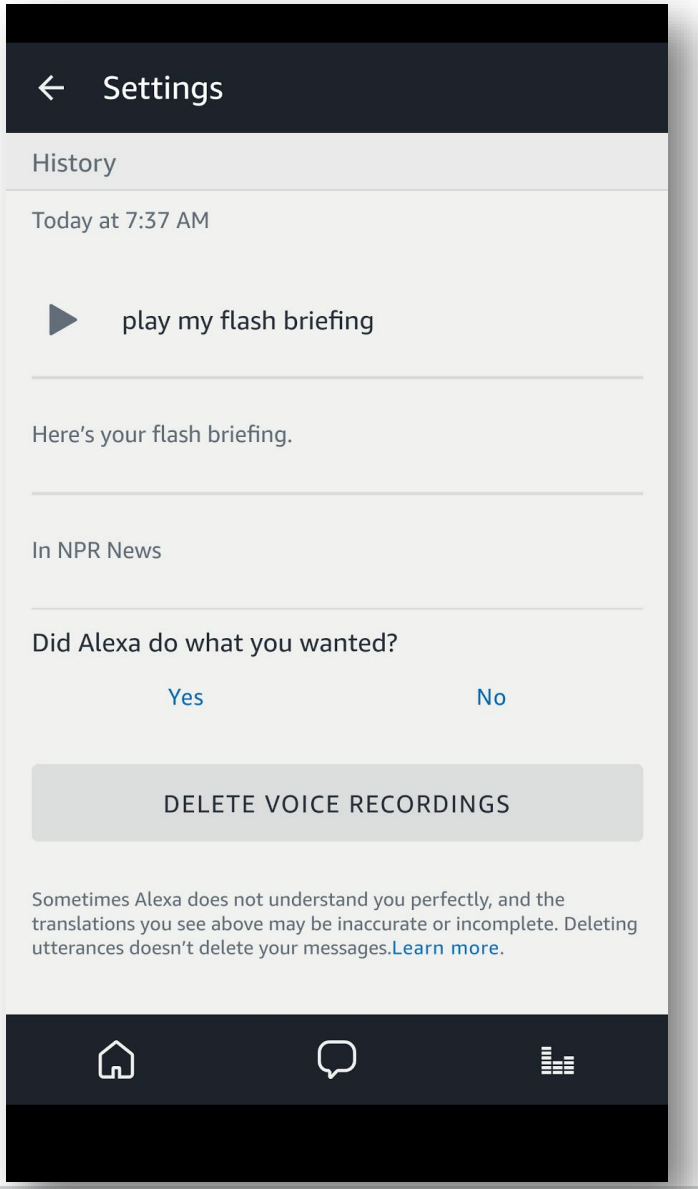
A look at the phone



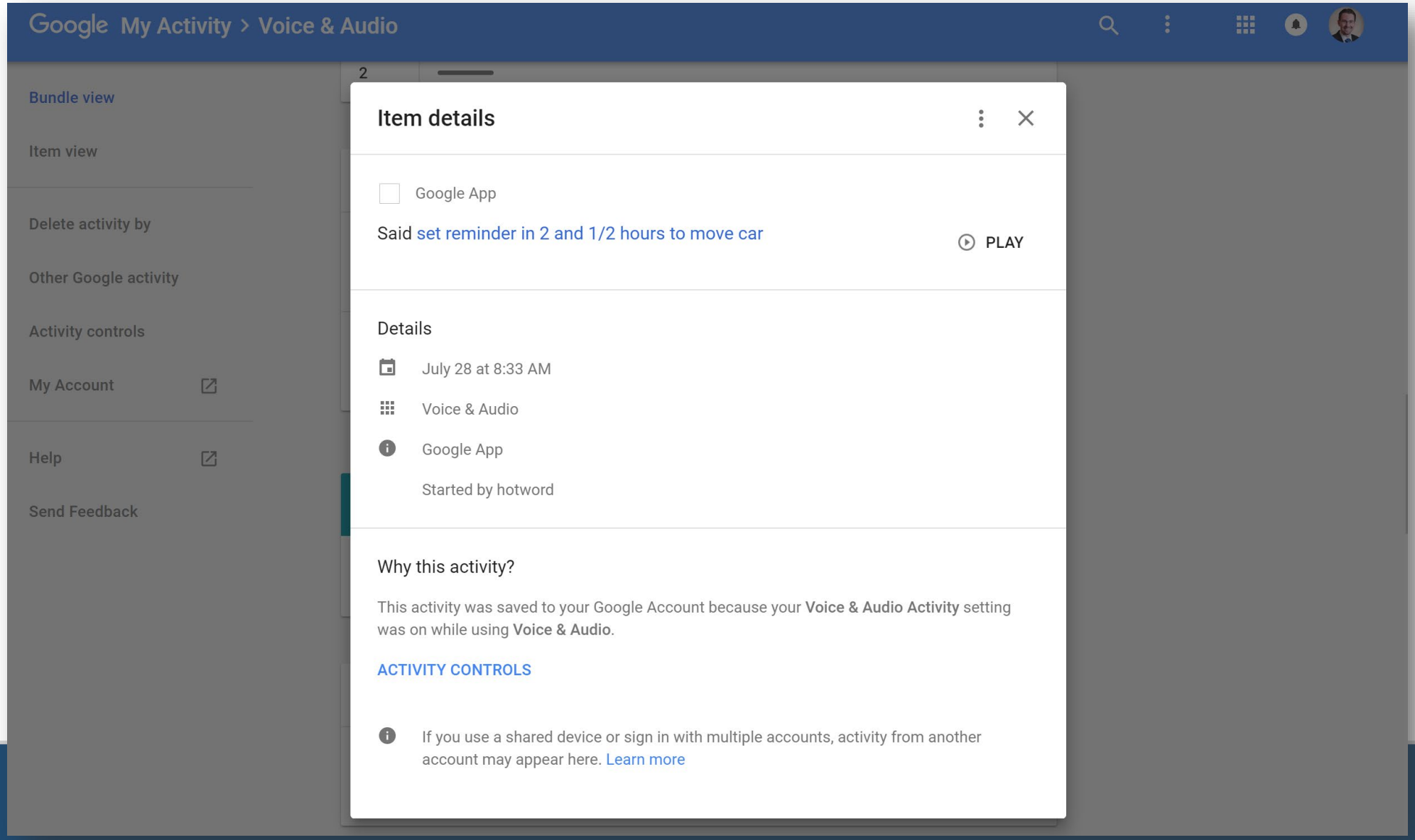
A look at the phone



A look at the phone



Google Voice Searches



Cloud Forensics

- Much of this data resides in the cloud
- There is forensic software for cloud based data
- Take authentication data from the phone
- Put that data into the cloud forensic software
- The forensic software then downloads the data from the cloud

Google Takeout

https://takeout.google.com

- You need client's username and password
- May need second factor device (like their phone)

Other Cloud Sources

Facebook	Instagram	Twitter	Amazon
• Go To Settings, Your Facebook Information	• Go to Privacy and Security, Data Download	• Go to Settings, Your Twitter Data	• Create an Order History Report

Is a warrant required?

Third-Party Doctrine

- No reasonable expectation of privacy in information knowingly and voluntarily revealed to third parties.
- See United States v. Miller (1976) and Smith v. Maryland (1979)

1986 Electronic Communications Privacy Act (Stored Communications Act) allows law enforcement to access account data without a warrant

- If a "wire or electronic communication" has been in electronic storage for more than 180 days or is held "solely for the purpose of providing storage or computer processing services" the government can use a search warrant, or, alternatively, a subpoena or a "specific and articulable facts" court order (called a §2703(d) order) combined with prior notice to compel disclosure.

But what about Carpenter?

Carpenter v. U.S., 138 S.Ct. 2206 (2018)

- Law Enforcement obtained 127 days of historical cell site location information
- Obtained under the Stored Communications Act
- Supreme Court rules a warrant required for 7 days or more
- Declines to apply third-party doctrine as CLSI is "an entirely different species of business record"

Carpenter raises the possibility that other kinds of records may required compliance with the Fourth Amendment:

Online Accounts

- Lower courts often required warrants for email, social media, etc.
- One Court has held a warrant is not required for IP Address information

Modern Bank Records

- Banks offer more services than they did at the time of *Miller.*
- May need a warrant if records resemble confidential communications

Smart Devices

- Smart device data stored in the cloud
- *Naperville Smart Meter Awareness v. City of Naperville,* 900 F.3d 521 (7th Cir. 2018) held that the collection of smart-meter electricity data at 15-minute intervals constituted a Fourth Amendment search.

What about Particularity Requirement?

United States v. Blake, 868 F.3d 960 (11th Cir. 2017)

- Suggests government should request particular categories of data, not the whole account
- "We are not convinced that the cases … which involve seizing an entire hard drive located in the defendant's home and then later searching it at the government's offices, are applicable in the social media account context."

Stored Communications Act

- Stored Communications Act – 18 USC 121, Sections 2701-2712
- Part of the 1986 Electronic Communications Privacy Act
- Prohibits a subpoena alone to obtain data

- Allows for disclosure when:
  - To the intended recipients or agent of intended recipient
  - With lawful consent of the communications originator, addressee, or intended recipient
  - Third party's employer or authorized to forward the communication to its destination
  - Disclosure to law enforcement (Warrant) or court order

The Lessons?

Don’t overlook the tiny devices	Some data types are easy and inexpensive to collect	Data can provide critical evidence in litigation	The data can be misleading
• Large amounts of data available from IoT Devices	• Cloud sources can often be obtained within hours	• Users’ locations, behaviors, and personal details may all be available	• Take precautions when evaluating the weight of the evidence

We’d love to hear from you!

Brian M. Chase, Esq.
Director, Digital Forensics

BChase@ArcherHall.com
(855) 839-9084

ARCHERHALL
AIM HIGH