

42 CALORIES
LOCATION: VIENNA

104 BPM
3.58 KM



HOW SAFE IS YOUR QUANTIFIED SELF?

ATTACK POINTS IN HEALTH APPS & WEARABLE DEVICES



Candid Wüest

SECURITY RESPONSE

Thanks To: Mario Ballano & Hon Lau

 Symantec

WHAT IS QUANTIFIED SELF?

Intersection of major consumer & IT trends
Recording everything about your life



WHERE THE BITS FIT IN

More moving parts = more risks



UNINTENTIONAL DATA LEAKS

The secret life of mobile apps...

MAX DOMAINS
CONTACTED

14

AVG DOMAINS
CONTACTED

5



APP ANALYTICS

AD NETWORKS

APP PROVIDER

OS PROVIDER

SOCIAL MEDIA

APP FRAMEWORKS

CRM/MARKETING

UTILITY API

VERIFY THE DEFAULT SETTINGS!

Example: Fitbit once had the “sexual activity” visible to all by default

Google search results for "sexual activity" site:fitbit.com:

About 199 results (0.05 seconds)

Advanced search

Everything Images Videos News Shopping More

Chicago, IL Change location

All results Sites with images Related searches

More search tools

Fitbit Profile www.fitbit.com/user/22DP9H/activities - Cached
Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 1:00 am. N/A 45 minutes 70 ...

Activities - Fitbit Profile www.fitbit.com/user/22B6GD/activities/date/2010-11-14 - Cached
Nov 14, 2010 – Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 12:00 am. N/A 30 minutes 37 ...

Fitbit Profile www.fitbit.com/user/222ZN6 - Cached
May 31, 2011 – **Sexual Activity**. General, moderate effort. started at 10:45 pm. N/A 20 minutes 36. Total N/A 20 minutes 36 ...

Activity Records Sat Jun 18 10:10:00 UTC 2011 See ... - Fitbit Profile www.fitbit.com/user/223C7F - Cached
Jun 20, 2011 – **Sexual Activity**. Active, vigorous effort. started at 11:30 pm. N/A 1 hour 30 minutes 191. Total N/A 1 hour 30 minutes 191 ...

Activities - Fitbit Profile www.fitbit.com/user/227QSS/activities
Feb 2, 2011 – **Sexual Activity**. Passive, light effort, kissing, hugging. N/A 10 minutes 9 ...
Sexual Activity. Active, vigorous effort. N/A 15 minutes 21 ...

DATA “CUSTODIANS”

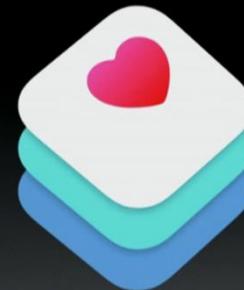
It is personal identifiable information, but not as we know it
“Apps that access HealthKit are required to have a privacy policy,...”
Apple.com

From the analyzed apps

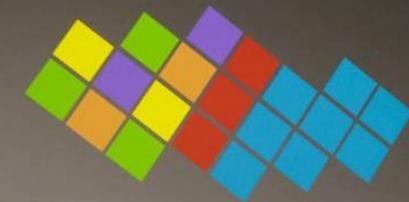
52% had no privacy policy



Google Fit



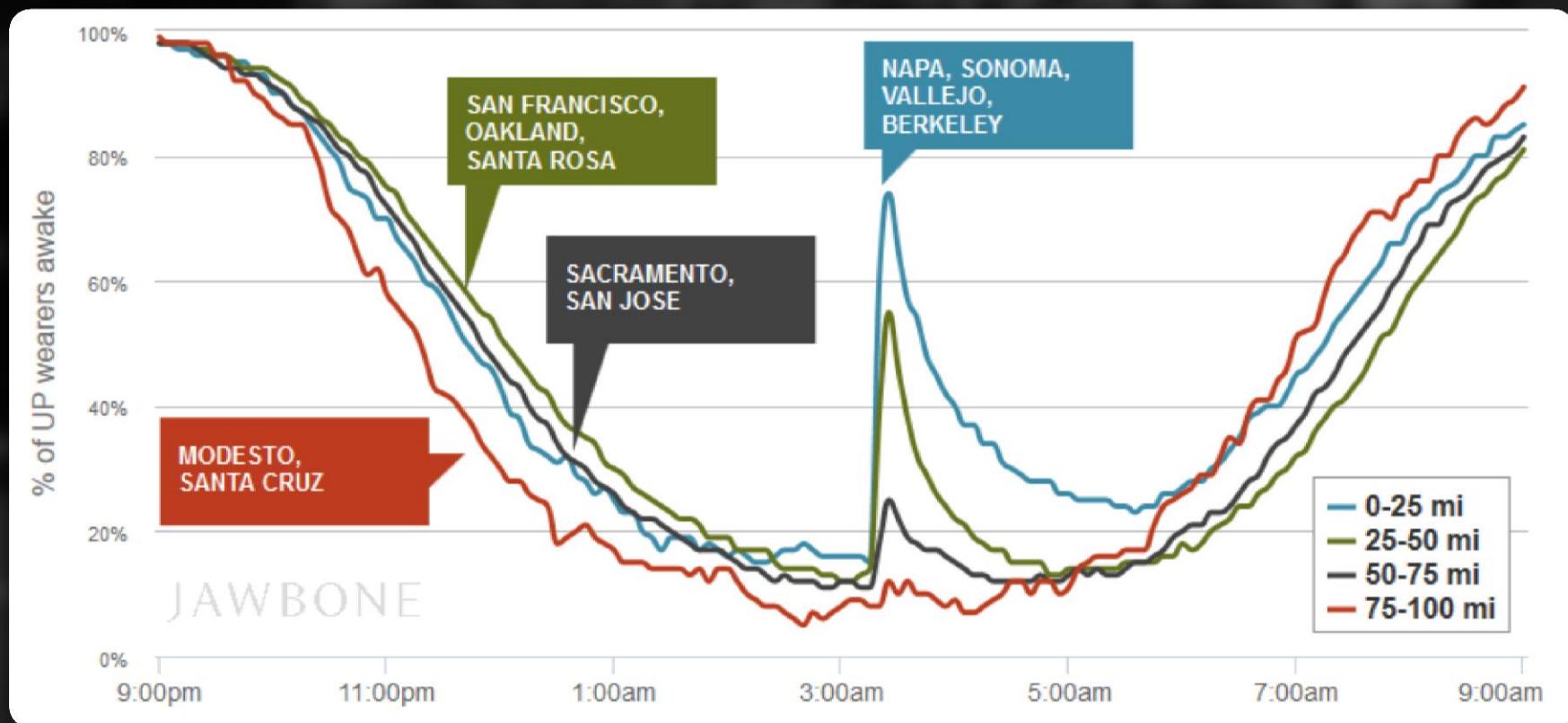
HealthKit



SAMI
Samsung Architecture Multimodal Interactions

YOUR DATA IS ALREADY ANALYSED

Jawbone: Who's asleep during San Francisco earthquake 2014?



DO YOU NEED AN ALIBI?

Fitbit used in court to show reduced activity levels



**Heyyy! NICE e-bracelet you've got there ...
SHAME if someone were to SUBPOENA it**

Court pops open cans of worms and whup-ass in Fitbit case

By Kieren McCarthy, 18 Nov 2014

20% SENT PASSWORD IN CLEAR TEXT

Larger proportion of the top 100 health apps leaked activity data through HTTP
Some apps accepted self-signed certificates or don't check revocation lists

POST http://api.*****.com/Mobile/Functions.ashx?action=RegisterUser

FName: ken
LName: west
GoalWeight: 68
Email: kenwest@this.tld
Password: P@SSw0rd
.....

GET http://*****.***/api/createUser?
username=KenWest
email=kenwest@this.tld
password=P@SSw0rd

POST http://*****.*****.net/cgi-bin/account

password: 8EEFB875DB938CEC08299BE7AA709EE0
action: create
email: kenwest@this.tld
preflang: de_CH
...

No need to crack
simply pass the hash

ENUMERATE USER DATA

HTTP GET /api/getUser/877

[No authentication needed]

```
{"result":true,"data":{"id":877,"name":"Kenwest","email":"ken@this.tld","password":"705bf40d40cb2904b04294fbc355XXXX","role":0,"about":null,"sex":Male,"age":null,"purpose":null,"coach_id":1,"heightfeet":null,"heightinch":null,"startweight":null,"_currentweight":null,"targetweight":null,"startbf":null,"currentbf":null,"targetbf":null,"systolic":null,"diastolic":null,"neck":null,"hips":null,"waist":null,"forearm":null,"wrist":null,"imageurl":null,"photo":null,"thumbnail_65":null,"thumbnail_150":null,"nike_user":null,"nike_pwd":null,"nikelink":null,"faceuid":null,"provider":null,"fitbit_join":0,"withings_token":null,"googleuid":null,"facebook_access_token":null,"facecache_last_update":null,"join":0,"first_run":0,"metric":0,"last_entry":null,"facecache":null,"last_update":null,"uid":d531c273a5a4273a8aa5aa200730axXX74aeef9cc446b80eb14391a6XXXX,"friendly":0,"follow":0,"currentweight":190,"sexnumber":1,"percent_to_lose":100,"percent_to_bf_loose":100,"totalbudget":1650,"systolic":null,"warning":bar bar-warning,"diastolic":null,"warning":bar bar-warning,"systolic":null,"diastolic":null,"warning":bar bar-warning,"startawayfrom":\Vimg\male\male_190,"avatar":\Vimg\male\male_190,"points":0,"avgminutes":44.0000,"avgweight":190,"sumweekcalories":Still working on weightloss,"level":Newbie,"xxxxscore":0.6039444444444444}}
```

Name
Email
Password
Birthday
Photo
Fitbit_token
Withings_token
Google_uid
Facebook_access_token

Ideal for spammers

Email, context and Social media accounts

OPEN REMAILER SCRIPT

POST http://www.***.com/members/community130204/sendmail.php
email: kenwest@this.tld
subject: Daily Activity
message: Dear User,
You have 1 new private message. Please go to ...

POST http://www.***.com/members/community130204/sendmail.php
email: kenwest@this.tld
subject: Your Daily Spam
message: Dear User,
You have 1 new SPAM message. Please click here...

POSSIBLE IMPACT

- **Account hijack**
 - The problem of password reuse
 - Costs: Sign the user up for premium services, commitments, ...
 - Change the privacy settings
- **Spam**
 - Enumerate user data to send spam with context
 - Create dummy accounts & use profile page as spam landing pages
 - Use social media accounts to find friends and spam them

GET REWARDED

Who said you have to run yourself? Dog-sitter?

Vitality points calculator

Through Vitality, we help you understand your health, and we suggest ways you can improve it.

Whenever you do certain healthy things we give you Vitality points. Your points count towards your Vitality status. Everyone starts at bronze, then you can work up to Silver, Gold then Platinum. The higher your Vitality status, the bigger the rewards!

Answer five simple questions to see what status you could achieve.

SINGLE

COUPLE / FAMILY

Get active

We give you points for being active. You can work out at one of our partner gyms or complete a parkrun. Alternatively, you can track your activity and earn Vitality points with Fitbug, Polar, Adidas miCoach, Nike+, Garmin and Fitbit devices. How many of these exercise sessions would you do each week?
(10 points per exercise session. Max 40 points per week.)

Person 1

- 0
- 1
- 2
- 3
- 4+



Get access to a range of health partners that help you get healthier and feel great.

Your predicted Vitality status

	Person 1
Education	200
Smoking	100
Screening	560
Get active	1,560
Eat well	-
	2,420
Total Vitality points	2,420

PLATINUM status

Savings calculator

See what savings you can get through Vitality as your status changes

POSSIBLE IMPACT

- **Loss of privacy**
 - Reveal personal details: Identity theft, profiling, extortion, ...
 - Reveal Location: Stalking, burglar, kidnapping, corporate misuse, ...
- **Loss of integrity**
 - Modify/inject data: Gain rewards, high scores, frustrate others ;-)
 - Delete the account and history
 - Brick/change the device through firmware updates

BLUETOOTH LOW ENERGY

aka Bluetooth SMART and BTLE part of BT 4.0 (2010)

- Different from classic Bluetooth
- Does frequency hopping but can still be sniffed
- Pairing has been broken (Mike Ryan)

”Bluetooth Smart (low energy) technology supports a feature that reduces the ability to track a Bluetooth device over a period of time by changing the address on a frequent basis.”

Bluetooth.org

SCANNING WITH A BLUEBERRY PI

TOTAL PRICE

\$75

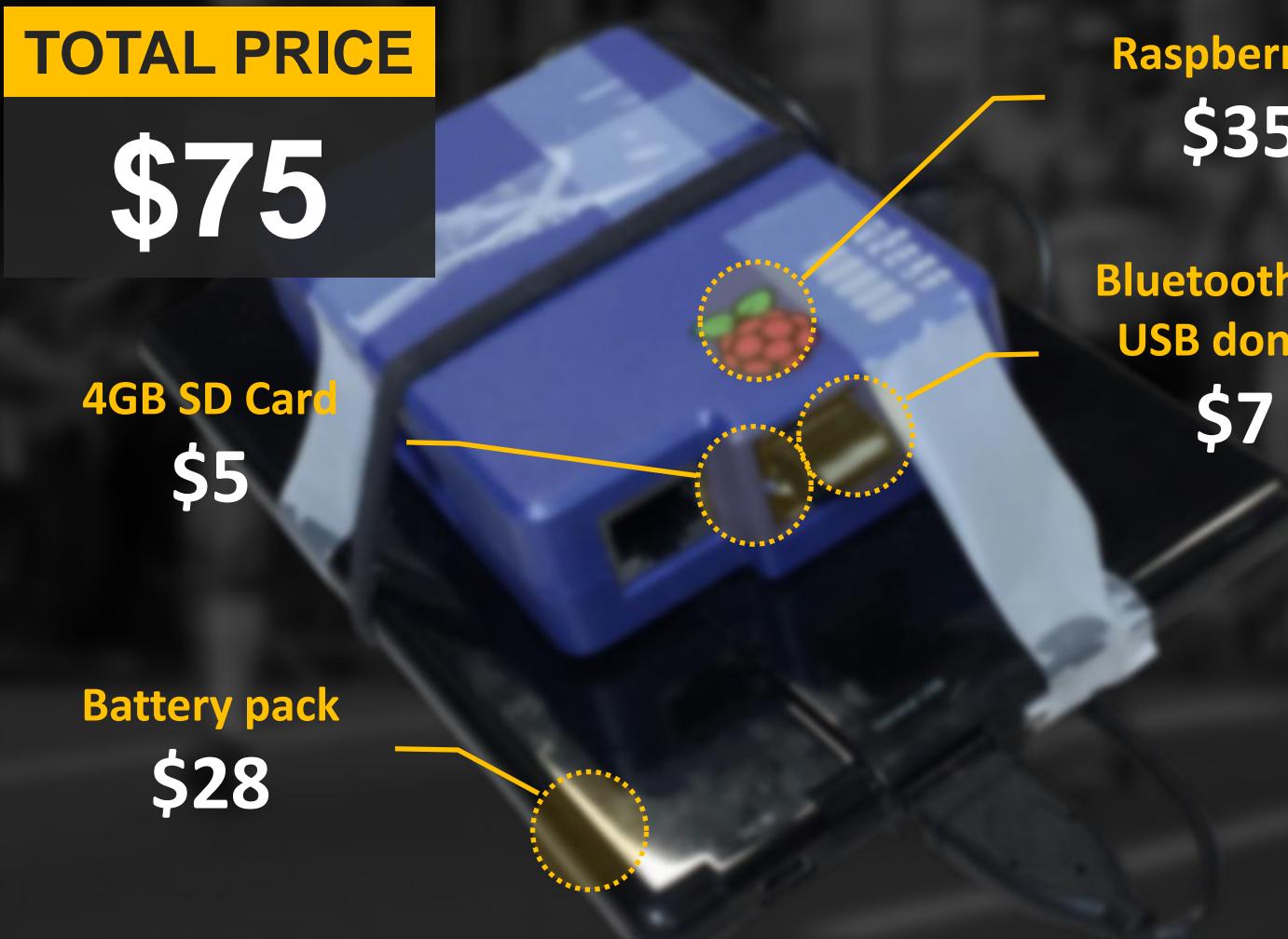
4GB SD Card
\$5

Battery pack
\$28

Raspberry pi

\$35

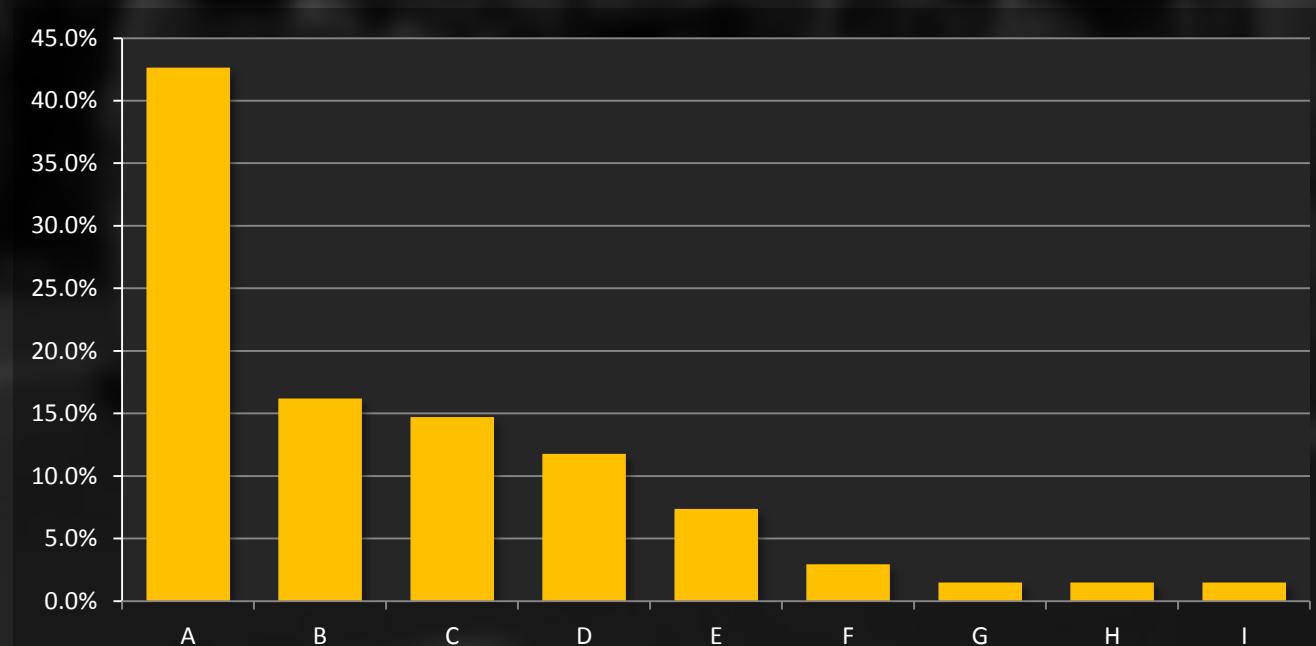
**Bluetooth 4.0
USB dongle**
\$7



OUR BLUETOOTH TRACKER

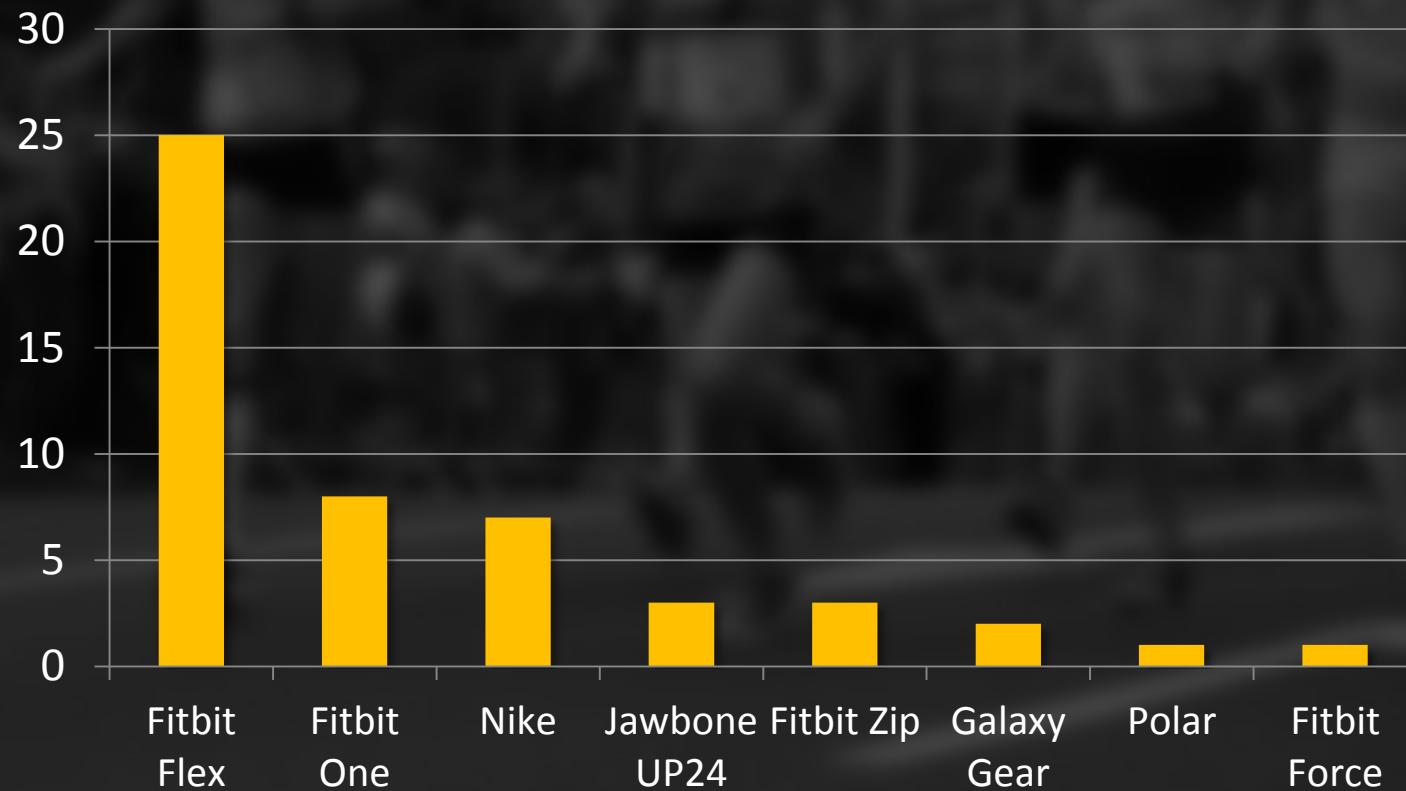
SCAN RESULTS FOR A MINI MARATHON

- The phone may reveal the real name associated with the device
- 30 from 563 devices had something like a person's name
 - Rita :)
 - Darren!
 - Franks phone
 - Erica
 - Dawson
 - Alieen's mobile!!:)
 - Garret rip xxx
 - Big hairy bollo



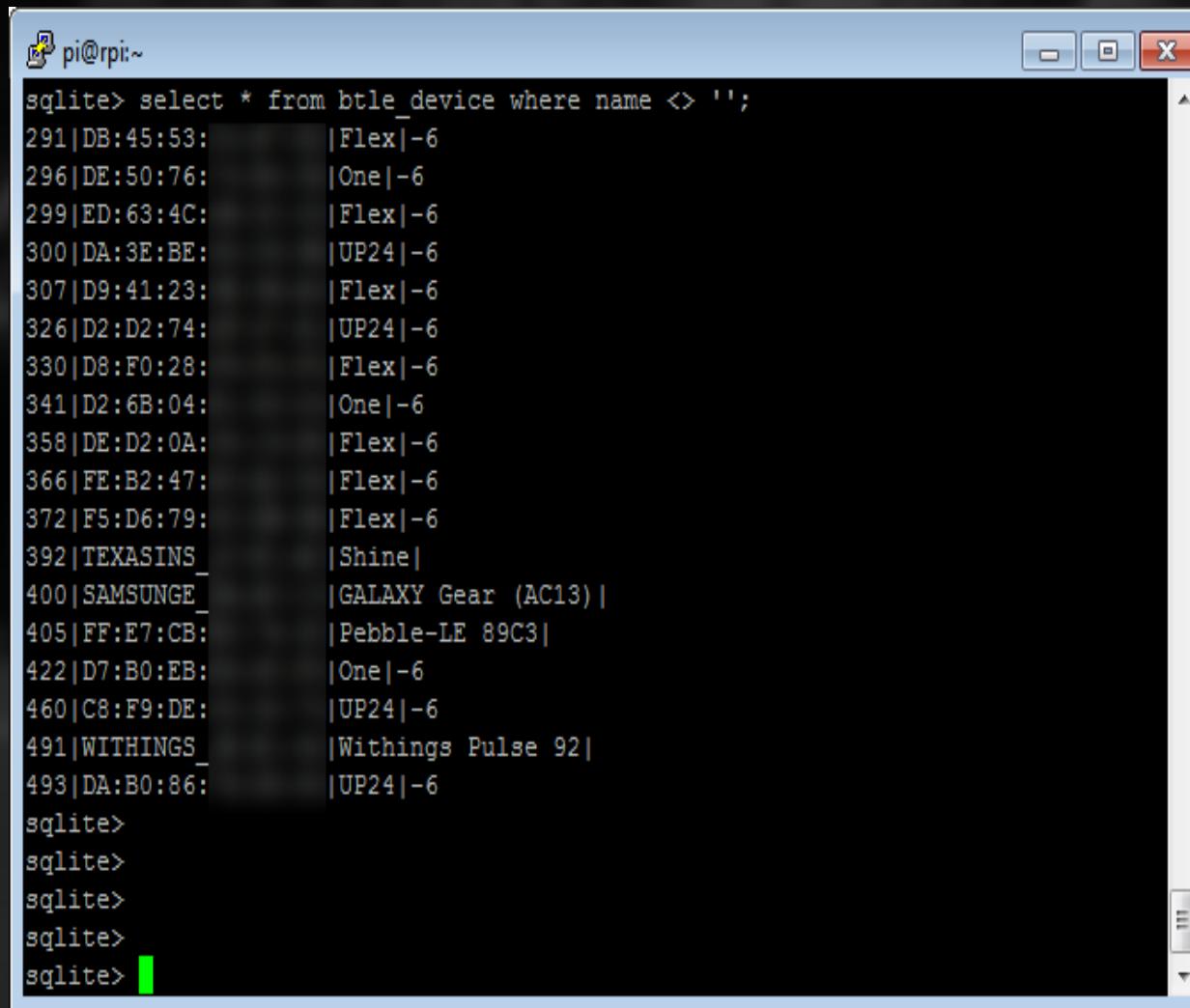
SCANNING AT VB CONFERENCE

- 50 devices at the Westin Hotel
- 29 seen till noon, not everyone made it to the breakfast ;-)



SCAN RESULTS FOR BLACKHAT EU/14

- 203 BTLE devices and 21 wearable fitness trackers seen

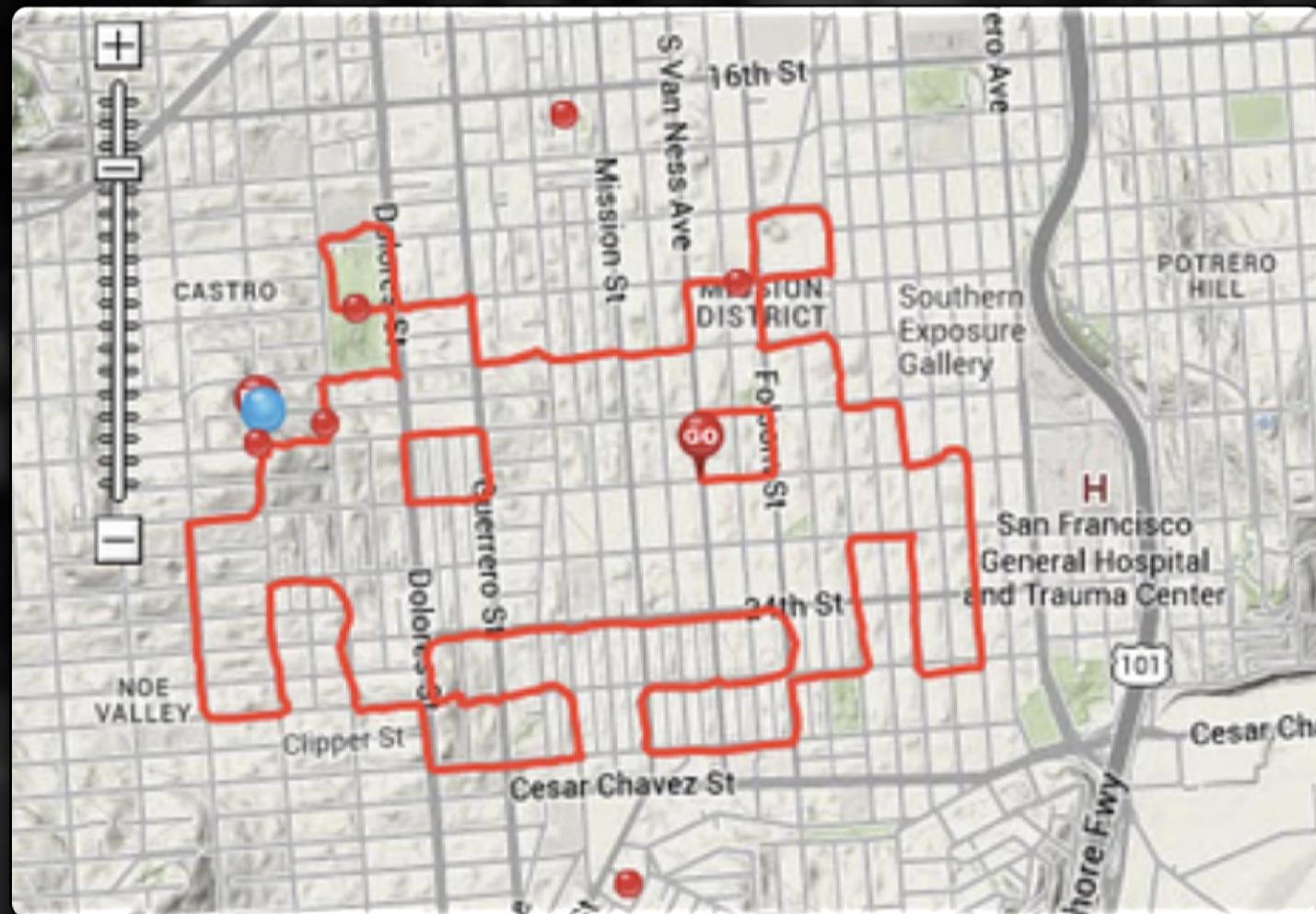


A screenshot of a terminal window titled "pi@rpi:~". The window displays the output of a SQLite command: "sqlite> select * from btle_device where name <> ''". The results are listed in a table format:

Address	Name
291 DB:45:53:	Flex -6
296 DE:50:76:	One -6
299 ED:63:4C:	Flex -6
300 DA:3E:BE:	UP24 -6
307 D9:41:23:	Flex -6
326 D2:D2:74:	UP24 -6
330 D8:F0:28:	Flex -6
341 D2:6B:04:	One -6
358 DE:D2:0A:	Flex -6
366 FE:B2:47:	Flex -6
372 F5:D6:79:	Flex -6
392 TEXASINS_	Shine
400 SAMSUNGE_	GALAXY Gear (AC13)
405 FF:E7:CB:	Pebble-LE 89C3
422 D7:B0:EB:	One -6
460 C8:F9:DE:	UP24 -6
491 WITHINGS_	Withings Pulse 92
493 DA:B0:86:	UP24 -6

The terminal prompt "sqlite>" appears at the bottom of the window multiple times, indicating the user has entered several commands.

SOME WANT THE DATA TO BE SEEN



Source: blog.everytrail.com

SELF-TRACKING CAN BE RISKY

Your digital footprint will be everywhere!



52%

Do not have a
privacy policy

20%

Login
credentials in
clear text

14

Domains
contacted by
apps

WHAT CAN USERS DO?

TURN OFF BLUETOOTH IF NOT REQUIRED

KEEP DEVICE/SOFTWARE/OS UPDATED

DON'T REUSE USERNAME/PASSWORDS

USE STRONG PASSWORDS

LOOK FOR A PRIVACY POLICY

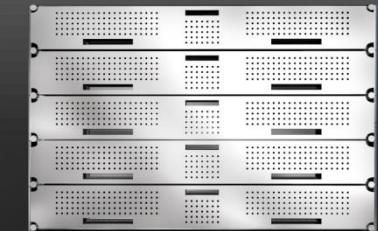
CHECK EXCESSIVE INFORMATION GATHERING

SCREEN LOCK

DEVICE ENCRYPTION

SECURITY SOFTWARE

I Am The Cavalry



WHICH QUESTIONS ARE STILL OPEN ?

MAY THE
MASS TIMES
ACCELERATION
BE WITH
YOU

THANK YOU!

BLOG

<http://bit.ly/1pgGefW>

WHITEPAPER

<http://bit.ly/1nGB4vw>

TWITTER

@threatintel

WEB

<http://www.symantec.com>