HOW SAFE IS YOUR QUANTIFIED SELF?

ATTACK POINTS IN HEALTH APPS & WEARABLE DEVICES

Candid Wüest

SECURITY RESPONSE

Symantec.

WHAT IS QUANTIFIED SELF?

Intersection of major consumer & IT trends

Sports & Recreation

Internet Of Things

Wearable Tech

QUANTIFIED SELF

Health

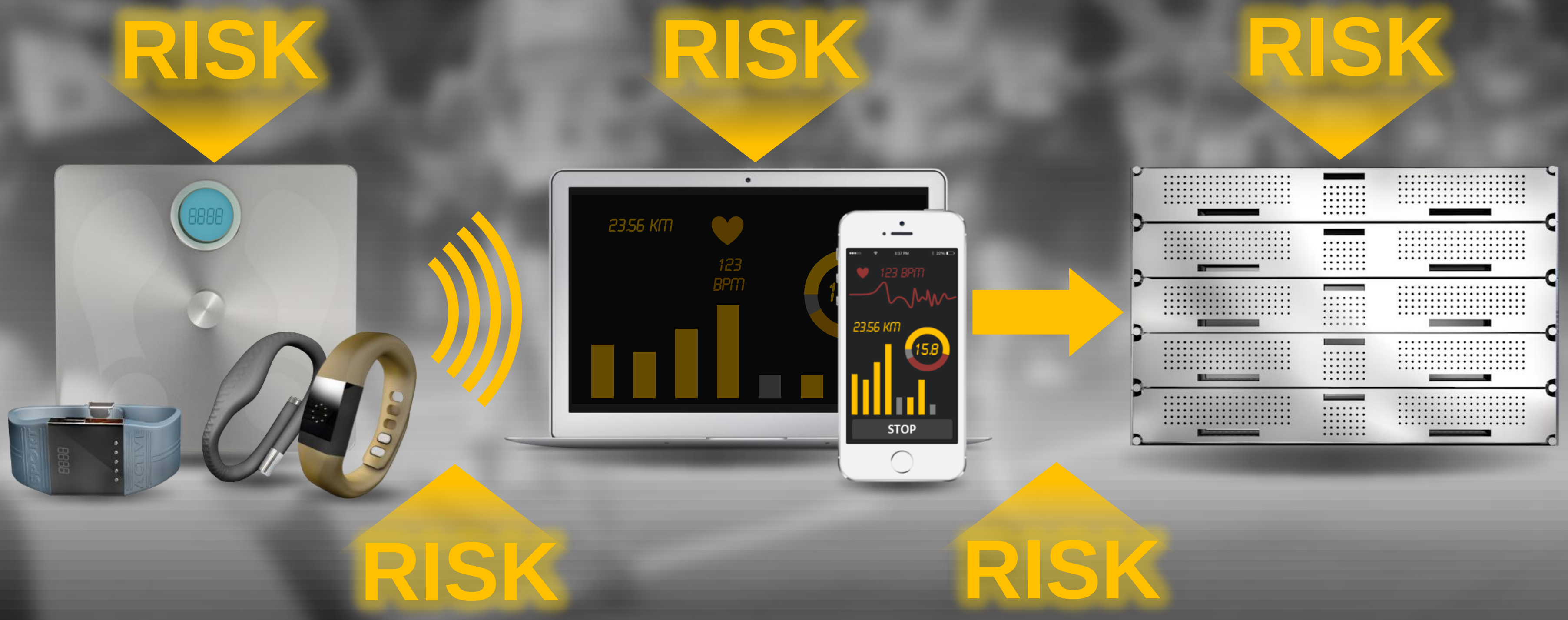
Business

Culture

Recording everything about your life

WHERE THE BITS FIT IN

More moving parts = more risks



RISK

RISK

RISK

RISK

RISK

DATA "CUSTODIANS"

It is personal identifiable information, but not as we know it

"Apps that access HealthKit are required to have a privacy policy,…"

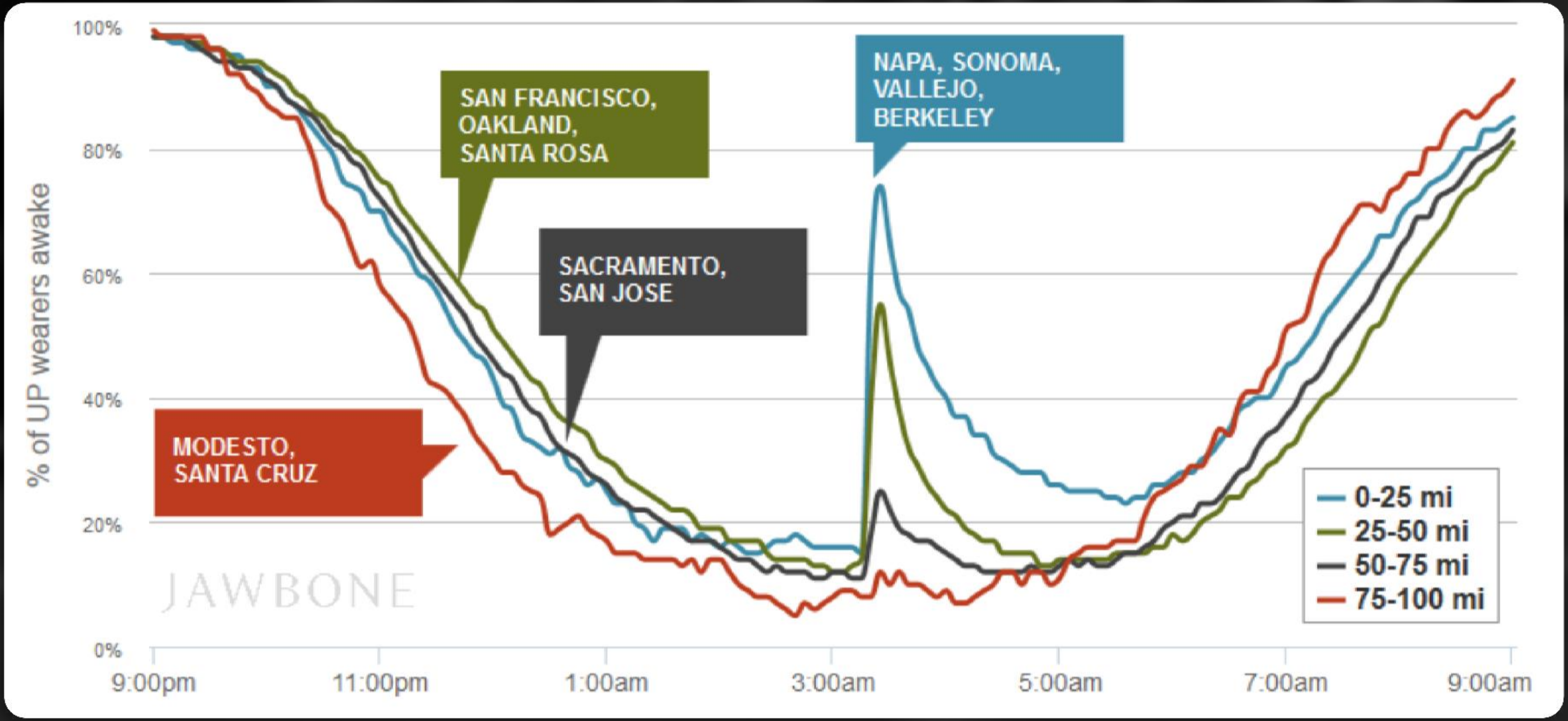
Apple.com

From the analyzed apps

52% had no privacy policy

YOUR DATA IS ALREADY BEING ANALYSED

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



UNINTENTIONAL DATA LEAKS

The secret life of mobile apps...

MAX DOMAINS CONTACTED

14

AVG DOMAINS CONTACTED

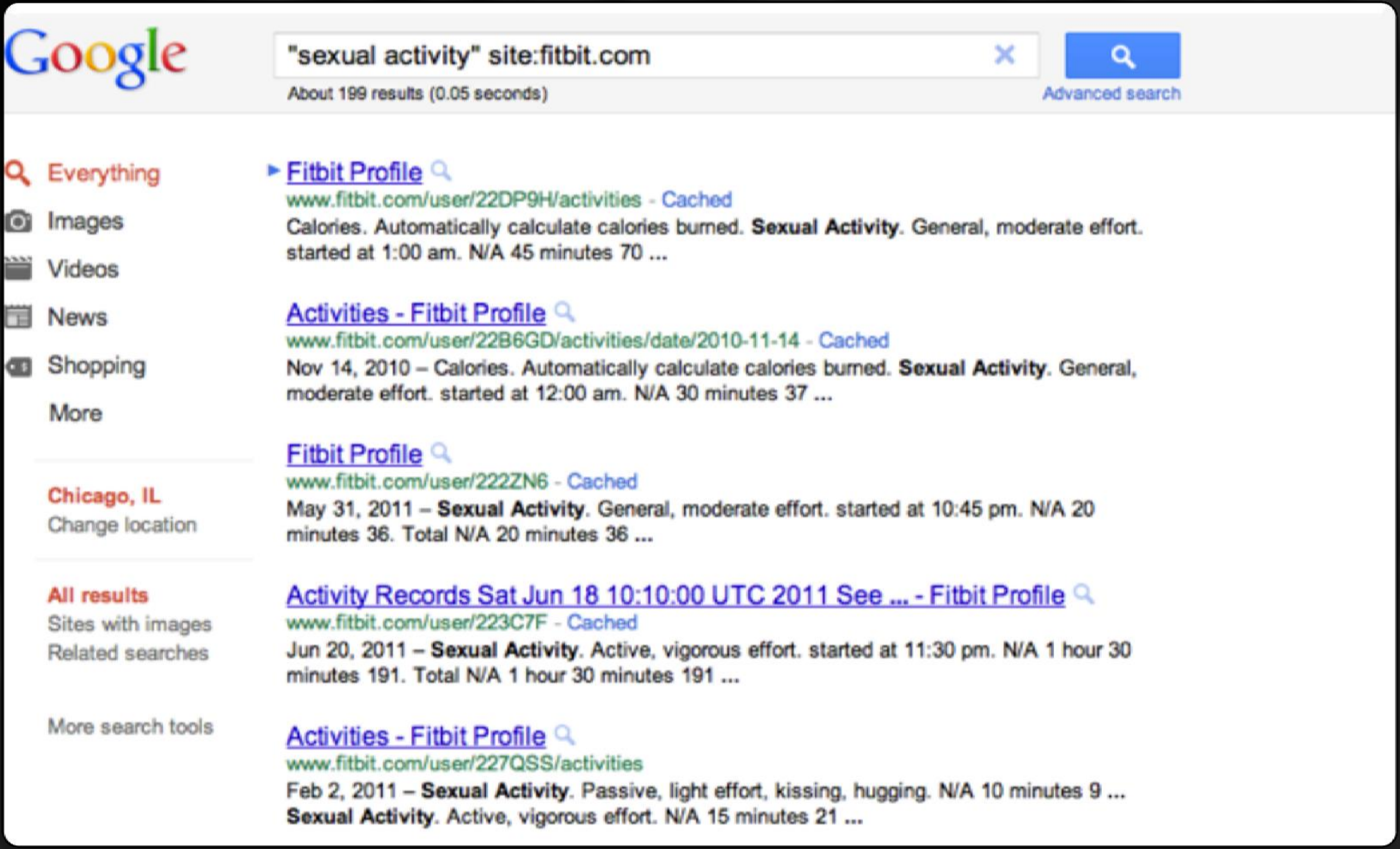
5

- APP ANALYTICS
- AD NETWORKS
- APP PROVIDER
- OS PROVIDER
- SOCIAL MEDIA
- APP FRAMEWORKS
- CRM/MARKETING
- UTILITY API

Symantec.

VERIFY THE DEFAULT SETTINGS!

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



About 199 results (0.05 seconds)

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 ...

Symantec.

20% SENT PASSWORDS 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 FOR SPAMMERS

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,"s
alt":"XgDLkaenP1","sex":"Male","age":null,"purpose":null,"coach_id":"1","heig
htfeet":null,"birthday":null,"heightinch":null,"startweight":null,"_currentweigh
t":null,"_targetweight":null,"_startbf":null,"_currentbf":null,"_targetbf":null,"_s
ystolic":null,"_diastolic":null,"neck":null,"_hips":null,"_waist":null,"forearm":n
ull,"wrist":null,"imageurl":null,"photo":null,"thumbnail_65":null,"thumbnail_1
50":null,"nike_user":null,"nike_pwd":null,"nike_join":"0","face_uid":null,"provi
der":"0","timezone":"America\/Los_Angeles","fitbit_token":null,"fitbit_secret"
:null,"fitbit_join":"0","withings_token":null,"withings_secret":null,"withings_us
erid":"0","withings_join":"0","google_uid":null,"google_join":"0",
"facebook_access_token":null,"face_join":"0","first_run":"0","metric":"0","last
_entry":null,"face_cache_last_update":null,"uuid":"d531e2973d5ad4276a8aa5
aaae0730aXXXX74aeefd9cc446b80eb14391a6XXXX","friendly":0,"follow":0,"cu
rrentweight":"190","sexnumber":"1","percent_to_lose":100,"percent_to_bf_lo
se":100,"totalbudget":1650,"systolic_warning":"bar bar-warning",
"diastolic_warning":"bar bar-warning","systolic":null,"diastolic":null,
"startavatar":"\/img\/male\/male_190","avatar":"\/img\/male\/male_190","p
oints":0,"avgcalories":"208.71263885498047","avgminutes":"44.0000","avgwe
ight":"190","sumweekcalories":"Still working on weight
loss","level":"Newbie",“xxxxscore":0.60394444444444}}
```

Name

Email

Password

Birthday

Photo

Fitbit_token

Withings_token

Google_uid

Facebook_access_token

Ideal for spammers

Email, context and

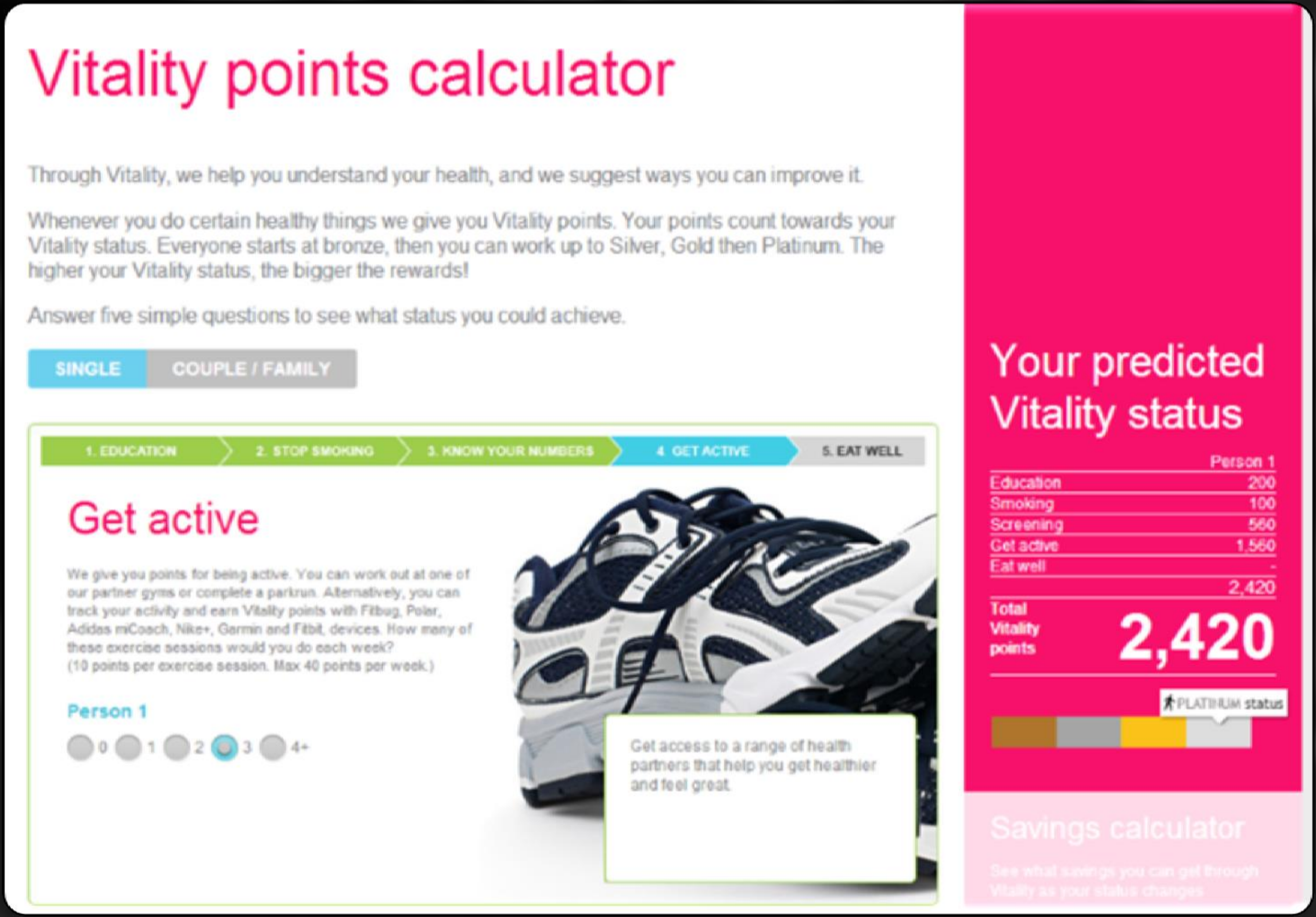
Social media accounts

POSSIBLE IMPACT

- Account hijack
  - Costs: Sign the user up for premium services, commitments, …
  - The problem of password reuse
- 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 other people ;-)
  - Delete the account and history
- Spam
  - Enumerate user data to send spam with context
  - Create dummy accounts & use profile page as spam landing pages

GET REWARDED

Who said you have to run yourself?



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.

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

Savings calculator

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

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)

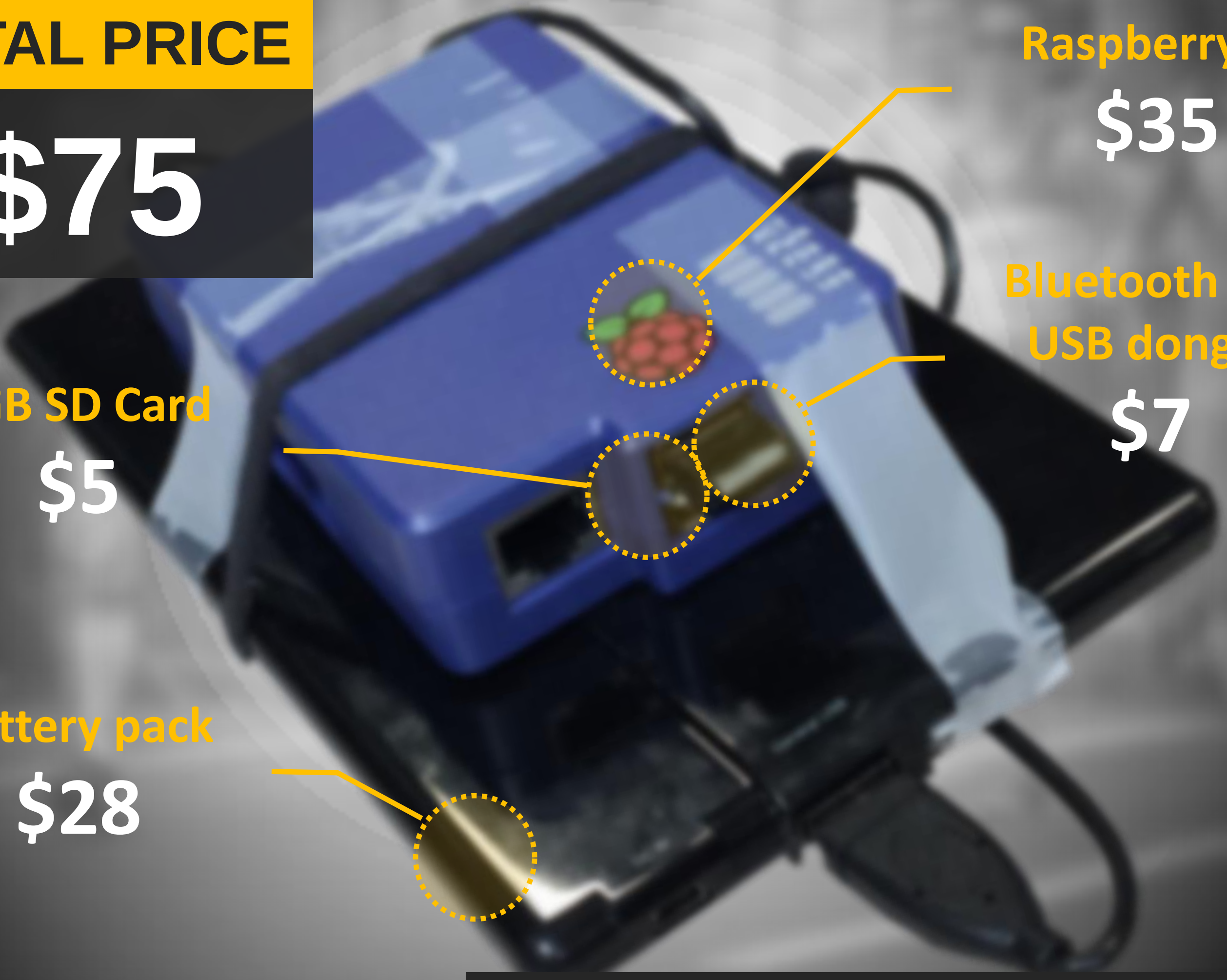
”Bluetooth Smart (low energy) technology supports a feature that reduces the ability to track a Bluetooth device over a period of time by changing the address on a frequent basis.”

Bluetooth.org

SCANNING WITH A BLUEBERRY PI!

TOTAL PRICE

$75



Raspberry pi

$35

Bluetooth 4.0 USB dongle

$7

4GB SD Card

$5

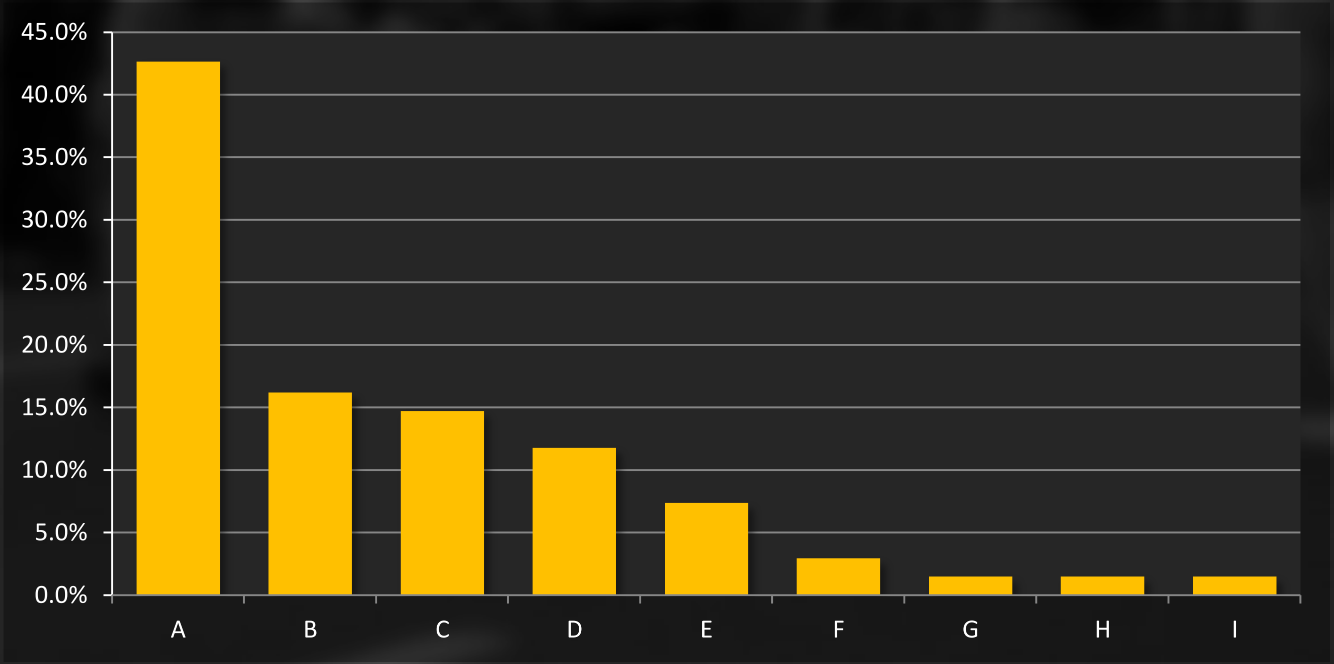
Battery pack

$28

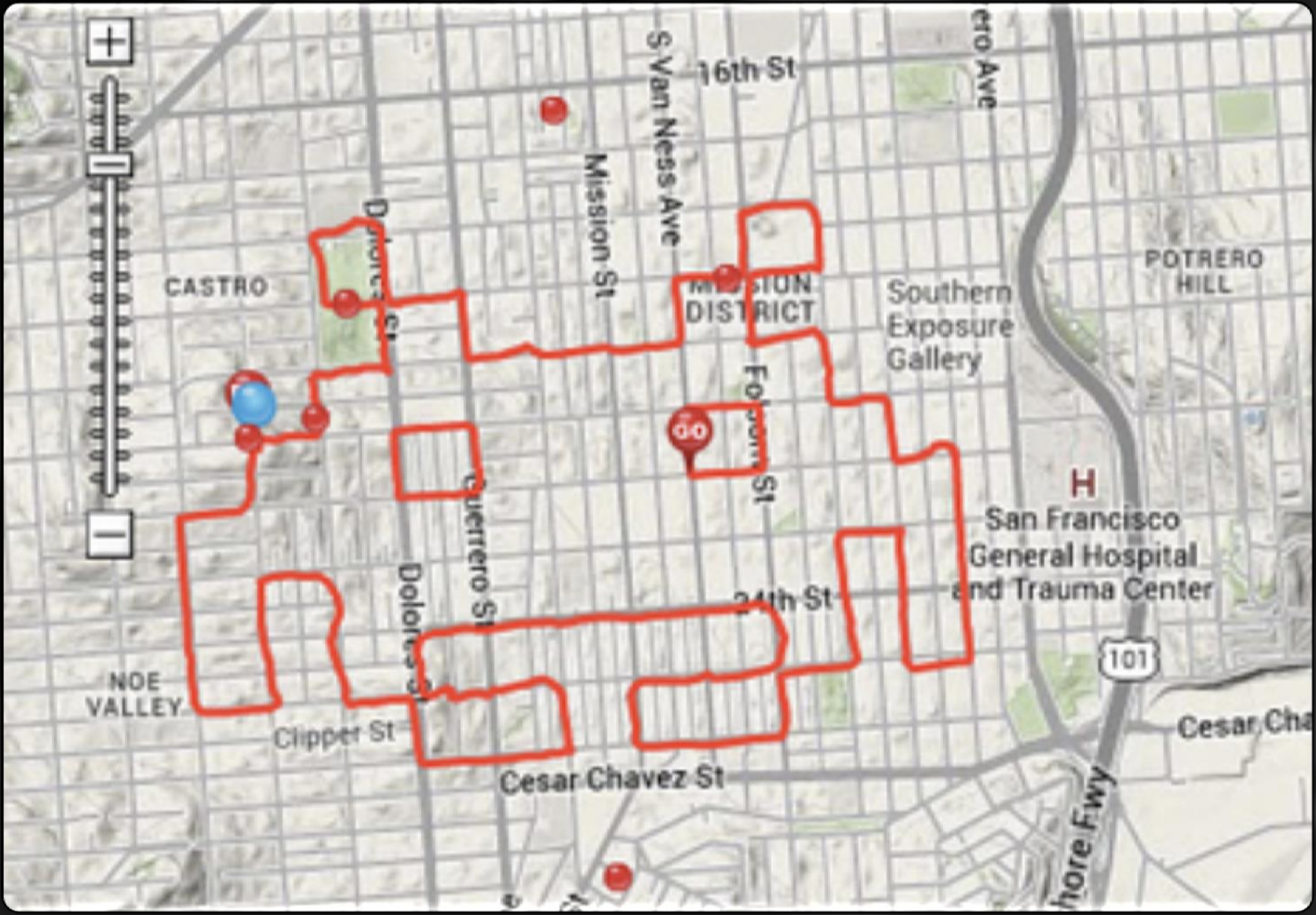
OUR BLUETOOTH TRACKER

SCAN RESULTS FOR 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



SOME WANT THE DATA TO BE SEEN



Source: blog.everytrail.com

Symantec.

SELF-TRACKING CAN BE RISKY FOR USERS

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

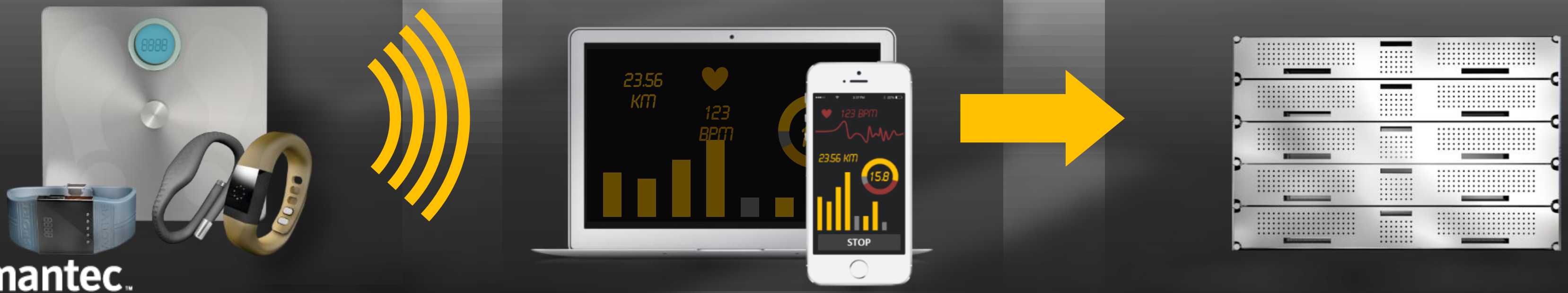
EXCESSIVE INFORMATION GATHERING

SCREEN LOCK

DEVICE ENCRYPTION

SECURITY SOFTWARE

I Am The Cavalry



Symantec.

QUESTIONS?

BLOG	http://bit.ly/1pgGefW
WHITEPAPER	http://bit.ly/1nGB4vw
TWITTER	@threatintel
WEB	http://www.symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec.

THANK YOU!

BLOG	http://bit.ly/1pgGefW
WHITEPAPER	http://bit.ly/1nGB4vw
TWITTER	@threatintel
WEB	http://www.symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec.