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

Sports & Recreation

Internet Of Things

Wearable Tech

QUANTIFIED SELF

Health

Business

Culture

What if there were no hypothetical questions?

WHERE THE BITS FIT IN

More moving parts = more risks

press space twice to save or once to cancel

UNINTENTIONAL DATA LEAKS

The secret life of mobile apps...

MAX DOMAINS CONTACTED

14

AVG DOMAINS CONTACTED

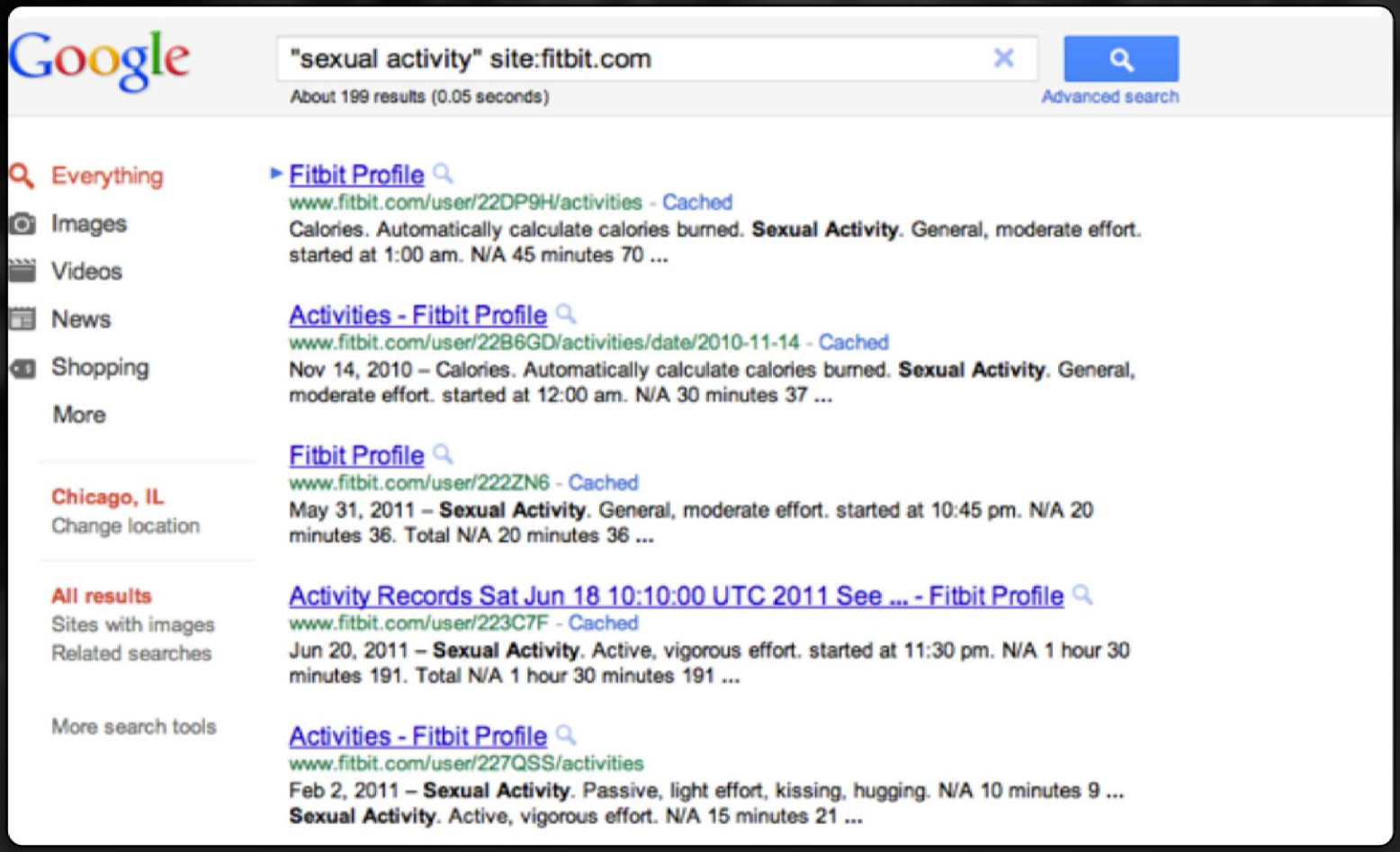
5

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

A clear conscience is usually the sign of a bad memory.

VERIFY THE DEFAULT SETTINGS!

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



I don't suffer from insanity. I enjoy every minute of it.

DATA "CUSTODIANS"

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

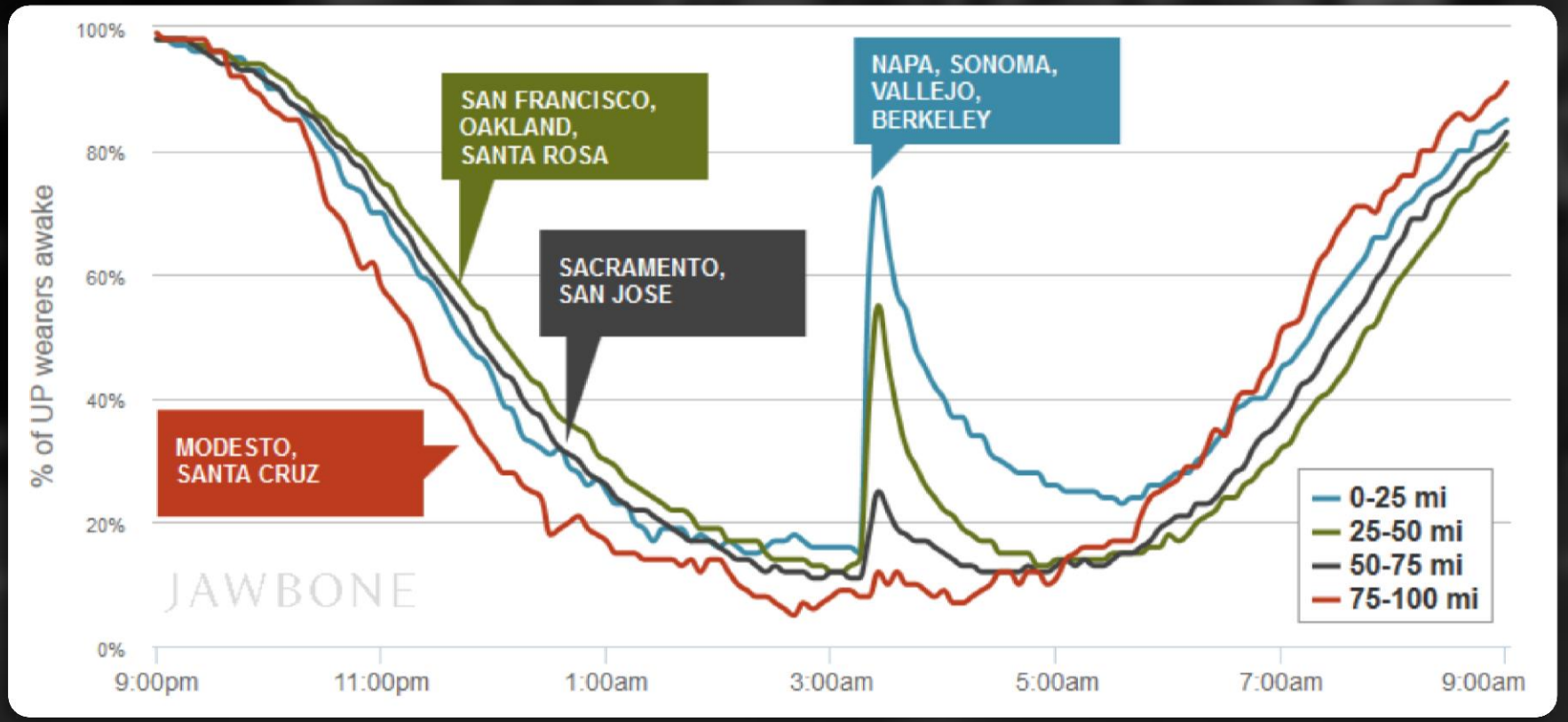
"Apps that access HealthKit are required to have a privacy policy,…"
Apple.com

From the analyzed apps

52% had no privacy policy

YOUR DATA IS ALREADY ANALYSED

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



All generalizations are false.

DO YOU NEED AN ALIBI?

Fitbit used in court to show reduced activity levels

I would love to change the world, but they won't give me the source code.

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

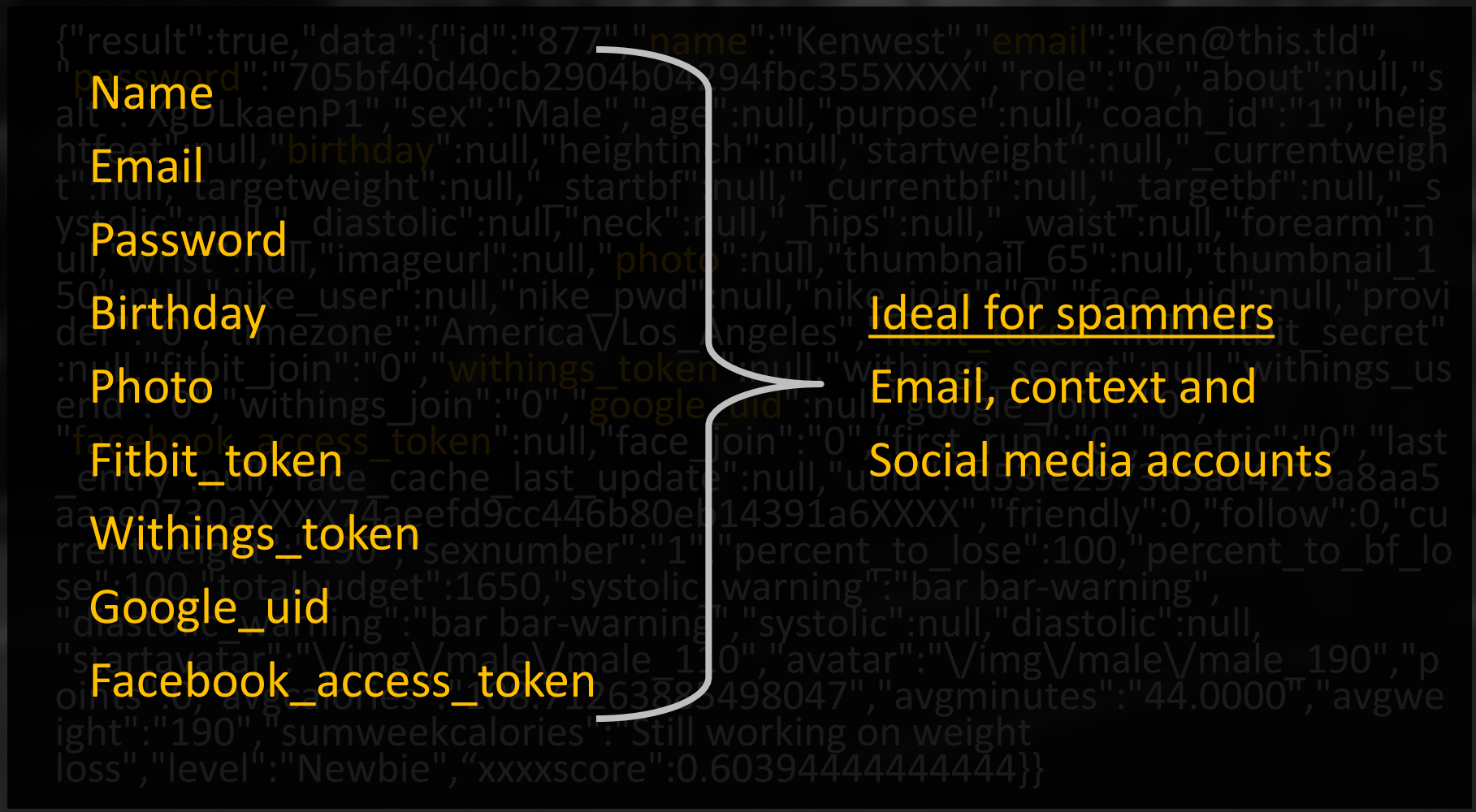
POST http://******.*******.net/cgi-bin/account

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]



If I agreed with you we'd both be wrong

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…

If brute force doesn't solve your problems, then you aren't using enough.

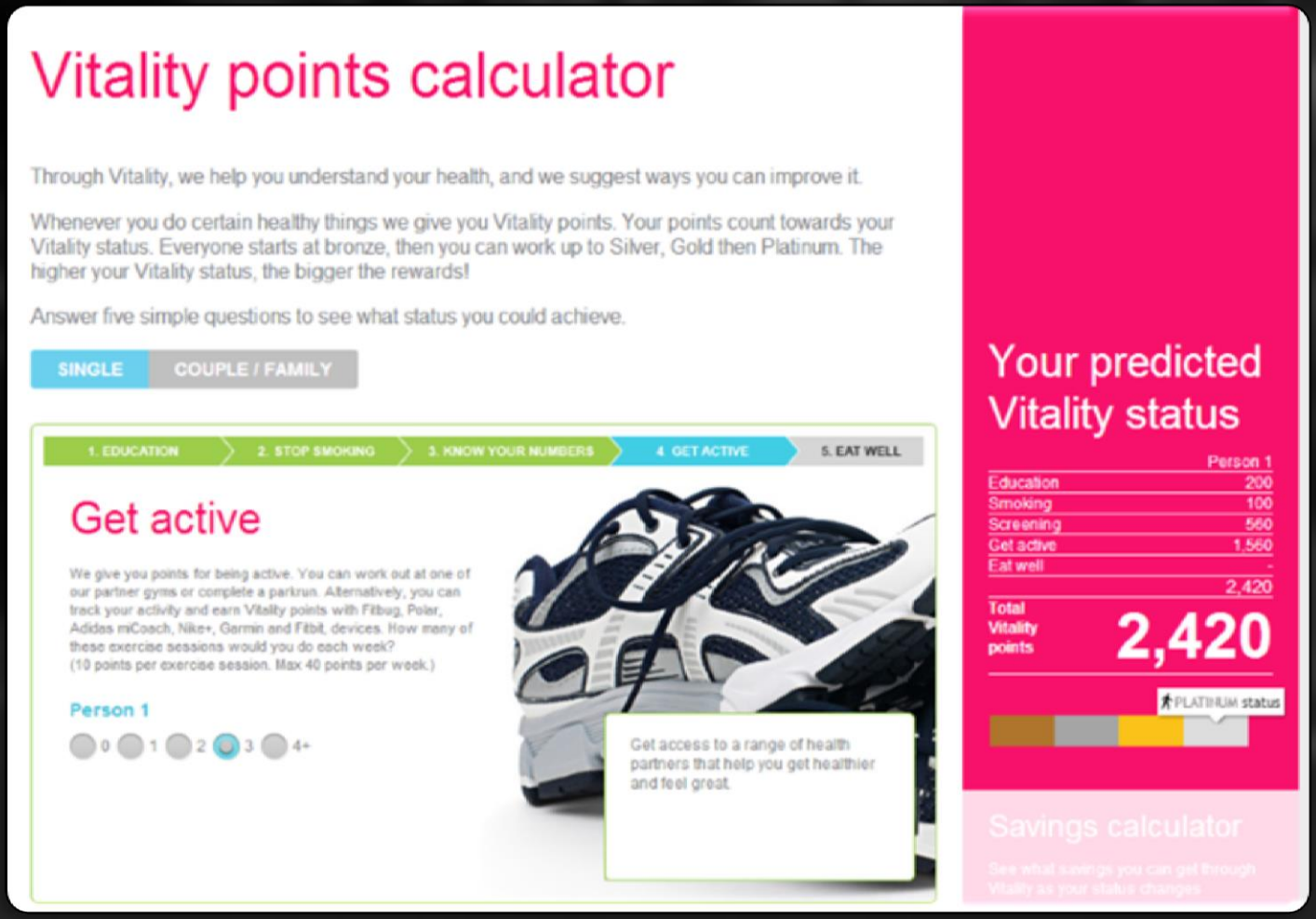
POSSIBLE IMPACT

- **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 socal media accounts to find friends and spam them

My software never has bugs. It just develops random features.

GET REWARDED

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



It’s true hard work never killed anybody, but I figure, why take the chance?

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

As far as we know, our computer has never had an undetected error

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

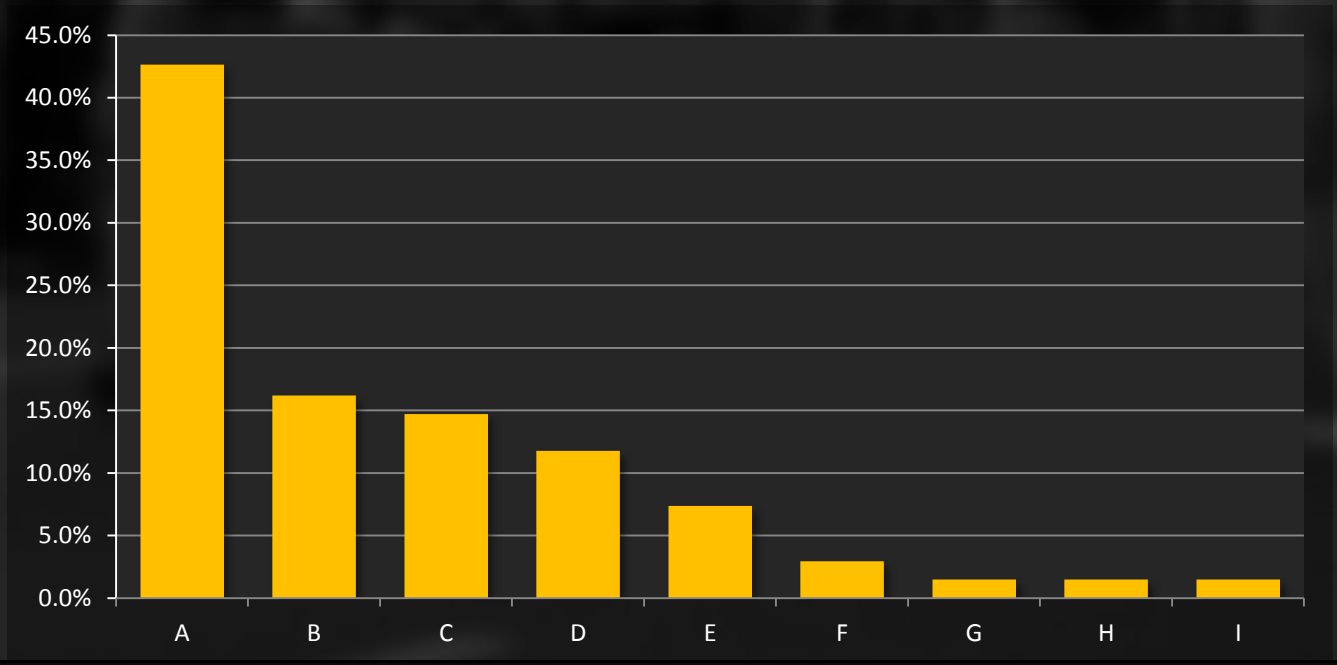
$75

OUR BLUETOOTH TRACKER

Enter any 11-digit prime number to continue.

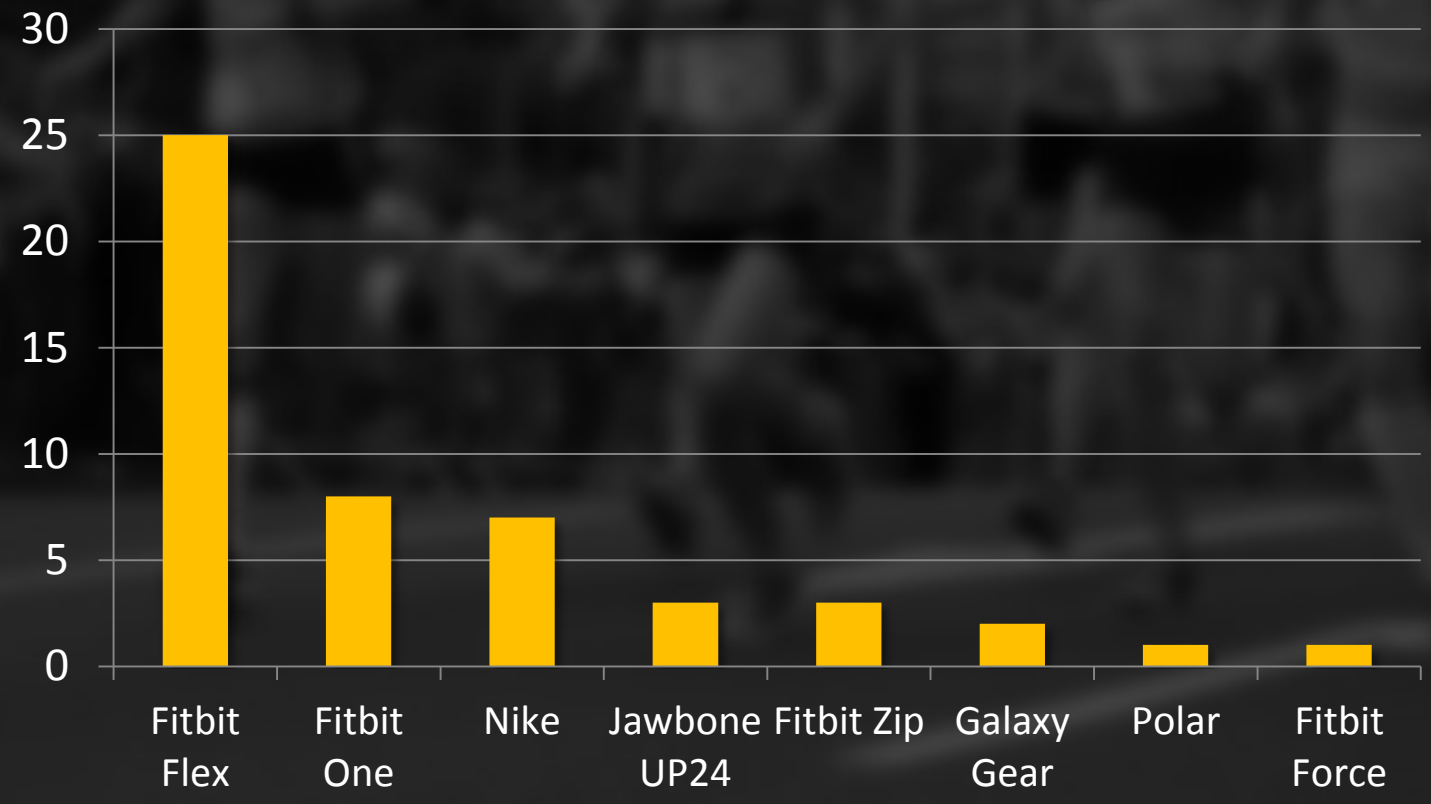
SCAN RESULTS FOR A MINI MARATHON

- 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

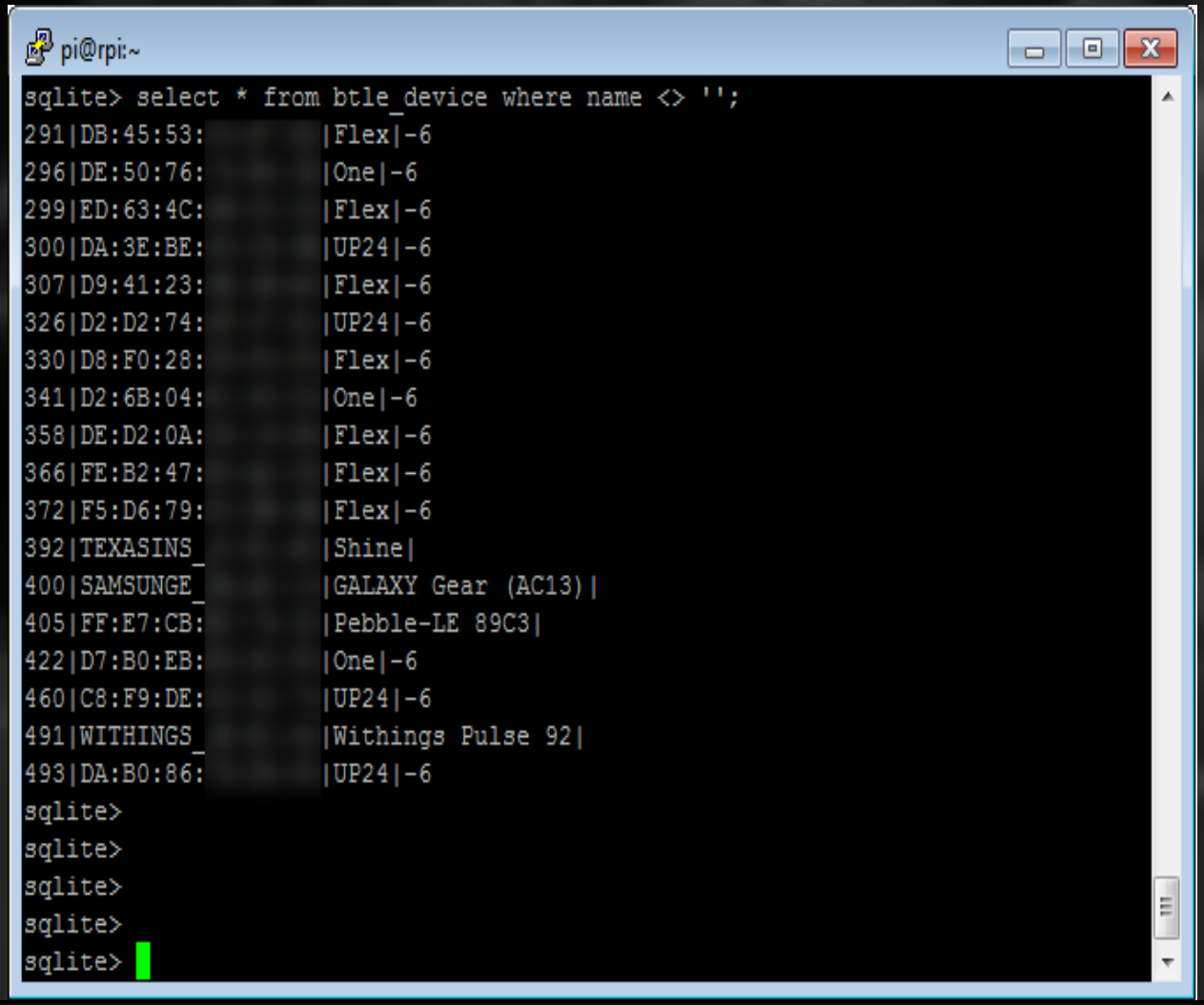
- 50 devices at the Westin Hotel
- 29 seen till noon, not everyone made it to the breakfast ;-)



I didn't say it was your fault, I said I was blaming you.

SCAN RESULTS FOR BLACKHAT EU/14

- 203 BTLE devices and 21 wearable fitness trackers seen



TTL jokes are short lived

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

An error? Impossible! My modem is error correcting

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 ?

THANK YOU!

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

Symantec