



Internet of Behavior

Gabriele Zanoni

Who's who
Gabriele Zanoni
@infoshaker

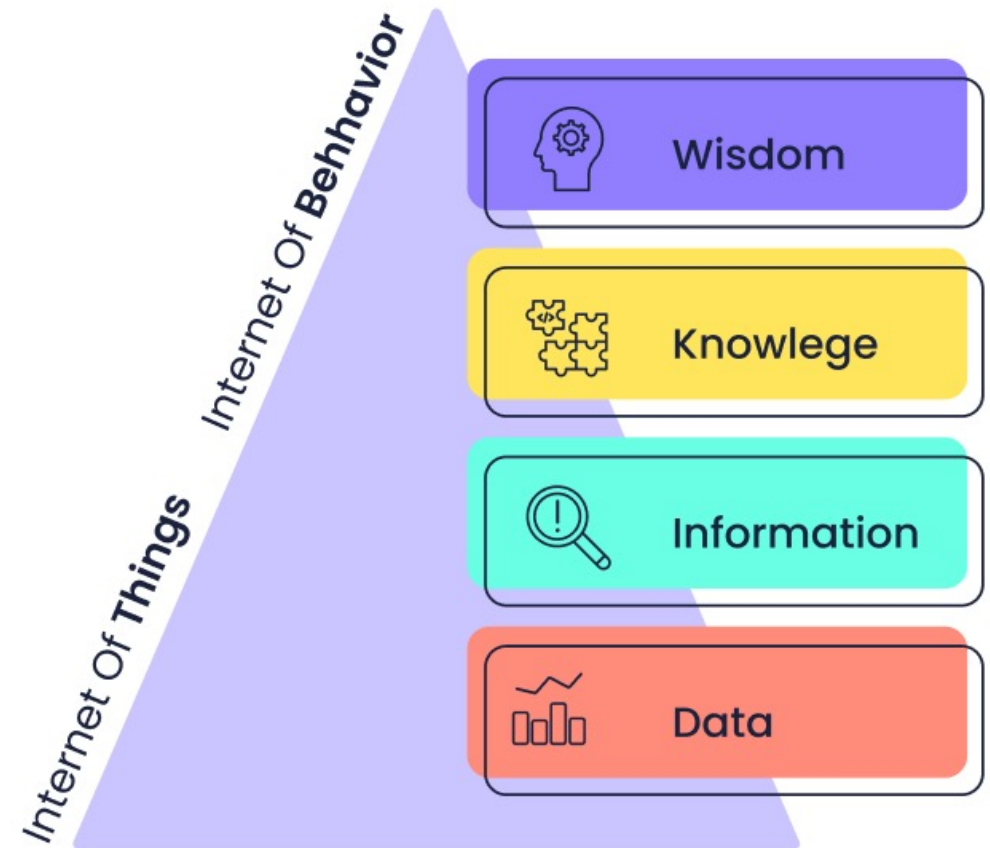
- Strategic Consultant
- Cloud Security
- Penetration testing
- Incident Response
- Anti-Fraud
- Computer Forensics
- Mobile Security

IoB #1

“The idea behind IoB is to offer individuals and/or communities a new means to indicate selected and meaningful behavior patterns by assigning a specific IoB address (analogous to the internet of things) to each behavior.”

“When this assignment has been done, automatically or by individuals themselves or by external observers or by learning systems, then it is possible to access these individuals engaged with these specific behaviors, to connect with their gear then, or to provide their environment information about their behaviors – if they allow it”.

Göte Sture Nyman
University of Helsinki



IoB #2

“By 2023, individual activities will be tracked digitally by an “Internet of Behavior” to influence benefit and service eligibility for 40% of people worldwide.”

Gartner

Examples of data tracked by IoT devices or Apps

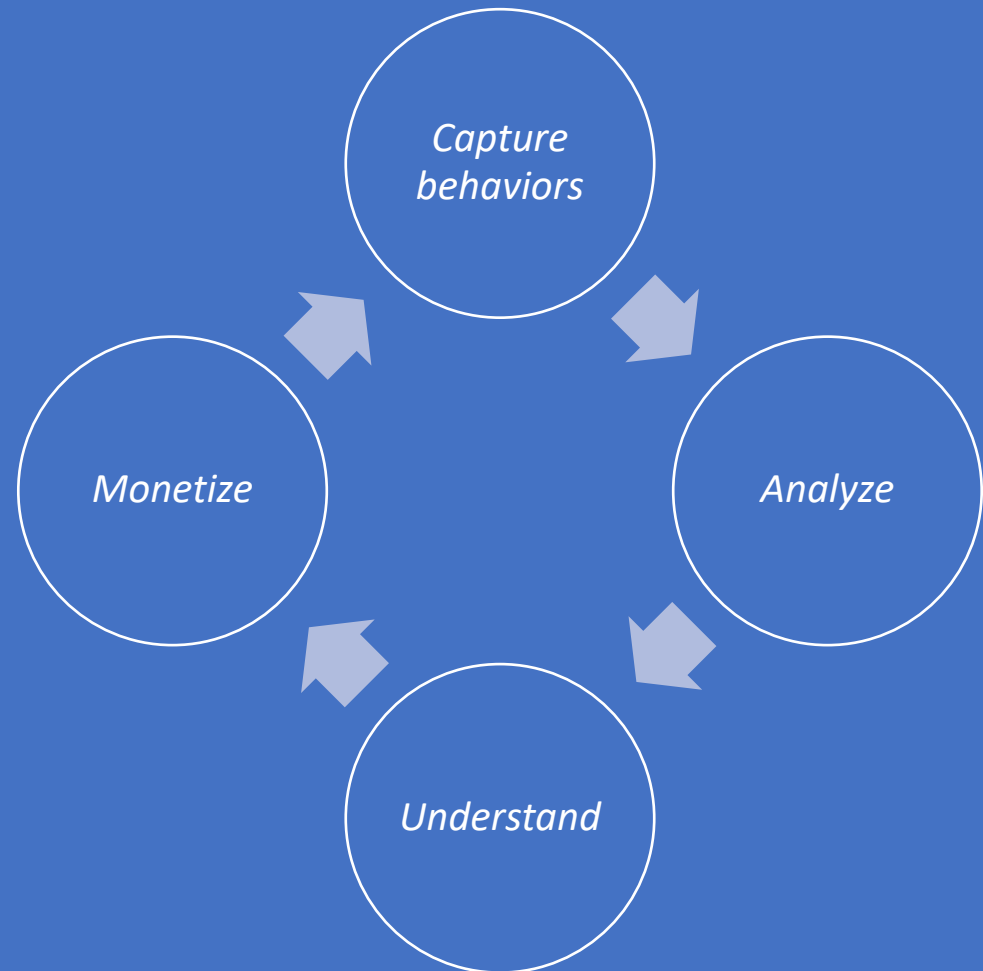
- Geo positions
- Info from your accelerometer
- Is your smart lamp/TV etc.. on?
- History of calls
- Your face, fingerprint etc..
- Wellness data (if you sleep well, if you are sporty)
- People or device near to you
- How you type
- How good/often you wash your hands
- Types of sound
- etc..

Set up Handwashing on Apple Watch

Your Apple Watch can detect when you start washing and encourage you to keep going for 20 seconds, the time recommended by global health organizations. Your Apple Watch can also notify you if you haven't washed your hands within a few minutes of returning home.

Benefits of IoB from data handler perspective

- Analyze customer's habits or needs (e.g. buying)
- Interactions users-device
- "Predictive analytics" in business, healthcare etc...
- Individual approach to each user
- Provide real time targeted ADS
- etc..



How such data can be (mis)used? 1/2

- Geo positions
 - for sending you a rocket or a SWAT team? [0]
 - check your compliance with health protocols (e.g. COVID)
 - check if you are part of a protest [1] (and the topic you support)
 - time spent watching a shop
- Info from your accelerometer
 - know the exact metro station where you are [2]
 - send you a spam email exactly when you have the phone in your hands
- Is your smart lamp/TV etc.. on?
 - check if you are at home or not
 - what time did you eat last night?
 - are you working from home?
- History of calls
 - so you called doctor? a subject matter expert in XYZ? [3]
 - who's your BFF?

[0] <https://ibrabo.wordpress.com/2014/12/30/new-zealand-jihadist-deletes-tweets-after-discovering-he-left-geotagging-on/>

[1] <https://www.npr.org/sections/alltechconsidered/2014/02/28/284131881/as-police-monitor-social-media-legal-lines-become-blurred?t=1559804031972>

[2] http://www.theregister.co.uk/2015/05/26/tracking_metro_riders_using_accelerometers_on_smartphones/?mt=1462545176702

[3] <http://webpolicy.org/2014/03/12/metaphone-the-sensivity-of-telephone-metadata/>

How such data can be (mis)used? 2/2

- Your face, fingerprint etc..
 - do you really need an example? [4]
 - illness
 - are you wearing a mask?
 - take a coffee [5]
 - targeting specific demographics
- Wellness data (if you sleep well, if you are sporty)
 - do you need a loan?
 - are you ill?
 - life-affecting reduced activity post injury [6]
- People or devices near you
 - I'm pretty sure you know some examples here
- How you type
 - how you type can be used to identify you [7]
- Types of sound
 - ShotSpotter [8]



Court sets legal precedent with evidence from Fitbit health tracker

Activity data from a fitness tracker will be used as evidence in a personal injury lawsuit for the first time



[4] <https://arstechnica.com/tech-policy/2014/06/first-chicago-robber-caught-via-facial-recognition-gets-22-years/>

[5] <https://www.dailymail.co.uk/news/article-5236957/Facial-recognition-tells-barista-coffee-order.html>

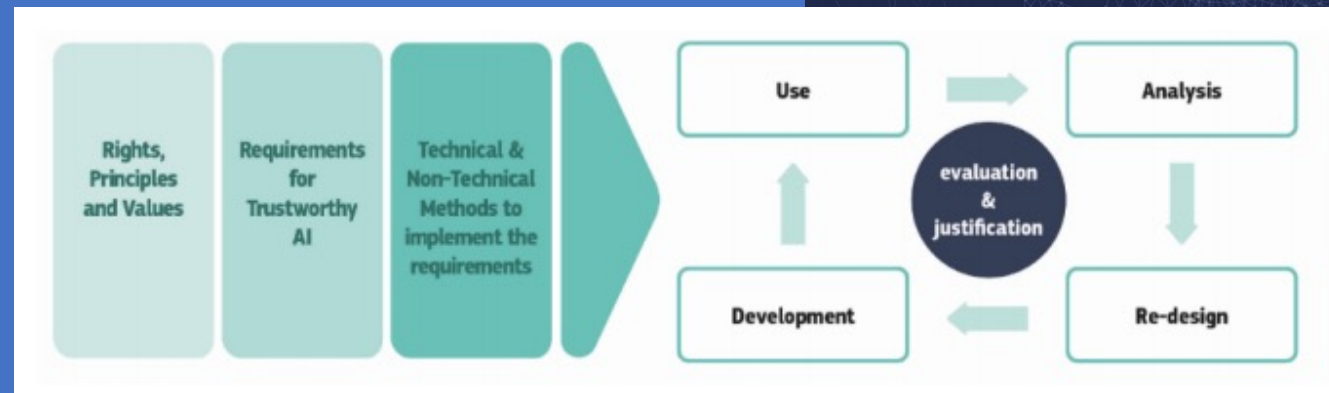
[6] <https://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker>

[7] How the way you type can shatter anonymity—even on Tor

[8] <https://www.techrepublic.com/article/gunshot-detection-technology-as-part-of-smart-city-design/>

Ethics of algorithms/AI, data usage and companies

- Concern about the creation of big data
- Controlling the data collection and the data access is hard in the digital world
- Ensuring the purposes have been agreed: the use of information to manipulate behaviour is not always good (e.g. exploitation of behavioural biases, addiction generation etc..) [1] [2]
- Algorithm transparency, auditing etc.. [2]
- Interconnecting our data with our decision-making, demands change at different levels (e.g. “significant concerns about lack of due process, accountability, community engagement, and auditing” - Whittaker et al. 2018: 18ff) [1] [2]



[1] <https://plato.stanford.edu/entries/ethics-ai/>

[2] <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

Appendix

- Previously for e-privacy on a «similar» topic:

https://urna.winstonsmith.org/materiali/2016/atti/ep2016se_20_zanoni_Gabriele_Zanoni_E-privacy_2016.pdf

http://urna.winstonsmith.org/materiali/2019/atti/ep2019se_27_zanoni_say_something_interesting_about_me.pdf