COLLEGE OF INFORMATION STUDIES

Where's my data going? Privacy, security, and ethical challenges in the era of ubiquitous data collection

Jessica Vitak
Assistant Professor, iSchool, University of Maryland
Email: jvitak@umd.edu | Twitter: @jvitak

Who am I?

- ✓ Assistant professor in the iSchool at UMD
- ✓ Research evaluates how people understand privacy implications of data sharing
- ✓ Research located at the intersection of Communication (home discipline), CSCW, and HCI
- ✓ Currently funded by NSF, IMLS, Facebook, and Google

COLLEGE OF INFORMATION STUDIES

UNIVERSITY of WISCONSIN UWMILWAUKEE

ERASMUS UNIVERSITEIT ROTTERDAM

PERVADE
PERVASIVE DATA ETHICS
for computational research

NSF Award #1640697

EAGER: Mapping Privacy & Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US

Goal: Cross-cultural evaluation of how people develop mental models of privacy and data sharing when using popular mobile apps like Fitbit, Whatsapp & Amazon Echo/Google Home.

NSF Award #1704369

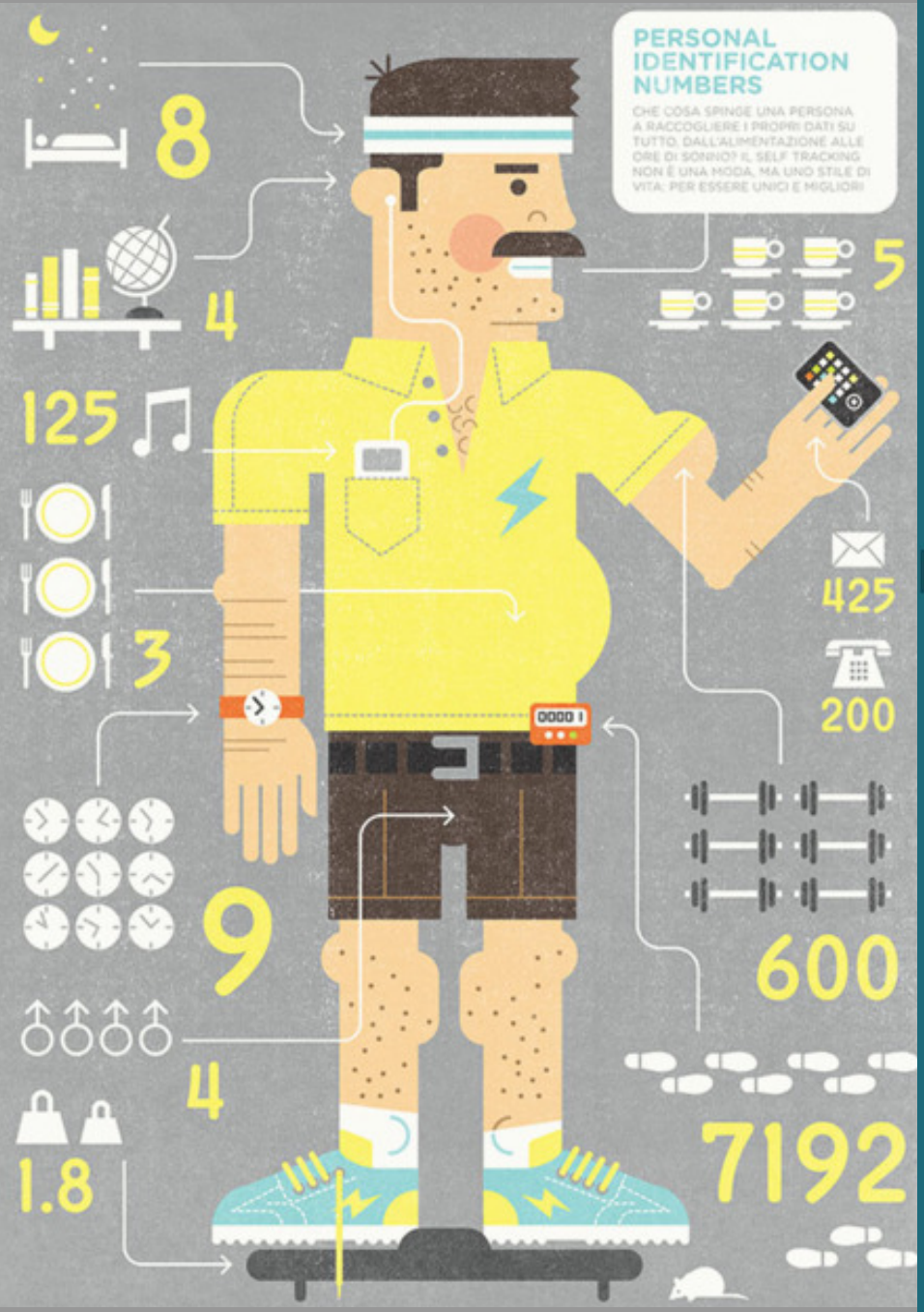
CHS: Large: Pervasive Data Ethics for Computational Research

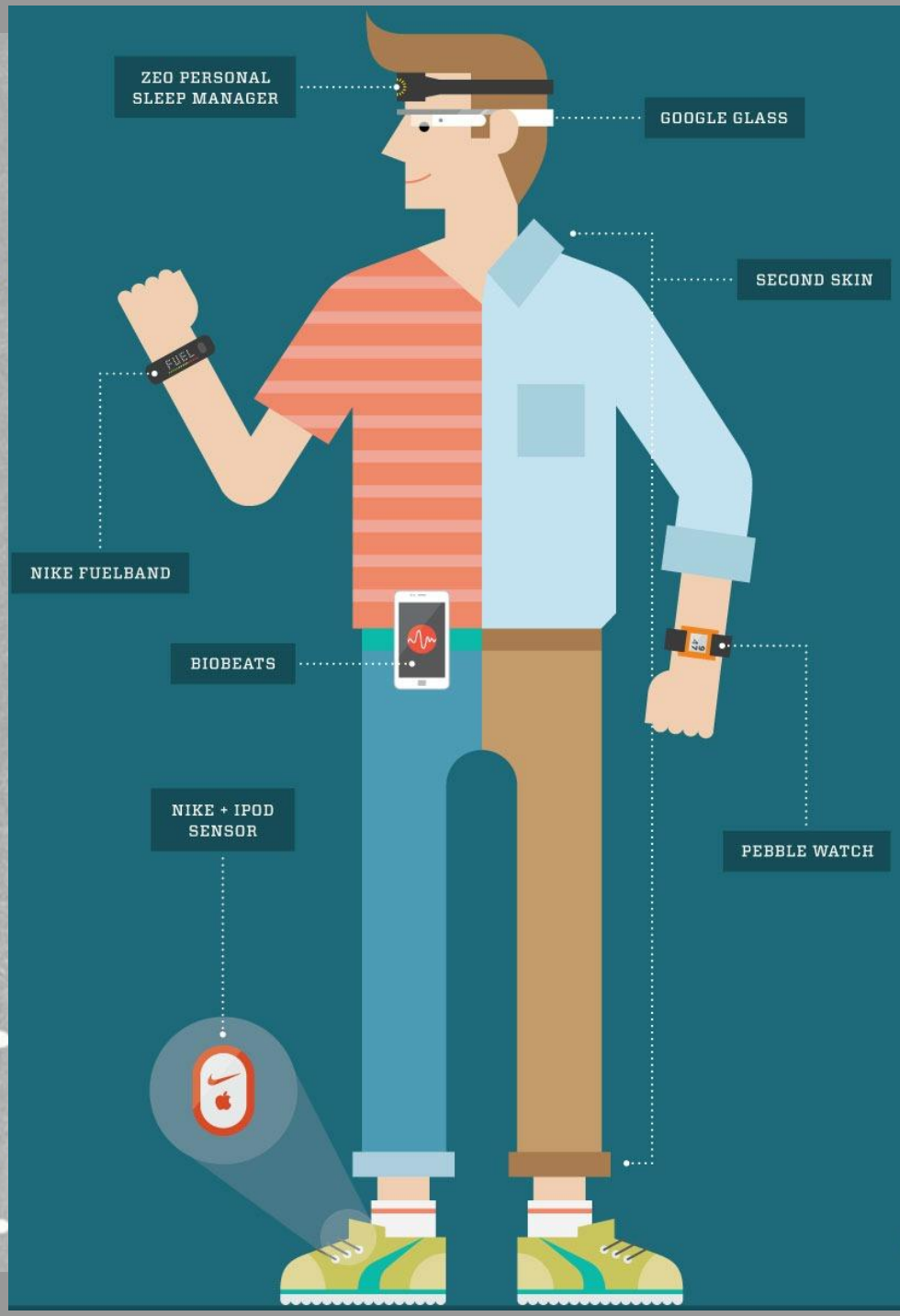
Goal: PERVADE is a collaboration of seven researchers' at six institutions exploring how people experience the reuse of their personal data within computational research.

Both purposefully and unwittingly, we are generating gigabytes of data about ourselves every week, month, and year.

What do we mean by the **quantified self**?

Self-knowledge through self-tracking using technology.


PERSONAL IDENTIFICATION NUMBERS
CHE COSA SPINGE UNA PERSONA A RACCOGLIERE I PROPRI DATI SU TUTTO, DALL'ALIMENTAZIONE ALLE ORE DI SONNO? IL SELF TRACKING NON È UNA MODA, MA UNO STILE DI VITA: PER ESSERE UNICI E MIGLIORI
8
4
125
3
9
4
1.8
5
425
200
600
7192


ZEO PERSONAL SLEEP MANAGER
GOOGLE GLASS
SECOND SKIN
NIKE FUELBAND
BIOBEATS
NIKE + IPOD SENSOR
PEBBLE WATCH

Tracking Every Breath You Take and Every Move you Make

Fitness trackers (including Fitbit and Apple Watch), collect **a lot of data**

- Steps taken
- Distance traveled
- Floors climbed
- Calories burned
- Time slept
- Heart rate
- Activity/workout statistics
- Location/GPS (sometimes)

Fitness trackers are increasingly designed to be worn unobtrusively on the body—and to collect data constantly while worn.

Devices That Always Listen

Intelligent Personal Assistants (IPAs) like Amazon Alexa and Google Home are increasingly popular in-home devices that passively listen and respond to voice commands.

However, these devices raise questions about what data is captured and how it is stored.

WHEN VISITING A NEW HOUSE, IT'S GOOD TO CHECK WHETHER THEY HAVE AN ALWAYS-ON DEVICE TRANSMITTING YOUR CONVERSATIONS SOMEWHERE.

Source: xkcd

[Technically Speaking] How did we get here?

1. Electronic sensors are smaller and better
2. Increased computing power of mobile phones
3. Public sharing (online) became normalized
4. Rise of the "cloud" to allow instant data transmission, aggregation, and analysis

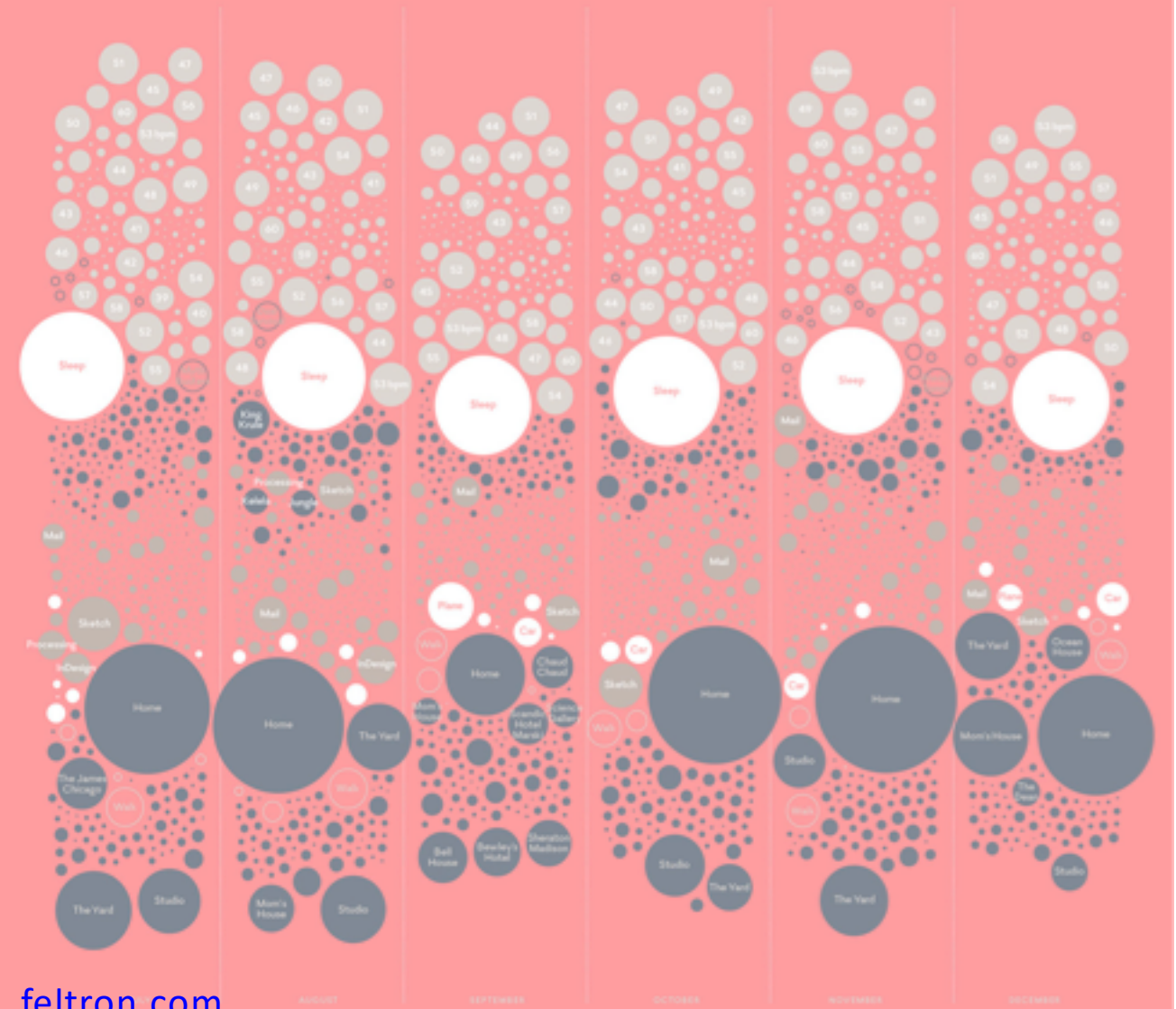
See "The Data-Driven Life" (2010) in *The New York Times* by Gary Wolf

But what else can be done with all this data being collected?

And who will get access to this data once we share it?

Flickr: ginnerobot

Inferring Behavior from **Data**



- Dietary habits
- Stress levels
- Alcohol use
- Exposure to pollutants
- Social context
- Movement patterns

- Insurance rates?
- Fidelity?

feltron.com

Fitbit tracking data comes up in another court case

Mariella Moon, @mariella_moon
06.28.15

Comments

302
Shares

HOMICIDE

Murder case cracked by Fitbit: Connecticut suspect enters plea

Published April 28, 2017 · Fox News

AddThis

SECTIONS

DAILY NEWS | NEWS

Crime U.S. World Politics

Police, attorneys are using fitness trackers as court evidence

Users, however, largely consider fitness tracker data to be non-sensitive.

Flickr: Kjetil Korslien

Sensitive data in the digital age

Personally identifiable information (PII) refers to data that can identify an individual in a dataset.

In the age of big data, we are creating increasingly complex digital footprint from our digital trace data.

Current Study: Research Questions

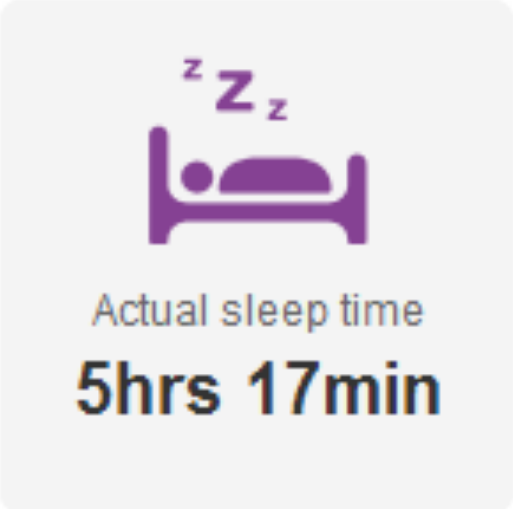
- How much do users know about the data practices of fitness tracking platforms?
- Do they feel that fitness trackers collect sensitive data?
- How do their (a) privacy concerns and (b) internet skills relate to their attitudes toward this data?

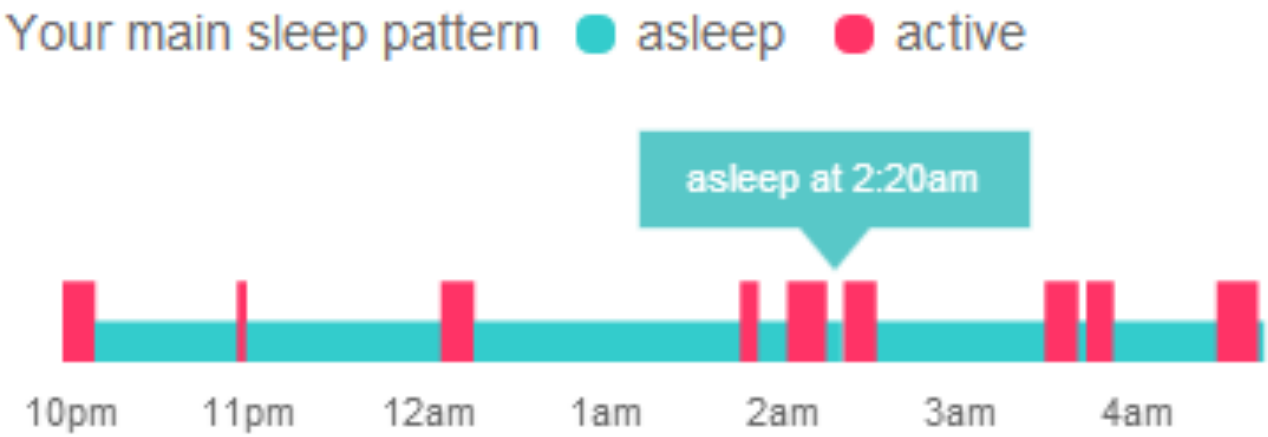
Image: Pixabay

Data we've collected

Survey of Fitbit & Jawbone users (N=361)

Follow-up interviews with a subset of users (N=33)





Summary of findings

1. Users spend little time engaging with fitness companies' data collection policies—and have low concerns about fitness data. (surveys and interviews)

2. Users' knowledge of these companies' data policies is **unrelated** to their concerns about and valuation of their fitness data. (surveys)

Summary of findings

3. Benefits of these devices far outweigh any perceived drawbacks. (interviews)

4. Users largely interface with trackers through mobile apps, which lack privacy feature granularity. (interviews)

Fitbit's Website Account Privacy Settings

Privacy

Personal Info

Pictures

Birthday

Gender

Height

Location

My Friends

Statistics

Badges & Trophies

Lifetime Steps, Distance, and Floors

Average Daily Step Count

Graphs

Calories Intake and Burn Graph

Steps, Distance, Floors Graph

Time Active Graph

Sleep Graph

Weight Graph

Fitbit's Mobile App Privacy Settings

Verizon 10:54 AM 88%

Cancel Friends Privacy Save

PRIVACY SETTING

Private

Friends ✓

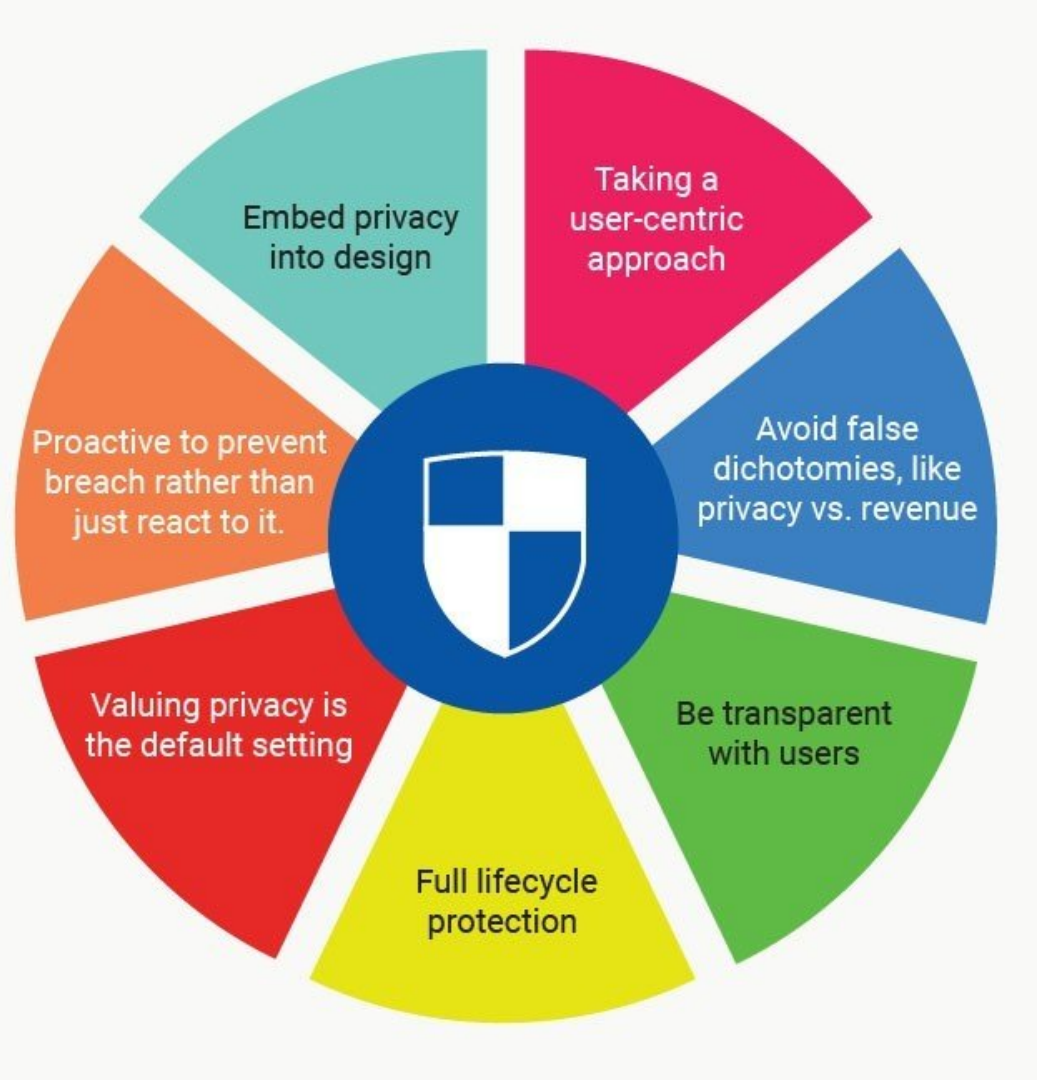
Public

Dashboard Challenges Guidance Community Notifications

Implications

How do you make users more aware of the potential uses (and misuses) of personal fitness data?

1. Embrace the Privacy by Design framework.
2. Nudge users toward privacy-focused decision making.
3. Ethical research considerations



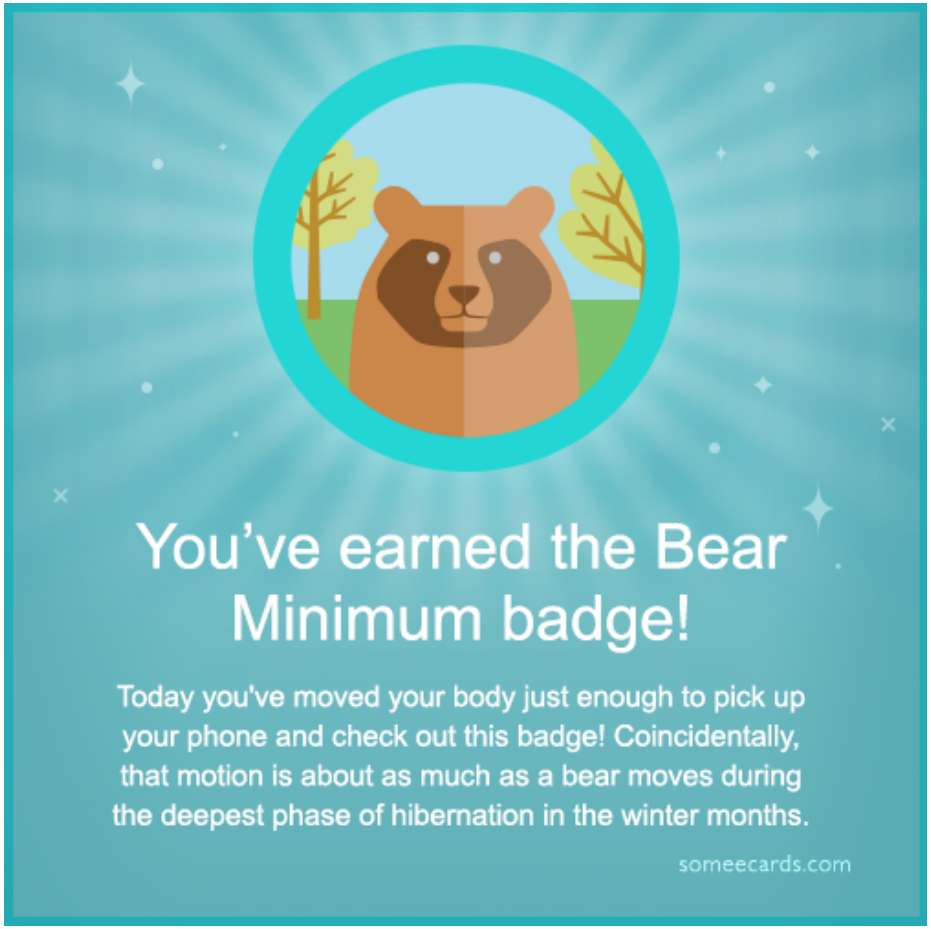
Thanks!

For more information, see pearl.umd.edu

Co-authors on this project:

Michael Zimmer, Priya Kumar, Yuting Liao, and Katie Kritikos

This project is being funded by the National Science Foundation (NSF), #1640697



Me? I'm Jessica Vitak

jessicavitak.com | jvitak@umd.edu | Twitter: @jvitak