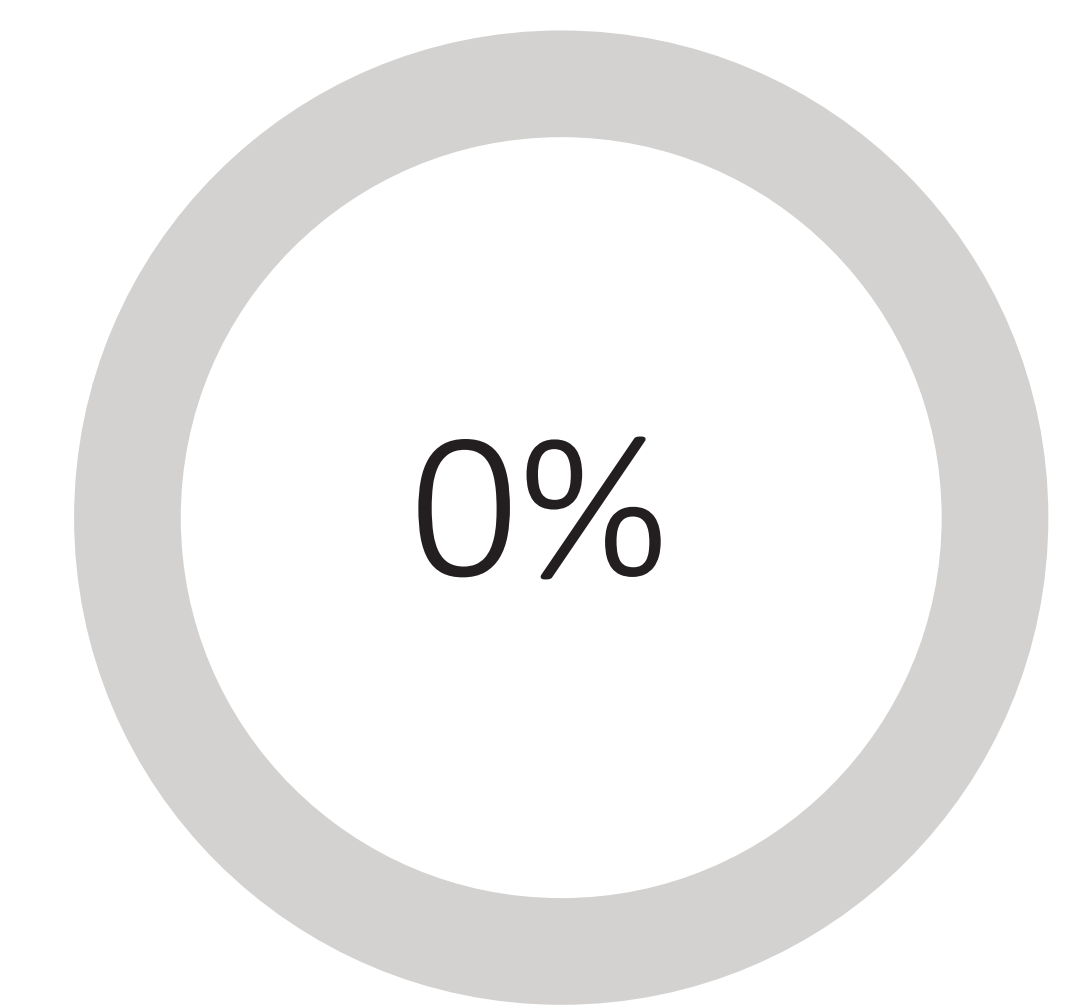


Nowadays, we always have discussions and conversations about turning of the location services on our phones, surveillance cameras and trackers on websites. But do we ever think about the trackers that aren't that obvious and widely discussed?

My research will dig into the question whether the non-human forms of sociality create implications for the privacy of Fitbit users. To answer this question, I looked into the non-human actors of a Fitbit, the Terms of Use and the Privacy Policies. This infographic shows the results from this research. Concluded is that the main privacy implication that is created by the non-human actors is the fact that users aren't aware of the fact that the Bluetooth connection that transfers the data from their Fitbit to their app is not encrypted and thus lacks security.

This infographic is based on the fitbit dashboard.

% of communication about privacy issues in the policies



Bluetooth



Third parties

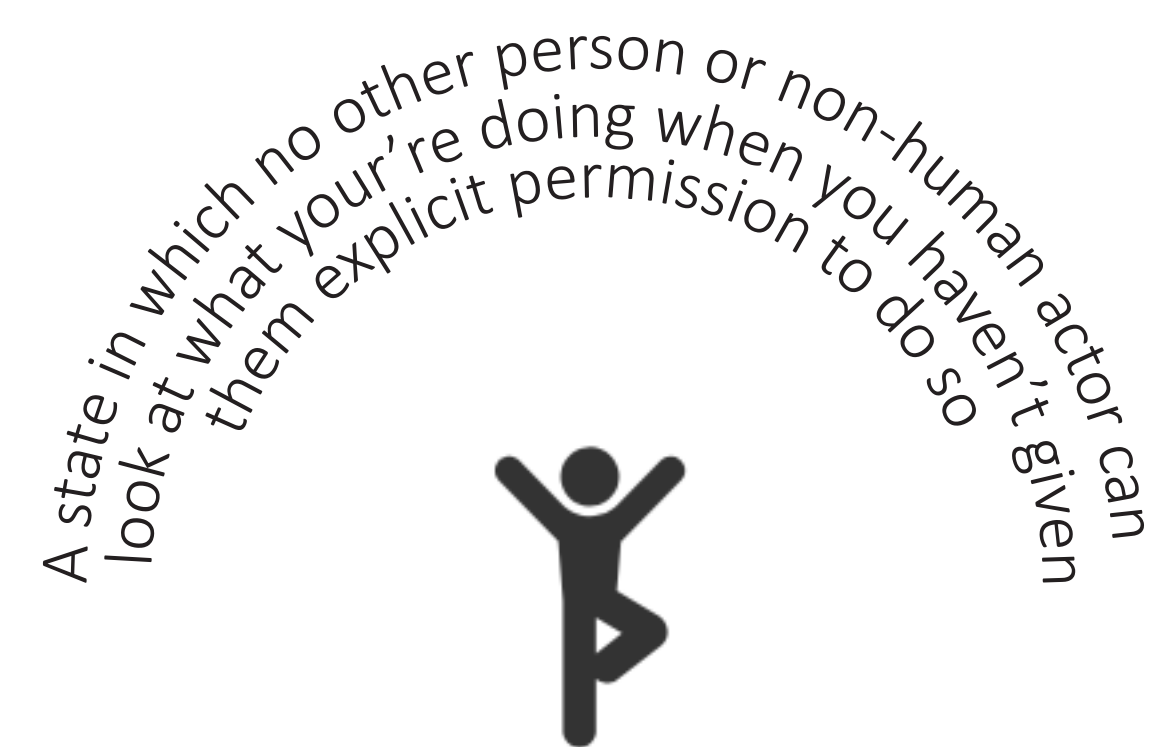


Data collecting



Data saving

Privacy



Data Fitbit collects

De-identifiable information

Data that can't be linked to the user where the information is from.

1

Identifiable information

Data that can be linked back to the user where the information is from.

2

Uploaded data

Data that got uploaded into the app by users.

3

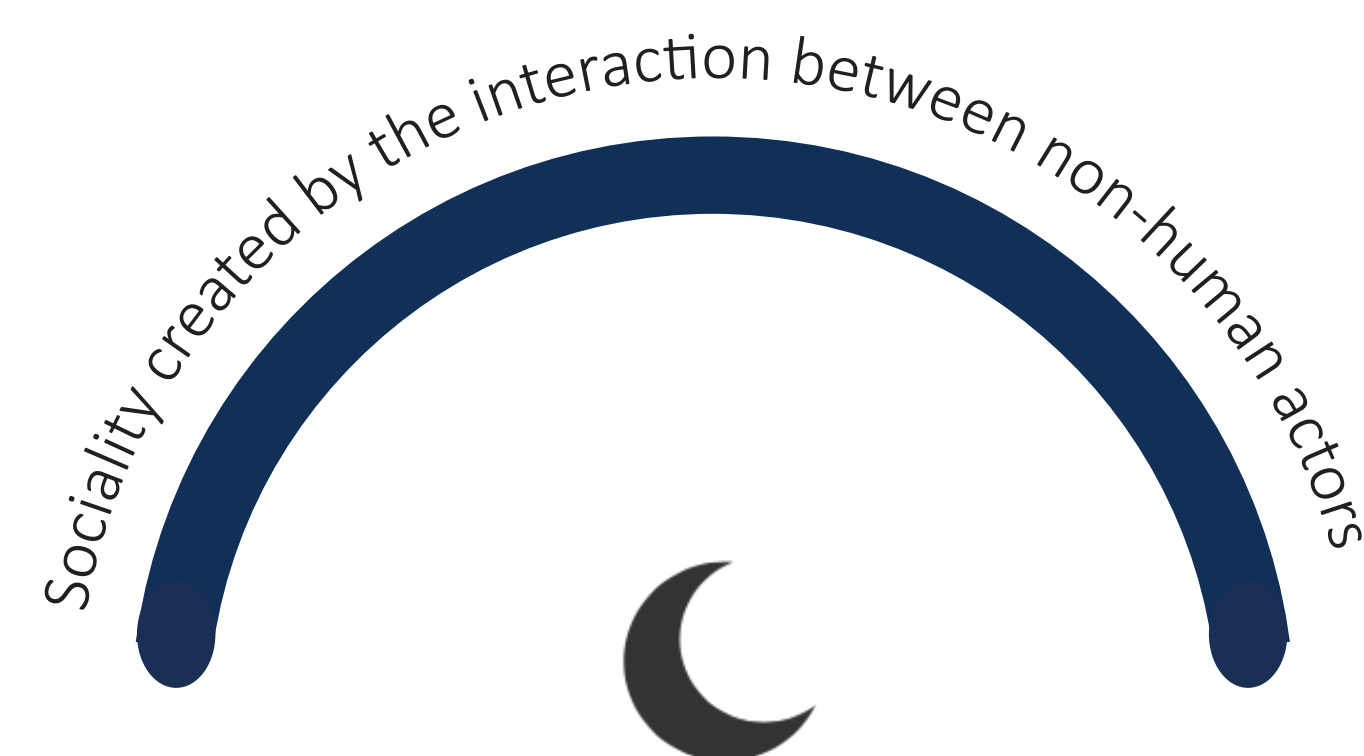
Keypoints policies

Terms of Use

- Everything uploaded is theirs
- Terms of Use do not apply to third party apps and content

Privacy Policy

- Personal information collected
- De-identifiable information collected
- All information stored on servers
- Information not shared, unless it's necessary



Non-human sociality