



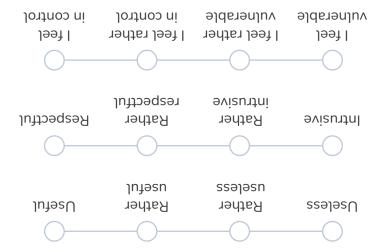


TECH // POWER-SAVING

SMART THERMOSTAT

- ★ Sensitive data collected / Sensors
- X Name and address
- X Heating and cooling usage information
- X Motion sensor
- X Environmental data: temperature, humidity, ambient light, carbon monoxide, smoke levels
- X Behavioural data such as sleep information and presence of residents (if at home or not)

- Risks and vulnerabilities
- ★ Low built-in protection: easy unauthorised access
- ★ Losing control of home temperature
- Can be used as a backdoor to break into the network and access other smart devices





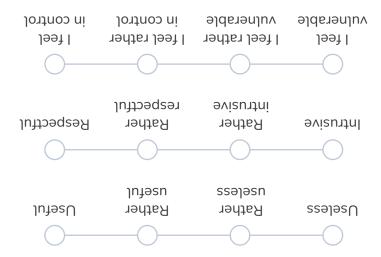




- X Sensitive data collected / Sensors
- **X** Real-time energy consumption tracking
- X Energy usage patterns
- X Behavioural data such as cooking or bathing routines
- ★ Low built-in protection: easy unauthorised access
- → Device hacking leading to fraudulent billing or blackout

★ Risks and vulnerabilities

- ★ Can be used as a backdoor to break into the network and access other smart devices
- ★ In case of a cyberattack on a smart meter network: large-scale disruptions in energy supply and widespread power outages



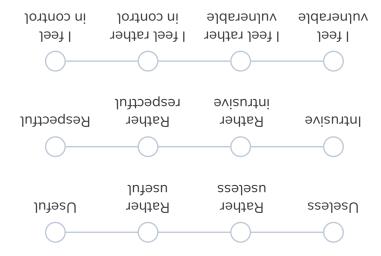






- X Behavioural data such as when and how often residents spend time in each room, bedtime routines
- X Music tastes and playlists (if the smart light is synchronised with other media)

- Risks and vulnerabilities
- carry out covert-channel exfiltration of a user's private data (within a range of 50 metres; needs a malware installation on the same network)
- or listening to, just by logging on to the pattern of the lighting (if the smart light is synchronised with other media)

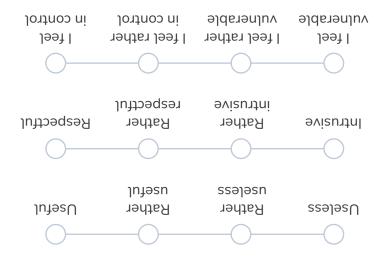








- X Sensitive data collected / Sensors
- **★** Risks and vulnerabilities
- X Local weather and soil moisture data
- X Yard mapping (used to plan irrigation precisely)
- ★ Entering and spoofing the system's configuration, the weather forecast, and various sensors (rain, water flow, soil moisture sensors) to manipulate the sprinklers
- ★ Sharing / selling of users' garden map
- 'Piping botnet': a botnet of smart sprinklers that can initiate the watering process and cause significant damage such as quickly emptying water towers and anti-flood water reservoirs—causing a reduction of the water flow or even water outages within an area



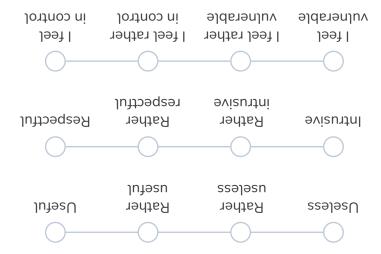




SMART ELECTRIC VEHICLE (EV) CHARGER

- ★ Sensitive data collected / Sensors
- X Vehicle and user data
- X Charging duration, location data, energy consumption
- **X** Charging schedules

- Risks and vulnerabilities
- ★ Being targeted by a large-scale cyberattack to affect the power grid
- ◆ Dependency on charging infrastructure: in Norway, smart electric chargers have taken over the fuel supply and are key for transport systems.







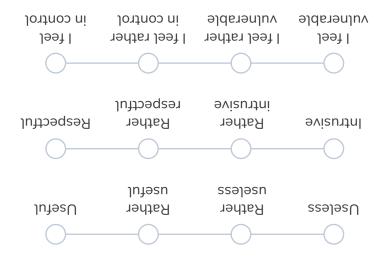


TECH // HOUSEHOLD

ROBOT VACUUM CLEANER

- X Sensitive data collected / Sensors
- X If equipped with a camera: pictures and video streams
- X Presence of pets
- X Presence of residents (if at home or not)
- X Frequency of use, cleaning schedules
- X House floor mapping
- × Recognising common household obstacles such as furniture

- Risks and vulnerabilities
- ★ Low built-in protection: easy unauthorised access to private pictures and video feeds
- ★ Sharing/selling maps of users' homes
- → Data can be analysed to know if the family is at home or away travelling
- other
- Data collected is sold to third parties for product improvement, marketing strategies or other purposes (although in most cases, service providers state that they do not sell data)





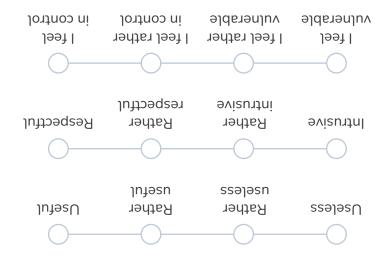


SMART KITCHEN EQUIPMENT (FRIDGE, OVEN, COFFEE MACHINE)

- ★ Sensitive data collected / Sensors
- Risks and vulnerabilities

- × Voiceprint
- ★ Food preferences, healthy/ unhealthy habits
- X Interfacing with other kitchen appliances (e.g. automatically preheats according to the recipe chosen on the fridge's display)
- X Family calendar, reminder, notes
- X Monitoring of frequent uses for optimisation purposes
- X Entertainment tastes (if the smart fridge includes built-in entertainment options, such as streaming music or TV shows)

- ★ Low built-in protection: easy unauthorised access
- ★ Sharing/selling of users' tastes to third-party companies
- ◆ Once the smart kitchen equipment is a few years old, it may stop receiving software updates from the manufacturer
- data
- Household members can monitor each other





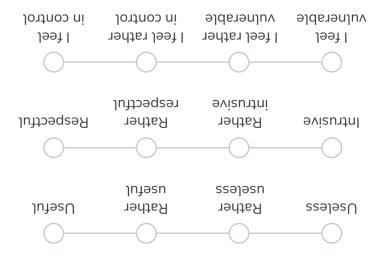




- X Sensitive data collected / Sensors
- **★** Risks and vulnerabilities

- X Air quality
- X Infrared dust sensor

- ← Clean air is dependent on Wi-Fi and stable connectivity
- allowing air quality tracking and setting modification





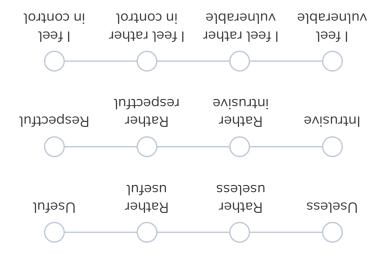




★ Sensitive data collected / Sensors

- × Presence of pets
- X Presence of residents (if at home or not)
- X Audio, pictures and video capture
- × Pets feeding schedule, food dispensing data

- Risks and vulnerabilities
- Data is not encrypted Hacking and losing control of the device: attacker can alter the feeding schedule and potentially endanger pet health, turn the feeder into a spying device, command it through a smart speaker (if linked with a smart speaker)
- Unauthorised access to private pictures and video feeds
- ← Can be used as a backdoor to break into the network and access other smart devices and sensitive data



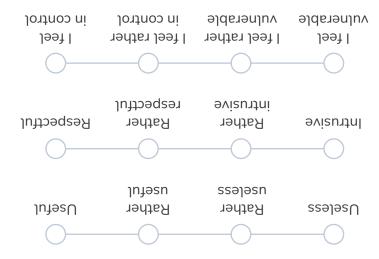
My evaluation of this technology





- X Audio and video footage X Motion sensor
- **X** Facial recognition
- ★ Metadata such as timestamps and device location
- X Interfacing with other smart home devices such as smart thermostat or lighting systems, for enhanced automation

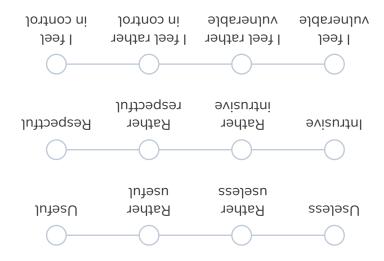
- **★** Risks and vulnerabilities
- pictures and video feeds
- Hacking and losing control of the device
- Used for remote and discreet observation of pets, children, tenants or house staff
- ★ Can be used as a backdoor to break. into the network and access other smart devices

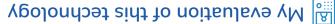






- Risks and vulnerabilities
- X Interfacing with other smart home devices such as smart light, smart alarm
- device; attacker can open and close garage doors, exposing home to burglars
- ← Can be used as a backdoor to break into the network and access other smart devices



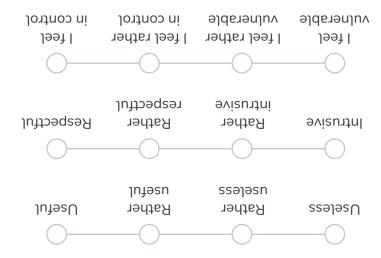






- X Sensitive data collected / Sensors
- X Infrared motion sensor, microphone and camera: audio and video footage
- X Residents' and visitors' faces and voiceprints
- × Presence of residents (if currently at home or not), residents' routines

- **★** Risks and vulnerabilities
- ◆ Data is not encrypted; can be used as a backdoor to break into the network and access other smart devices
- User identification failure (foreign accent)
- ✦ Home street location, home IP address
- ★ Footage shared with the police without authorisation
- ★ Stalking: anyone who can physically access one of the doorbells can take over the device by pairing
- ★ Many products are sold under labels and brands that disguise where it comes from (for instance Chinese products sold under Norwegian brand names)

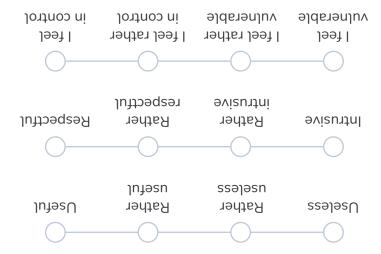






- ★ Sensitive data collected / Sensors
- X Motion sensor inside and outside
- X Voice-control activation can be remotely activated through a smart speaker
- X Presence of residents (if at home or not), residents' routines
- X Interfacing with other smart home devices such as connected shutters and lights

- Risks and vulnerabilities
- Hacking and housebreaking
- ◆ Discreet surveillance: to know when a person comes home (e.g. child surveillance)



My evaluation of this technology



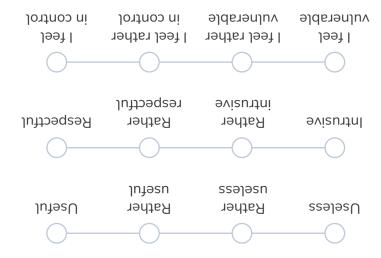


TECH // HEALTH AND WELFARE

SMART HEALTH DEVICE (INSULIN PUMP, FALL DETECTION DEVICE)

- X Sensitive data collected / Sensors
- **★** Risks and vulnerabilities
- X Health data, depending on the device: insulin level, glucose monitoring data, dose history, meal history; Accelerometer, falling incident history
- X GPS. location
- * Emergency contacts list

- danger, cause physical harm
- ★ A simple loss of Internet connection can cause malfunction
- ★ The help button battery can be depleted or defective
- ★ False alarms can lead users to lose. trust in the device
- Hacking gives access to very sensitive data; health data exploitation by third parties
- ★ Risk of isolation, relying only on IoT to age at home; not seeking medical attention or a doctor when needed





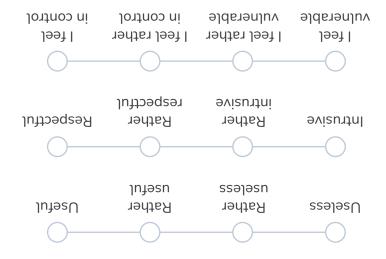


TECH // HEALTH AND WELFARE

SMART WATCH / TRAINING BRACELET

- ★ Sensitive data collected / Sensors
- X Heart rate, skin temperature, stress and mindfulness data like mood
- X Fertility and cycle trackers
- X Sleep stages, snoring & sound events (noise detection)
- X Steps and distance data, workout and activity data, sports achievements like badges and celebrations
- X Calories burned; Manually entered data
- X User account: address, height, weight, gender, and age; Interfacing with other apps gives access to name, profile picture, e-mail address, friends list

- Risks and vulnerabilities
- Hacking gives access to very sensitive data: health data exploitation by third parties
- ★ Combining body composition data with physical activity can help build a digital human twin; identity hijacking
- ★ Self-monitoring trend can lead to obsession, phobia, or enhanced competition
- ★ Accelerometer data and repetitive movement can be analysed to reveal passwords and credit card numbers
- ★ Lack of industry standards; cheap smart watches can be hackable simply by sending a text message



My evaluation of this technology





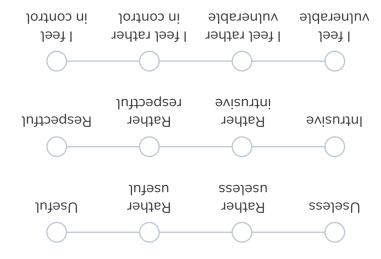
× Weight

TECH // HEALTH AND WELFARE

SMART SCALE

- X Sensitive data collected / Sensors
 - **★** Risks and vulnerabilities
- ★ Body mass index (BMI)
- X Body composition: muscle mass, bone mass, fat, water, protein
- X Heart rate monitoring
- X Fitness goals

- ★ Combining body composition data with physical activity measurements (from devices such as smart watches) could contribute to building a digital human twin, deepfakes
- ★ Self-monitoring trend can lead to obsession, phobia, or enhanced competition
- eating disorders
- ← Health data exploitation by third parties





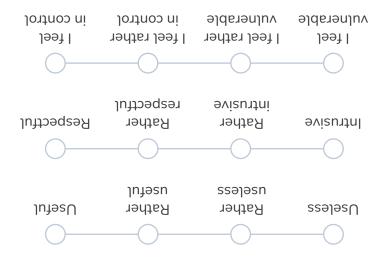


★ Sensitive data collected / Sensors

- × Watched videos history X Interests, preferences
- **X** Behaviours
- X Voiceprint, conversations
- X Cross-device tracking: data collected via a smart TV is combined with information from other smart devices such as mobile phones, laptops and home automation gear for profiling (geolocation history, web browsing activity and social media information)

Risks and vulnerabilities

- → Data collected is sold to third parties for data brokerage and advertising targeting
- ★ Camera & microphone hacking Microphones can capture conversations and other sounds within range
- ★ Automated Content Recognition (ACR): a feature often turned on by default allowing identification of video and audio running on the TV
- ★ Eavesdrop on the browser's traffic and cookies for authentication to online services, such as social media accounts or online banking

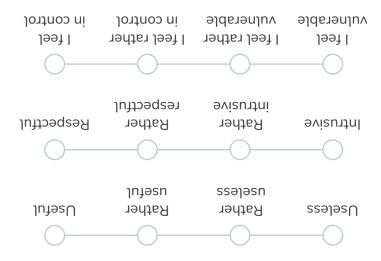








- **★** Risks and vulnerabilities
- X Voice recordings, conversations and ambient sounds
- × Voiceprint
- X Interests, preferences
- × Behaviours, daily routines
- ★ Always listening 'by design' unless the microphone is muted; microphone hacking and eavesdropping risk; collection of sensitive information such as passwords
- recordings—a percentage of these recordings are reviewed by humans to develop AI voice recognition
- → Data collected sold to third parties for data brokerage and advertising targeting
- ★ Through speaker, taking remote control of other smart devices by voice command
- Can be hacked with a simple laser pointer aimed at the speaker through a window







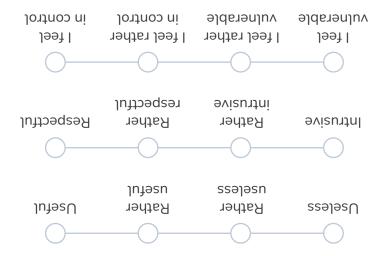


★ Sensitive data collected / Sensors

- X If microphones, cameras: movements, pictures, videos and sounds
- X Childrens' identity, voiceprint
- X Interactions with users' relatives such as parents, teachers, babysitter
- X Childrens' locations and activities over time, tastes, routines

Risks and vulnerabilities

- ★ Children are too young to fully understand the impacts of data collection
- ★ Children often share their deepest fears and dreams with their trusted tovs
- → Portable: children bring them everywhere, allowing recording of intimate moments
- ★ Attackers can take control of the toy, talk to the child through the device, cause extortion or harassment
- ★ Smart toys can be used to monitor or stake out children, capture physical location
- ★ Parents can monitor children without them knowing it



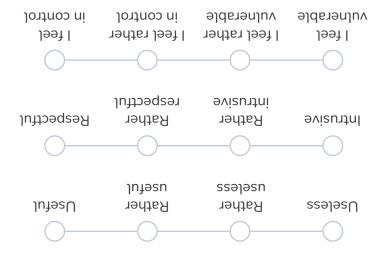






- X The player's skills, interests, consumption habits and personality traits
- X Social data: users' social activities. game preferences, amount of time spent on each game
- X Biometric data: users' physiological and emotional responses to gameplay, e.g. eye tracking through infrared cameras, recording of the player's voice, facial recognition, emotion recognition, body motion tracking
- X Behavioural data known as 'in-game telemetry' encompasses players' virtual responses to stimuli within the game

- **★** Risks and vulnerabilities
- ∮ In-game data collection
- Hacking can give access to name, address, passwords, security answer, e-mail, birthday, purchase history, credit card and bank account information
- ◆ Data-crossing and correlations between gameplay and social/ biometric/behavioural data can be exploited to build a deepfake or even a digital human twin of the player

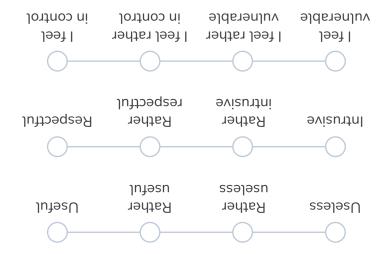






- ★ Sensitive data collected / Sensors
- X A lot of data passing through, as this is the central hub of the home Internet network: all of the traffic from all of the Wi-Fi devices pass through on its way to the Cloud
- ★ Users' browsing history

- Risks and vulnerabilities
- ◆ Data is shared with third parties for advertising targeting
- as at the office
- ★ Routers and wireless access points are becoming the most common entry points for malware
- → Hacked to conduct illegal activities, monitor and capture web traffic or steal personal files



My evaluation of this technology

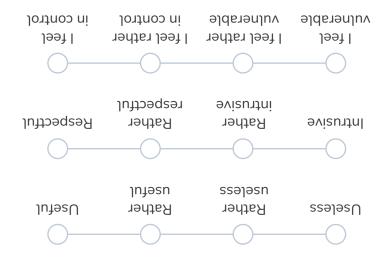


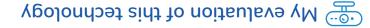


- X Sensitive data collected / Sensors
- **★** Risks and vulnerabilities

- × Activation periods
- × Print history

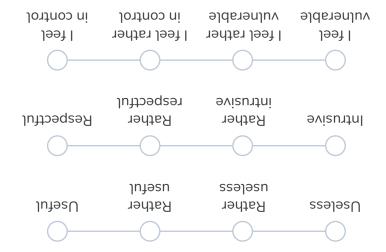
- ◆ Can be used as a backdoor to break. into the network and access other smart devices
- Hacking: losing control of the device, access to sensitive data







- **✗** Sensitive data collected / Sensors
- × Photos and video footage
- **X** Estimated working hours and routine
- Risks and vulnerabilities
- Hacking and surveillance, blackmail, extortion
- 'Camfecting': hacker takes control of the webcam and deactivate the indicator light so the user does not know they are being watched





- X Sensitive data collected / Sensors
- **X** Beverage temperature
- X Full or empty
- X Estimated caffeine intake
- **X** Estimated lifestyle or working routine
- * Interfacing with other devices such as smart watch
- ∳ Push alerts through paired app
- Correlation between coffee mug use and working hours

★ Risks and vulnerabilities