My evaluation of this technology

TECH // POWER-SAVING

SMART METER

Sensitive data collected / Sensors

- Real-time energy consumption tracking
- Energy usage patterns
- Behavioural data such as cooking or bathing routines

Risks and vulnerabilities

- Low built-in protection: easy unauthorised access
- Device hacking leading to fraudulent billing or blackout
- 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

My evaluation of this technology

TECH // POWER-SAVING

SMART THERMOSTAT

Sensitive data collected / Sensors

- Name and address
- Heating and cooling usage information
- Motion sensor
- Environmental data: temperature, humidity, ambient light, carbon monoxide, smoke levels
- 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

TECH // POWER-SAVING

SMART LIGHT

Sensitive data collected / Sensors

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

Risks and vulnerabilities

- Use the bulbs' infrared capabilities to 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)
- Uncover what someone is watching or listening to, just by logging on to the pattern of the lighting (if the smart light is synchronised with other media)

TECH // RESOURCE-SAVING

SMART SPRINKLER

Sensitive data collected / Sensors

- Local weather and soil moisture data
- Yard mapping (used to plan irrigation precisely)

Risks and vulnerabilities

- 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

My evaluation of this technology

TECH // POWER-SAVING

SMART ELECTRIC VEHICLE (EV) CHARGER

Sensitive data collected / Sensors

- Vehicle and user data
- Charging duration, location data, energy consumption
- 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.

My evaluation of this technology

TECH // HOUSEHOLD

ROBOT VACUUM CLEANER

Sensitive data collected / Sensors

- If equipped with a camera: pictures and video streams
- Presence of pets
- Presence of residents (if at home or not)
- Frequency of use, cleaning schedules
- 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
- Household members can monitor each 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)

My evaluation of this technology

TECH // HOUSEHOLD

SMART KITCHEN EQUIPMENT (FRIDGE, OVEN, COFFEE MACHINE)

Sensitive data collected / Sensors

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

Risks and vulnerabilities

- 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
- Collection and leak of users' health data
- Household members can monitor each other

My evaluation of this technology

TECH // HOUSEHOLD

SMART AIR PURIFIER

Sensitive data collected / Sensors

- Air quality
- Infrared dust sensor

Risks and vulnerabilities

- Clean air is dependent on Wi-Fi and stable connectivity
- Most often connected to an app allowing air quality tracking and setting modification

My evaluation of this technology

TECH // HOUSEHOLD

SMART PET FEEDER

Sensitive data collected / Sensors

- Presence of pets
- Presence of residents (if at home or not)
- 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

TECH // SECURITY

SMART SECURITY CAMERA

Sensitive data collected / Sensors

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

Risks and vulnerabilities

- Unauthorised access to private 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

My evaluation of this technology

TECH // SECURITY

SMART DOORBELL

Sensitive data collected / Sensors

- Infrared motion sensor, microphone and camera: audio and video footage
- 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)

My evaluation of this technology

TECH // SECURITY

SMART GARAGE DOOR

Sensitive data collected / Sensors

- Interfacing with other smart home devices such as smart light, smart alarm

Risks and vulnerabilities

- Hacking and loss of control of the 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

TECH // SECURITY

SMART ALARM SYSTEM

Sensitive data collected / Sensors

- Motion sensor inside and outside
- Voice-control activation can be remotely activated through a smart speaker
- Presence of residents (if at home or not), residents' routines
- 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)*

TECH // HEALTH AND WELFARE

SMART HEALTH DEVICE (INSULIN PUMP, FALL DETECTION DEVICE)

Sensitive data collected / Sensors

- Health data, depending on the device: insulin level, glucose monitoring data, dose history, meal history; Accelerometer, falling incident history
- GPS, location
- Emergency contacts list

Risks and vulnerabilities

- Malfunction can put the person in 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

My evaluation of this technology

TECH // HEALTH AND WELFARE

SMART SCALE

Sensitive data collected / Sensors

- Weight
- Body mass index (BMI)
- Body composition: muscle mass, bone mass, fat, water, protein
- Heart rate monitoring
- Fitness goals

Risks and vulnerabilities

- 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
- Ultra precise measures can favour eating disorders
- Health data exploitation by third parties

My evaluation of this technology

TECH // HEALTH AND WELFARE

SMART WATCH / TRAINING BRACELET

Sensitive data collected / Sensors

- Heart rate, skin temperature, stress and mindfulness data like mood
- Fertility and cycle trackers
- Sleep stages, snoring & sound events (noise detection)
- Steps and distance data, workout and activity data, sports achievements like badges and celebrations
- Calories burned; Manually entered data
- 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

TECH // ENTERTAINMENT

SMART SPEAKER

Sensitive data collected / Sensors

- Voice recordings, conversations and ambient sounds
- Voiceprint
- Interests, preferences
- Behaviours, daily routines

Risks and vulnerabilities

- Always listening *'by design'* unless the microphone is muted; microphone hacking and eavesdropping risk; collection of sensitive information such as passwords
- Unwanted activation and accidental 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

My evaluation of this technology

TECH // ENTERTAINMENT

SMART TV

Sensitive data collected / Sensors

- Watched videos history
- Interests, preferences
- Behaviours
- Voiceprint, conversations
- 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

My evaluation of this technology

TECH // ENTERTAINMENT

CONNECTED TOY

Sensitive data collected / Sensors

- If microphones, cameras: movements, pictures, videos and sounds
- Childrens' identity, voiceprint
- Interactions with users' relatives such as parents, teachers, babysitter
- 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 toys
- 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

My evaluation of this technology

TECH // ENTERTAINMENT

GAMING CONSOLE

Sensitive data collected / Sensors

- The player's skills, interests, consumption habits and personality traits
- Social data: users' social activities, game preferences, amount of time spent on each game
- 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
- 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

My evaluation of this technology

TECH // REMOTE WORKING

SMART PRINTER

Sensitive data collected / Sensors

- Activation periods
- Print history

Risks and vulnerabilities

- 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
- Used to install malware

My evaluation of this technology

TECH // REMOTE WORKING

WIRELESS ROUTER

Sensitive data collected / Sensors

- 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
- Not the same cyberprotection at home 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

TECH // REMOTE WORKING

WEBCAM

Sensitive data collected / Sensors

- Photos and video footage
- 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

My evaluation of this technology

TECH // REMOTE WORKING

SMART MUG

Sensitive data collected / Sensors

- Beverage temperature
- Full or empty
- Estimated caffeine intake
- Estimated lifestyle or working routine
- Interfacing with other devices such as smart watch

Risks and vulnerabilities

- Push alerts through paired app
- Correlation between coffee mug use and working hours