# TRUST WHEN WE ARE LIVING INSIDE A COMPUTER

**Rory Bradley**
Institute of Art
Design + Technology

Dublin, Ireland
rory.bradley@iadt.ie

**Dr. Hilary Kenna**
Institute of Art
Design + Technology

Dublin, Ireland
hilary.kenna@iadt.ie

## Abstract

The Internet of Things can provide a range of benefits to society, from better managing resource consumption to increased security and health care. For this technology to grow and achieve widespread adoption, consumers must sufficiently trust it (Benbasat & Wang, 2005). Proposals have been put forward by researchers, designers and governments to inform users of the implications of using these devices (Emami-Naeini et al., 2020). A recurring proposal is a personalised privacy assistant (PPA) that can help users better manage their privacy in a smart home (Colnago et al., 2020). This pictorial focuses on exploring this need.

### Authors Keywords

Smart Home; Personal Privacy Assistants; Trust; Human Centred Design

### Images

All images are author own except where stated



## Overview

This pictorial will feature the main points from a literary review. It will show a breakdown of a smart home configuration and how data flows through it. It will illustrate how and why this data is collected and suggest a PPA as a means to control this flow of data. It will then introduce the Stanford d.School design thinking process (Dam & Siang, 2020) as a means to explore the design of a PPA and test it for levels of trust.

## Background

The internet of things (IoT) is a network of devices that can send and receive data about the environment they are situated in. An increasingly popular application for these devices is in the domain of smart homes. Smart homes are homes that have been augmented with IoT devices. In the near future smart homes could help us live longer healthier lives (Ziefle et al., 2011), better manage consumption of energy, food and water (Williams et al., 2017) and integrate with artificial intelligence to make decisions on our behalf (Gulati et al., 2018). This research is taking place during the Covid-19 pandemic, currently ways of helping treat patients of the virus are been explored using smart home devices (Nasajpour et al., 2020).

As we add more smart home devices to our homes we must to ensure they adhere to our notions of privacy (Paradiso & Siewiorek, 2020). Studies have shown that while users are concerned about privacy, they have little knowledge of the privacy practices and data collection of these devices (Das et al., 2018). Shoshana Zuboff states that the imbalance of information between the users of connected devices and the manufacturers who extract data through them is unprecedented (Zuboff, 2019).

## Literary review

Eight key points were derived from a literary review covering the area of smart homes, PPA and trust as it relates to technology.

### Smart Homes

**1** The market for smart home technology and connected devices is growing (Mestrado & Projecto, 2019).

**2** Widespread smart home adoption could bring many benefits (Acquisti et al., 2017; Bennett et al., 2017; Gulati et al., 2018; Williams et al., 2017; Ziefle et al., 2011).

**3** Users are concerned about privacy and data collection within smart homes (Caltrider, 2017; Deloitte, 2016; Paradiso & Siewiorek, 2020; "Securing IoT," 2019).

**4** Some users fit the privacy paradox (Emami-Naeini et al., 2020; Williams et al., 2017).

### PPA

**5** Researchers, non-profits and designers are exploring ways to help users mange their data (Emami-Naeini et al., 2020; Margot James, 2019; Zheng et al., 2018).

**6** Personal Privacy Assistants, have been proposed as a way to help users (Colnago et al., 2020; Das et al., 2018; Sadeh, 2019).

### Trust as it relates to technology

**7** Trust is vital for Smart Homes (Cannizzaro & Procter, 2020; Williams et al., 2017).

**8** Trust in a technology could be associated with ease of use (Flavián et al., 2006; McKnight, 2012).

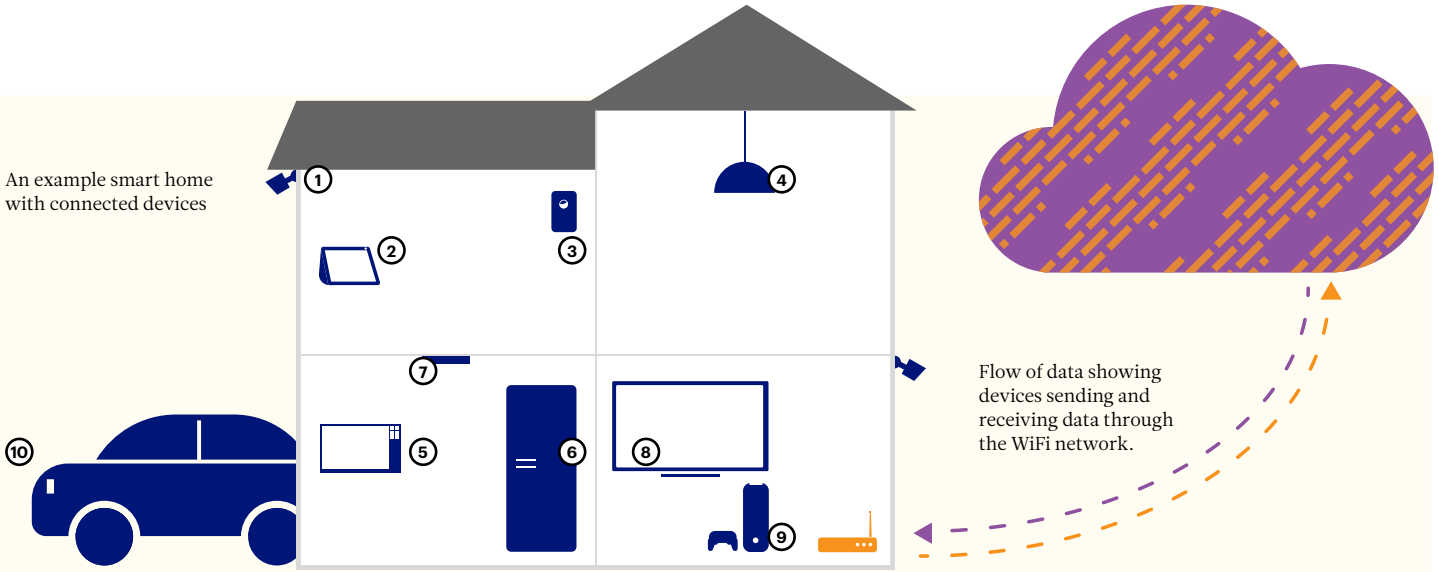
# FLOW OF DATA THROUGH A SMART HOME

A smart home can have many configurations and is continuing to evolve (Williams et al., 2017). A common model is a home enhanced with monitoring and control functionality from connected devices, these are usually connected through the homes WiFi network (Sadowski, 2019).

These connected devices allow the user to control applications such as heating, water systems, lighting, windows, blinds, doors, TV's and washing machines. Some connected devices also have sensors to allow them to collect data from their environments such as audio, visual, location, temperature, humidity, air quality and rainfall.

## Smart Homes

Smart homes feature an array of devices connected together via a network, this network is often provide by a WiFi Router. The router acts as way for data to flow in and out of the home. Data flowing out is often sent to cloud services where it is processed and stored.




An example smart home with connected devices

Flow of data showing devices sending and receiving data through the WiFi network.

### Connected devices

These are electrical devices or appliances that have the capacity to sense and record data about their environment. They are connected to the internet or other devices. They can be controlled by a user interface, voice user interface or via smart phones, tablets and smart watches (Zuboff, 2019).

1. Security camera
2. Smart hub
3. Smart thermostat
4. Smart light
5. Smart oven
6. Smart fridge
7. Smoke alarm
8. Smart TV
9. Games console
10. Smart car

### WiFi Network

WiFi serves as the network layer of a smart home. It connects together the connected devices in the house. It allows them to send and receive data to one another and cloud services. Other infrastructures such as Bluetooth or ZigBee can also serve this function (Sadowski, 2019).

### Cloud Services

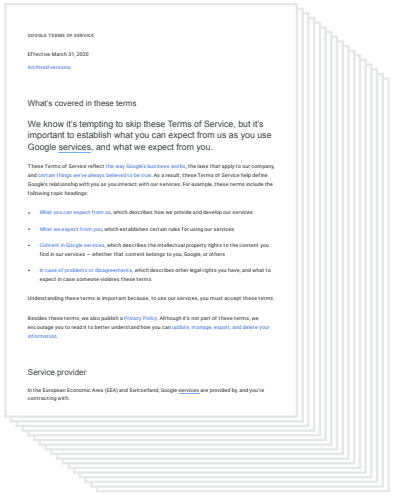
The data collected via connected devices is sent through the WiFi router to Cloud Services. This is where the data is processed and, depending on the type of data, can be used in a number of different ways (Sadowski, 2019).

# ACCESSING OUR DATA

Interacting with connected devices generates large amounts of data. This data is very valuable to companies, it is sometimes referred to as data capital. When companies seek consent to record and extract this data it is typically done through end-user licensing agreements(EULAs) (Sadowski, 2019). In a smart home context, they will appear before a user can access the service's available to their connected device.

EULAs are long, dense legal documents. One study estimated that it could take 201 hours a year to read all of the EULA a person will encounter in their life (Mcdonald & Cranor, 2008). If a user does not agree with the EULAs the functionality and security of their connected device can be compromised (Zuboff, 2019). EULAs are not easily understood and some consider them less a form or consent and more a form or compliance (Sadowski, 2019).

Googles terms of service is a 17 page document. In order to utilise their services the user must agree to all of the terms laid out.


GOOGLE TERMS OF SERVICE

Effective March 31, 2020

Archived versions

What's covered in these terms

We know it's tempting to skip these Terms of Service, but it's important to establish what you can expect from us as you use Google services, and what we expect from you.

These Terms of Service reflect the way Google's business works, the laws that apply to our company, and certain things we've always believed to be true. As a result, these Terms of Service help define Google's relationship with you as you interact with our services. For example, these terms include the following topic headings:

- What you can expect from us, which describes how we provide and develop our services
- What we expect from you, which establishes certain rules for using our services
- Content in Google services, which describes the intellectual property rights to the content you find in our services — whether that content belongs to you, Google, or others
- In case of problems or disagreements, which describes other legal rights you have, and what to expect in case someone violates these terms

Understanding these terms is important because, to use our services, you must accept these terms.

Besides these terms, we also publish a Privacy Policy. Although it's not part of these terms, we encourage you to read it to better understand how you can update, manage, export, and delete your information.

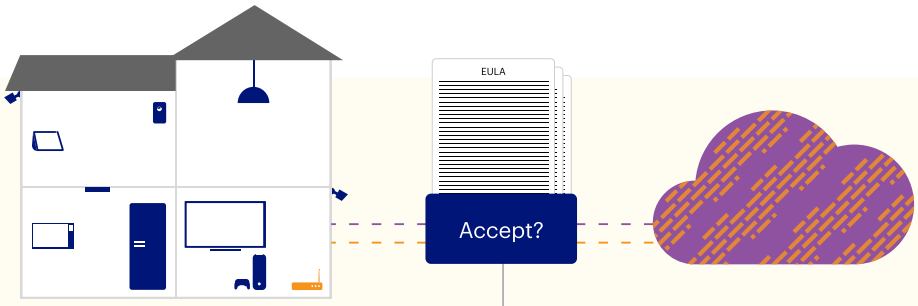
Service provider

In the European Economic Area (EEA) and Switzerland, Google services are provided by, and you're contracting with:

## Creating value from our data

Value is drawn from data in a number of ways, typically the most sought after is user data (Zuboff, 2019). Below are some examples of how this data can be turned into value for companies.

These examples are based on research by Sadowski (2019) and Zuboff, (2019). These examples are not exhaustive and companies are actively discovering more ways to use data.




### Profile and target people

Your data can inform targeted ads, prices based on customer characteristics or identifying segments of people susceptible to certain kinds of political messaging.

### Predictive Behaviour Models

As more data is collected companies can identify trends and forecast probabilities based on your behaviour.

### Optimise systems

In a smart home context, how you use a device could be informing your experience of a system compared to someone else.

### Build digital systems

Many digital services and systems are built on data, for example Uber uses real time data on the location of it's drivers and customers.

### Tracking and Analytics

Using connected devices, you can track various aspects of your life. For example a smart fridge could track your diet or a smart thermostat could track your energy use.

### Grow the value of assets

Buildings, vehicles and machinery can depreciate over time but upgrading assets with ability to collect data on this wear and tear helps to combat deterioration.

## PPA

A PPA is an application on a smart phone or watch that helps users discover connected devices in their vicinity and learn about their data practices (Sadeh, 2019). This in an emerging technology in the context of a smart home but it follows other examples of moves to educate users on how their data is collected and used.

For the purposes of this pictorial a PPA will be designed for use in a smart home context. It will utilise privacy nudges as a way to nudge users towards more secure decisions without limiting their options.

## PRIVACY NUDGES

"Soft Paternalism" uses research from behavioural economics to "nudge" users towards making more secure choices while not limiting their options (Story et al., 2020). Food labelling and driver feedback signs are examples of nudging towards more responsible actions. Acquisti et al., (2017) layout dimensions of these nudges and how they can assist users in making secure choices. These dimensions will be applied to the design of the PPA.



The nudges are:

### - Information

Provide information to reduce the imbalance of information between users and manufacturers of connected devices.

### - Presentation

Create a presentation that provides necessary contextual cues in the user interface to reduce cognitive load and convey any possible risks.

### - Defaults

Configure the defaults of the system to priorities privacy.

### - Incentives

Incentivise users to configure the system according to their stated privacy preferences.

### - Adjustable Settings

Allow users to recover from mistakes, opt out or adjust their settings.

### - Timing

Nudge users at appropriate times, this can give contextual information on why data is been collected.

# METHODOLOGY

This pictorial proposes to design and test two versions of a PPA prototype to control the flow of data from a smart home:

PPA-1 – included privacy nudges

PPA-2 – did not include any privacy nudges

The main research question of this pictorial is

**Will users trust the PPA with privacy nudges more than the PPA without?**

To answer this question the following hypothesis are put forward.

**H1** The PPA with privacy nudges will have a higher rating of trust than the PPA without privacy nudges.

**H2** The PPA with privacy nudges will have a higher useability rating than the PPA without privacy nudges.

# THE DESIGN PROCESS

This pictorial will follow an explanatory sequential mixed methods research design, first gathering quantitative data and then performing qualitative user testing. The project will be broken into the five stages of the design thinking methodology developed at the Standford d.school. This methodology is useful for understanding the human needs involved in a project and takes an iterative design approach to developing artefacts (Dam & Siang, 2020).

The satges of the process are:

**1 - Empathise**
**2 - Define**
**3 - Ideate**
**4 - Prototype**
**5 - Test**

# 1 - EMPATHISE

In the first stage of the design thinking process, the goal was to gain an empathic understanding of how people use and feel about connected devices (Dam & Siang, 2020). To do this the following research activities were completed:

## Catalogue

A catalogue of connected devices was produced. This was to gain a well-rounded understanding of the range of devices available to consumers. The devices were collected from the Google store, Apple Homekit and Amazon as well as research by Mozilla, (2020) and Williams et al. (2017)

## Questionnaire

Research by Williams et al. (2017) and Caltrider, (2017) informed the design of a quantitative questionnaire that was sent out to participants via social media and special interest groups. The questionnaire collected quantitative information about the respondent's smart home devices and their attitudes towards these devices.

## Expert Interview

Expert interviews were conducted with

**Sarah Gold** - CEO of Projects by IF, a design studio that helps organisations to use data responsibly.

**Catherine Friend** - An associate lecturer and researcher on cyberpsychology and cyber security.

## Key Findings

### Catalogue

78 Manufactures of smart home devices

56 Types of smart home devices

14 Categories of use

13 Types of sensors

### Questionnaire

Most respondents did not own their own home, lived with one other person and used their smart home devices everyday.

Most devices were in the sitting room and entertainment devices were the most popular type. Entertainment was also the most popular use.

Some respondents showed a distrust of connected devices while also expressing a desire to use their products linking into the privacy paradox (Williams et al., 2017).

Respondents were split over who should be responsible for protecting data their smart homes devices collect.

Most respondents don't know who to trust to help them learn how to protect their data.

**"I usually am resistant to the idea of these devices, then I end up trying one and it's usefulness wins me over. Sneaky lil things...".**

Connected device user
Male, late 30s

**"I've lost all trust for Google, Amazon, and Apple."**

Connected device user
Male, late 30s

### Interviews

The interviews were transcribed and a thematic analysis was performed to discover key themes:

- Privacy concerns around data collection are not yet mainstream.
- Consumers need choice when it comes to their data.
- Devices must be able to handle the complexity of modern human homes.

**"they don't see the effect being immediate, it doesn't really affect their immediate use of a product".**

Catherine Friend when speaking on privacy concerns.

**"how do you have understanding, trust and accountability when you're living in a computer? In the context of human life, which is really messy?"**

Sarah Gold when speaking on current challenges

# 2 - DEFINE

Findings from Catalogue, Questionnaire and Interviews in the previous stage were formulated into Peronsas and Empathy Maps. Actual responses were used to illustrate the personas opinions on smart home technology.

These act as a tool to align the design of products and services around specific groups of people rather than generic users (Harley, 2015).

**Rob and Liz live together in an apartment in Dublin. They each have differing opinions on connected devices. They are described through the following human centred design tools.**

## Personas

### Rob

32 | Male | Booterstown, Co. Dublin

Works in security at a financial company.

Very proficient with technology.

"I think they are useful but if Mozilla or another non-profit entered this space with a decent product, I'd be happy to buy it."

### Liz

30 | Female | Booterstown, Co. Dublin

Works in client relations.

Very proficient with technology.

"It feels like it's just more complication and intrusion in our lives."

Persona images sourced from Unsplash. (Man Using His Smartphone Photo, 2021; Woman in Black Fur Coat and Orange Knit Cap, 2021)

## Empathy Maps

### Rob

**Says**

Well I'd like an easy way to be in charge of it but it'll take the government developing policies to allow that to happen...

**Thinks**

- I wish this was a bit simpler.
- How do they know so much?

**Does**

- Set's up the devices.
- Links them to his accounts.
- Uses them for playing music, streaming videos, setting reminders and hosting meetings.

**Feels**

- Excited when they work.
- Frustrated when they don't work.
- Anxious when he thinks about his privacy.

### Liz

**Says**

Seems a bit creepy, my phone and computer are already a bit much I don't need a fridge listing to me.

**Thinks**

- I've lost all trust for Google, Amazon, and Apple.
- Do we really need these?

**Does**

- Avoids using smart home devices.
- Keeps the camera on her laptop covered with tape.

**Feels**

- Unsure about devices.
- Annoyed they are in her house.
- Awkward talking to Rob about them.

## Scenario

Rob bought a new connected device for the apartment.


## Jobs to be done statements

These are used to focus the brainstorming in the next stage (Dam & Siang, 2020).

### Rob

"When I use my smart home devices I want to trust them so I don't feel conflicted about my privacy."

### Liz

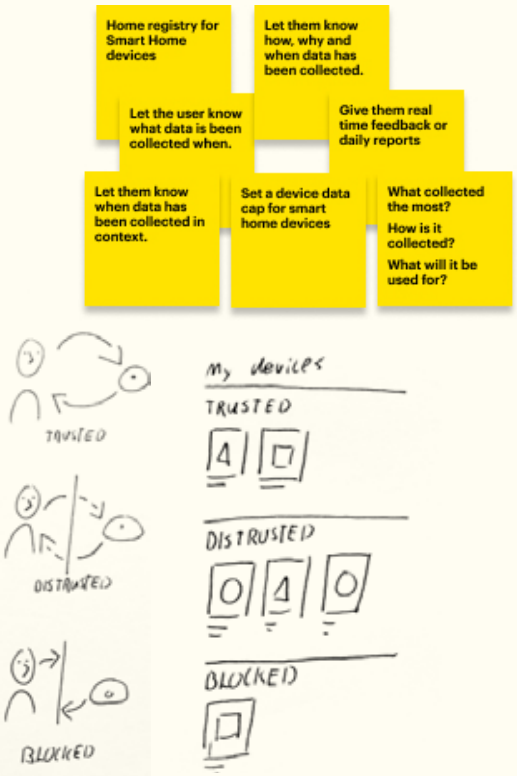
"When I am in the apartment I want to be sure no devices are spying on me so I can feel comfortable and in control"

# 3 - IDEATE

In the third stage of the process a good understanding of the users and their needs has been achieved. Brainstorming and research was used to generate several approaches to developing solutions for Rob and Liz (Dam & Siang, 2020).

## Brainstrom

Ideas were generated in quick succession on post it notes and sketching. These were evaluated on their suitability to answer the Jobs to be Done statements.

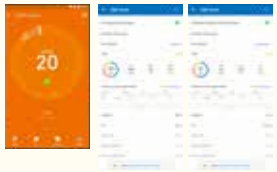



## Research

Research on other types of nudges in domain or non-domain contexts was used to inform ideation.

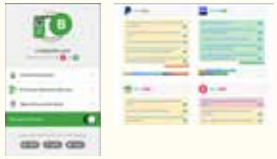
Food land energy labels

Energy and diet apps



IoT security project and Mozilla Privacy not included project

Duck Duck Go web privacy plugin and Terms of Service, Didn't Read project



A competitor analysis was carried out to identify features or patterns that could be used in the PPA.

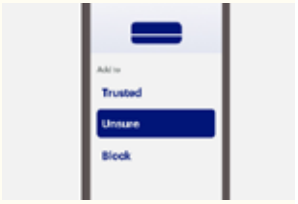

## Scenario

The most successful ideas of the brainstorm were formed into a narrative. This sets out a scenario that answers the jobs to be done statements.


**1 Rob sets up a new connected device.**


**2 The WiFi detects the new device on the network.**


**3 Liz get's notified by her PPA of the new device in the network.**




**4 She can decide what permissions the device is granted based on her privacy preferences.**


**5 She can review information about the device before she decides.**

**6 She decides she isn't sure, the device will ignore Liz unless she unlocks it.**

# 4 - PROTOTYPE
## LOW RES

In this phase a number of protypes were quickly produced focusing on specific features of the product. The protypes were iterated on and improved through informal testing (Dam & Siang, 2020).

### Features

The features of the PPA to be prototyped are based on research in the pervious stages. They are:

- Giving device information
- Assign device permissions
- Data access requests
- Giving data use context
- Giving pre-purchase device information

### Guerrilla testing

Participants were asked to complete tasks on a paper prototype using the guerrilla testing method (IxDF, 2016). The features they commented on are heighted in yellow, the comments are recorded below.

## Prototype 01


**How do I control them?**


**Is this me?**

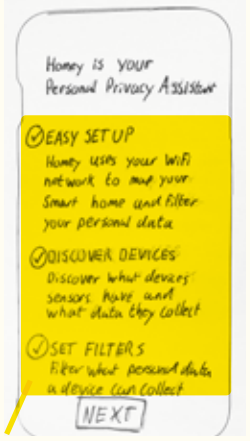

**These names aren't clear**


**Is this the refresh symbol?**

### User-Centered Design

The prototyping process followed a user-centred design methodology. This is a design process based on an understanding of users, tasks and environment (User-Centered Design, n.d.).

## Prototype 02




**Too much info**



**Titles still not clear enough**


**This isn't clear to me**


**Can I buy the device here?**

# 4 - PROTOTYPE
## HIGH RES

Through iterating the low-resolution protype a high-resolution digital protype was produced. This was split into two versions, one that would utilise privacy nudges and one that would not.

Homey

Be smart about your smart home data

A brand and tone of voice was developed for the app, it was named Homey.

FEATURE

## Device information

The PPA gives each device a responsible data rating. This is based on a rating system from Mozilla(2020).


The PPA with nudges uses colour to communicate the appropriate level of risk.

### Privacy nudges used

- Information
- Presentation


The version without nudges does not apply a colour system to the rating.

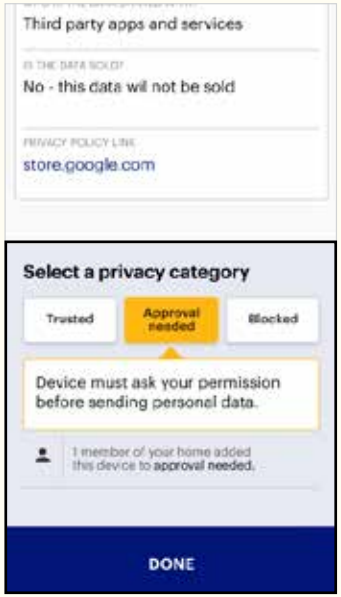
### Privacy nudges used

- Information

FEATURE

## Assign permissions

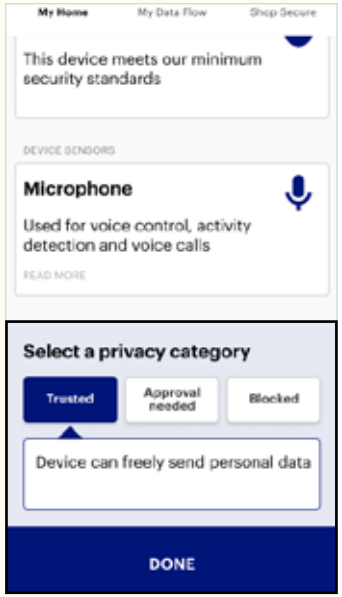
A user can place device in one of three buckets, Trusted, Approval Needed and Blocked. This dictates what permissions the device has.




The PPA with nudges has the default privacy category set to the responsible data rating. If other users in the home have rated this device it will also display their ratings.

### Privacy nudges used

- Information
- Presentation
- Defaults
- Incentives
- Reversibility




The version without nudges does not use defaults or show how other house members have rated the device.

### Privacy nudges used

- Information

FEATURE

## Data access request

Devices in the Approval Needed category must get consent from the user before they can access their data. This appears as a pop-up on their smart phone device.


The PPA with nudges uses information and hierarchy to give more detail about the interaction.

### Privacy nudges used

- Information
- Presentation
- Timing


The version without nudges just gives the request.

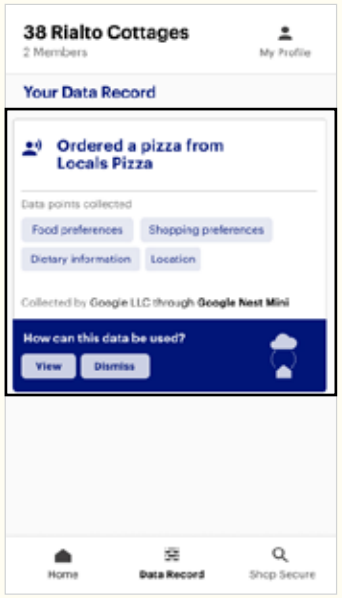
### Privacy nudges used

- Information
- Timing

FEATURE

## Data use context

The PPA will keep a record of all the data the user has shared. It records who it is shared with and gives the user insight into how this data could be used.




The PPA with nudges uses information and hierarchy to give more detail about the interaction and give context about how the users data could be used.

### Privacy nudges used

- Information
- Presentation
- Incentives
- Timing

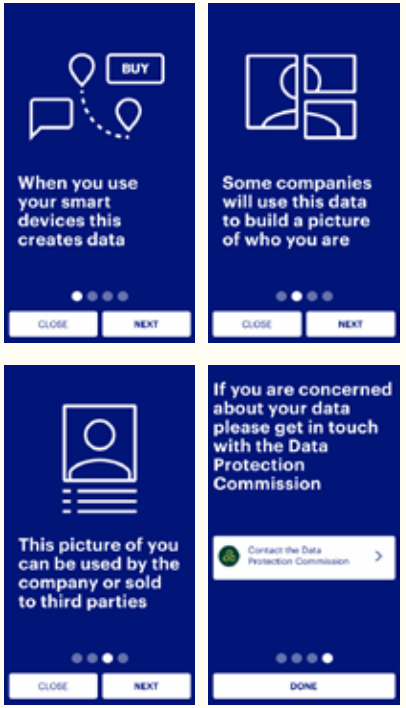

The version without nudges does not.

### Privacy nudges used

- Information

FEATURE

## Contextual information gallery




Information galleries were offered to users at key moments when using the app. These were an attempt to improve users understanding of how their data could be collected and used in context. These galleries were available in both versions of the app.

# 5 - TEST

In this stage the prototype PPA was tested using online testing software. The results of the test were used to answer the hypothesis set out in the Methodology section. The test followed the same procedure for both versions of the PPA.

The PPA's were randomly assigned to participants. The participants were asked to complete three tasks using the PPA and then fill out a 26-point scale to measure for trust and usability. This scale is adopted from the trust scale created by Flavián et al. (2006). The tasks useed images and text to create a scenario for the participant, they were then presented with a PPA to complete the task and then asked to fill out the scale.

## Participants

Participants were drawn from different sources. Some had taken part in the previously discussed quantitative questionnaire and indicated they wished to take part in this round of testing. Some were drawn from a group of students who agreed to take part in the testing.To be considered valid response, a participant had to pass the screener for the test:

- Be over 18 years of age
- Use smart home devices

### Task 01

Start using Homey and connect to the smart assistant

### Context

Your housemate has set up a new smart assistant. They suggested you use an app called Homey to manage it.

### Features Tested

- Device information
- Assign Permissions

### Task 02

Review the request from the device and decide if you will grant access


### Context

You use the smart assistant to buy lunch. Homey manages what data the assistant can access

### Features Tested

- Data Access Request
- Data Use Context

### Task 03

Homey alerts you of the update - decide if you will review it.

### Context

The manufacturer of your smart assistant has added a new feature and updated their privacy policy.

### Features Tested

- Policy Update Context

### Task 04

Use Homey to review and select a smart assistant for your friend.


### Context

Your friend thinks the smart assistant is really useful - their birthday is coming up and you want to surprise them with one.

### Features Tested

- Pre-Purchase Device Information

# RESULTS

## Quantitative testing

Participants were recruited and split into two groups; they each completed the same set of tasks using a PPA. One version of the PPA had privacy nudges and one did not. They then completed a Likert scale developed by (Flavián et al., 2006) to measure the levels of trust and usability between the two types of PPA. The final sample size that took part in the test was n=30. The results of the test were input into SPSS Statistics and mean between the two groups was determined using a series of t-tests and Mann Whitney tests (Pallant, 2010).

**The results of the test rule both hypotheses to be null.**

**H1** The PPA with privacy nudges will have a higher rating of trust than the PPA without privacy nudges.

In this case the presence of privacy nudges appears to have had no effect on the levels of trust, this hypothesis is null.

**H2** The PPA with privacy nudges will have a higher usability rating than the PPA without privacy nudges.

In this case the presence of privacy nudges appears to have had no effect on the levels of usability, this hypothesis is null.

## Qualitative testing

As Sadeh (2019) sates, a PPA is an emerging technology so would benefit from exploratory research (Hvas Mortensen, 2020). A second phase of qualitative testing was undertaken to explore users opinions on a PPA in general. This testing took place using a separate pool of participants but with the same screener as previously discussed. There were n=11 valid responses. These responses were analysed and coded using a thematic analysis. The codes were then applied to the responses, and themes were established (Rosala, 2019).

**Key themes that could prove areas for further investigation are:**

### Making personal data tangible

Some of the themes discussed earlier recurred. The idea that privacy concerns around data collection are not yet mainstream.

**"I think the whole concept is just a bit new, the idea of data as a commodity that we should protect".**

Connected device user
Female, early 30s

### Automation

Some participants questioned if they would continue to use the app long term, This could suggest that granting a PPA permission to make decisions on behalf of a user could be explored. Colnago et al., (2020) discuss this idea.

**"If I have to approve every interaction it could become tiresome".**

Connected device user
Male, early 30s

### Purchasing decisions

Several participants mentioned that the information provided by the PPA could affect which devices they purchase.

**"It would make me feel less suspicious of new device's, at the moment I feel like everything is taking my information all the time".**

Connected device user
Male, early 30s

## CONCLUSION

This pictorial contributes towards designing a more human-centred approach to data management, specifically in a smart home context.

It used the design thinking methodology to move towards developing an understanding of use for a PPA device, what features it may require and what design patterns the user interface would utilize.

This process has raised further questions around implementing a PPA from a technological and ethical point of view. For a PPA to be successful it would need to to establish itself as a credible and reliable source to its users.

As the quantitative questionnaire undertaken as part of this research revealed, most respondents were unsure about where to get information on how to protect their privacy. Some respondents believed that it was necessary for legislation to be introduced to protect user's data online. Further research would be necessary into how a PPA would fit into this possible landscape.

# REFERENCES


[1] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Giovanni Leon, P., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys, 50(3). https://doi.org/10.1145/3054926

[2] Benbasat, I., & Wang, W. (2005). Trust In and Adoption of Online Recommendation Agents. Journal of the Association for Information Systems, 6(3), 72–101. https://doi.org/10.17705/1jais.00065

[3] Bennett, J., Rokas, O., & Chen, L. (2017). Healthcare in the Smart Home: A study of past, present and future. In Sustainability (Switzerland) (Vol. 9, Issue 5). MDPI AG. https://doi.org/10.3390/su9050840

[4] Caltrider, J. (2017). 10 Fascinating Things We Learned When We Asked The World "How Connected Are You?" - The Mozilla Blog. https://blog.mozilla.org/blog/2017/11/01/10-fascinating-things-we-learned-when-we-asked-the-world-how-connected-are-you/

[5] Cannizzaro, S., & Procter, R. N. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. In PLoS ONE (Vol. 15, Issue 5). https://doi.org/10.1371/journal.pone.0231615

[6] Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L. F., & Sadeh, N. (2020, April 21). Informing the Design of a Personalized Privacy Assistant for the Internet of Things. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3313831.3376389

[7] Dam, R. F., & Siang, T. Y. (2020, November 21). 5 Stages in the Design Thinking Process | Interaction Design Foundation (IxDF). Interaction Design Foundation. https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process

[8] Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized Privacy Assistants for the Internet of Things An Infrastructure for Notice and Choice in the Internet of Things.

[9] Deloitte. (2016). Switch on to the connected home The Deloitte Consumer Review. http://www.deloitte.com/view/consumerreview

[10] Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020). Ask the Experts: What Should Be on an IoT Privacy and Security Label? http://arxiv.org/abs/2002.04631

[11] Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. Information and Management, 43(1), 1–14. https://doi.org/10.1016/j.im.2005.01.002

[12] Gulati, S., Sousa, S., & Lamas, D. (2018). Modelling trust in human-like technologies. ACM International Conference Proceeding Series, 1–10. https://doi.org/10.1145/3297121.3297124

[13] Harley, A. (2015). Personas Make Users Memorable for Product Team Members. https://www.nngroup.com/articles/persona/

[14] IxDF. (2016). 10 Hints for Carrying Out Better Guerrilla Usability Testing | Interaction Design Foundation (IxDF). https://www.interaction-design.org/literature/article/10-hints-for-carrying-out-better-guerrilla-usability-testing

[15] Man using his smartphone photo. (2021). Unsplash. https://unsplash.com/photos/Lrfw0U_o9I0

[16] Margot James. (2019). Plans announced to introduce new laws for internet connected devices - GOV.UK. Gov.Uk. https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices

[17] Mcdonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. http://www.is-journal.org/

[18] McKnight, D. H. (2012). Trust in Technology_TMIS_Final_0428.

[19] Mestrado, T. D. E., & Projecto, E. M. (2019). A review on Technology, Architecture, Applications, Challenges and Future Vision of Internet of Things. IET- Sri Lanka Network Standards, 5(5), 13783–13783.

[20] Nasajpour, M., Pouriyeh, S., Parizi, R. M., Dorodchi, M., Valero, M., & Arabnia, H. R. (2020). Internet of Things for Current COVID-19 and Future Pandemics: an Exploratory Study. Journal of Healthcare Informatics Research, 4(4), 325–364. https://doi.org/10.1007/s41666-020-00080-6

[21] Pallant, J. (2010). SPSS Survival Manual Survival Manual. www.openup.co.uk/spss

[22] Paradiso, J. A., & Siewiorek, D. (2020). Attention Paid Versus Paying Attention in Pervasive Computing. IEEE Pervasive Computing, 19(2), 8–12. https://doi.org/10.1109/MPRV.2020.2986903

[23] Sadeh, N. (2019). Personalized Privacy Assistant Project. https://privacyassistant.org/

[24] Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. Big Data and Society, 6(1). https://doi.org/10.1177/2053951718820549

[25] Securing IoT. (2019). The Economist Intelligence Unit .

[26] Story, P., Smullen, D., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2020). From Intent to Action: Nudging Users Towards Secure Mobile Payments. https://www.usenix.

org/conference/soups2020/presentation/story

[27] User-Centered Design. (n.d.). Usability.Gov. Retrieved April 11, 2021, from https://www.usability.gov/what-and-why/user-centered-design.html

[28] Williams, M., Nurse, J. R. C., & Creese, S. (2017). Benefits and risks of smart home technologies. Energy Policy, 103(December 2016), 72–83. https://doi.org/10.1016/j.enpol.2016.12.047

[29] Woman in black fur coat and orange knit cap. (2021). Unsplash. https://unsplash.com/photos/-YVR-PBSSsXc

[30] Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW). https://doi.org/10.1145/3274469

[31] Ziefle, M., Röcker, C., & Holzinger, A. (2011). Medical technology in smart homes: Exploring the user's perspective on privacy, intimacy and trust. Proceedings - International Computer Software and Applications Conference, June 2014, 410–415. https://doi.org/10.1109/COMPSACW.2011.75

[32] Zuboff, S. (2019). The Age of Surveillance Capitalism. Public Affairs.