opaque

Background Request
Camera
Uncertified
Ambient
Microphone
Health
3rd parties
12875

Executive Summary

By 2040, almost all of the average consumer's daily activities will be supported by products and services developed by a select set of major technology companies. Their schools, workplaces, healthcare systems, retails stores, and transport networks, will be tied together by these firms connected systems. These companies will use this to record consumers' every physical and digital action to develop ultra-high-fidelity models of their interests, personalities, and behaviours.

They will use these models to make decisions about them. Insurance premiums, mortgage rates, job opportunities, priority in healthcare systems, access to education and so much more will be decided by the models these firms have created. Knowing that their every action could affect their future prosperity will cause consumers great stress and anxiety – and lead them to crave a safe space from invasive data collection.

With governments, organisations, and employers integrating technology firm's connected services into every aspect of a consumer's life, the home will be the last domain the average consumer can escape this data collection. However, technology firm's will be pushing into this domain too - by launching new home and personal devices, linked to their services, that offer consumers unimaginable utility and convenience but sacrifice this last private domain.

Therefore, Opaque's aim is to let consumers reap the benefits of 2040's technologies, whilst securing the home of 2040 as a safe space from invasive data collection. To do this we conceptualised an entirely new product – a complete home privacy system called the Opaque Dial.

Throughout the last 8 weeks we have refined this concept, validating it with experts, and developing and testing a set of features to help consumers understand, control, and minimise their home data leakage. We researched which 2040 technologies could be used to support its features, created a plan for how the concept could become a viable business, and proposed how we could make Opaque a trustworthy name for consumer privacy.

Finally, we embodied this concept to create an online demo and video to demonstrate it's features to consumers. This portfolio outlines our development and highlights how the Opaque Dial's key features can help consumers understand, control, and minimise their home data leakage to secure their homes as a safe space from invasive data collection.

Opaque Demo: https://opaque.house

Opaque Video: https://www.youtube.com/watch?v=SHrgTPzX9E0

Developed by: Oliver M. Colebourne (01500345), Alexander C. Gibson (01506897), Theo M. Kane (01504329), Patrick D. McGuckian (01508175), & Jack J. A. Polturak (01544289).

With Thanks to: Dr Nejra Van Zalk & Dr David Boyle.

Introduction

Concept Design & Engineering

A Privacy Business

The Opaque Dial

Future Scenario

Where are we now?

To use Facebook and Google's 'free' services, users are having to give up their data privacy [1]. By recording user's every action, these firms are building up detailed models of their behaviour and using these to hyper-personalise services to increase engagement and monetise user attention. This approach to driving user engagement is being emulated by firms with non advertising-based business models - meaning almost every action a user takes online is being used to build detailed models of their behaviour.

High profile scandals like Facebook and Cambridge Analyitica influencing the 2016 US election [2] and trending documentaries like Netflix's The Social Dilemma mean consumers are slowly starting to wake up to the extent of this invasive data collection. Governments are starting to clamp down on this new 'surveillance capitalism' - with the EU introducing GDPR, and the US's ongoing antitrust case, against Google. While some technology firms are starting to sell a 'privacy premium' - like Apple introducing numerous privacy measures in iOS (e.g. data collection opt-in and privacy labels) in tandem with a highly publicised media campaign criticising data collection of firms like Facebook [3].

Where are we going?

Despite a growing resistance to our loss of privacy, big tech's data collection will continue to grow - spilling out of online platforms into new physical domains [1]. Digital assistants will tie together every aspect of a consumer's life including work, health, transport and education - providing so much utility that the users won't be able to opt-out. Firms will continue to build their portfolio of connected products and services by buying niche companies with strategic and valuable user data (e.g. Google acquiring Fitbit). All of this leads to a small set of major firms having an incredibly complete view of a users behaviour and personality - which will be used to make decisions that affect user prosperity. This could include our insurance premiums, what products we buy, our access to education and health care services, or job opportunities.

These firms having so much control over our prosperity will raise eyebrows among governments. However, their services will become so ingrained into our daily life that they won't be broken up. Instead, ever-increasing regulation will attempt to curb their data collection abilities. To survive, firms will innovate around the problem by developing new strategies and technologies to infer similar information [1].

What do consumers feel?

By 2040 the average consumer will be more savvy to their data being collected and more concerned about the impacts it could have on their prosperity. These concerns can be generalised into three categories:

1. Finance: Some may think twice about how their devices could affect their personal finances (e.g., being concerned that health monitoring services may increase their health insurance premiums).
2. Opportunity: Some may worry that their private offline behaviour may affect their future opportunities (e.g., private conversations recorded by smart speakers may decrease an 'employability score' given by recruitment companies).
3. Security: High-profile figures may have concerns that highly sensitive information could leak to the public (e.g., Politicians may be concerned a hack could release home security camera recordings exposing confidential information on government affairs)

Knowing they are continuously monitored - the constant concern that their trivial actions may effect their future prosperity will cause consumers significant stress and anxiety. Users will crave a safe space from invasive data collection to protect their 'privacy health'.

Home of 2040

With governments, organisations, and employers integrating technology firm's connected services into every aspect of a consumer's life, the home will be the last domain the average consumer can control. However, these firm's will be pushing into this domain too - by launching new home and personal devices, linked to their services, that offer the user unimaginable utility and convenience. A modern home would contain so many intertwined connected devices - manually adjusting each of their privacy settings would be infeasible. Therefore if the user chooses to incorporate them they will be sacrificing their last private domain.

Serving Inhabitants

Appliances will automate previously manual and time consuming tasks (e.g., a kitchen robot cooking meals).

Personalised to Inhabitants

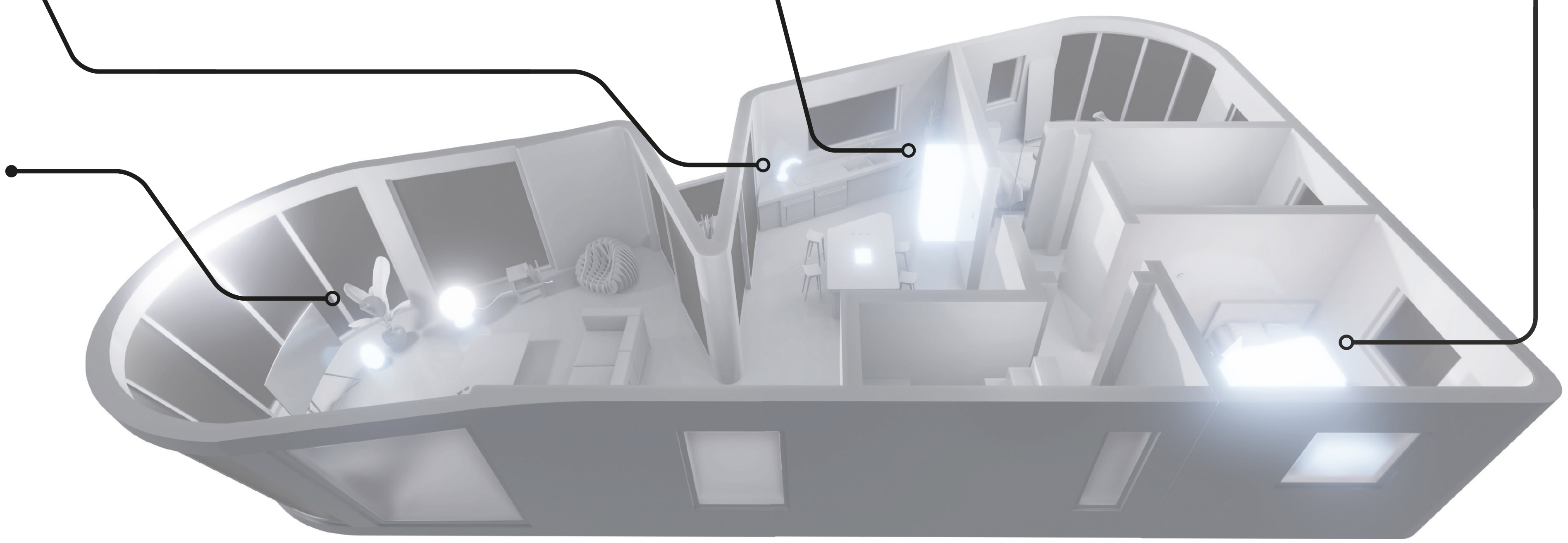
Devices will keep the home in the ideal state for the user (e.g., a smart fridge predicting what a user will want to eat assuring it is stocked).

Connected

Data will be shared between the users personal devices and the homes smart appliances to facilitate these complex processes.

Optimising Health & Wellbeing

Devices will monitor user's biometrics to improve their health and well-being (e.g., a smart mattress changing the air temperature to improve sleep quality or a wearable changing light intensity and music being played to reduce stress levels or increase productivity).



[1] Colebourne O, Gibson A, Kane T, McGuckian P D and Polturak J . *DE3 Futures - December 2020. Hide & Seek 2040 - Interim Report - Group 08.*
[2] Confessore N. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times.* Available from: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [Accessed: 11th March 2021]
[3] Taylor J. *Facebook v Apple: the looming showdown over data tracking and privacy. The Guardian.* Available from: https://www.theguardian.com/technology/2021/feb/14/facebook-v-apple-the-looming-showdown-over-data-tracking-and-privacy [Accessed: 11th March 2021]

Aims and System Diagram

The impact invasive data collection could have on consumer's future prosperity will cause them great stress and anxiety. The 2040 home will be the last domain a consumer can avoid this data collection. However, opting-out of modern smart home systems means living without life changing utility. Consumers will be stuck choosing between this incredible utility and their privacy health. Our intervention aims to solve this problem - letting consumers reap the benefits of 2040's technology while maintaining their home as a data privacy safe space to preserve their 'privacy health'. To achieve this we have broken the problem down into three aims:

01 Understand

The system should help the user understand the current state of their data privacy, by showing them how much of their data is leaking from the home, and which devices or services are responsible. This will give them peace of mind if data leakage is low, or highlight what steps should be taken to limit exposure if data leakage is high.

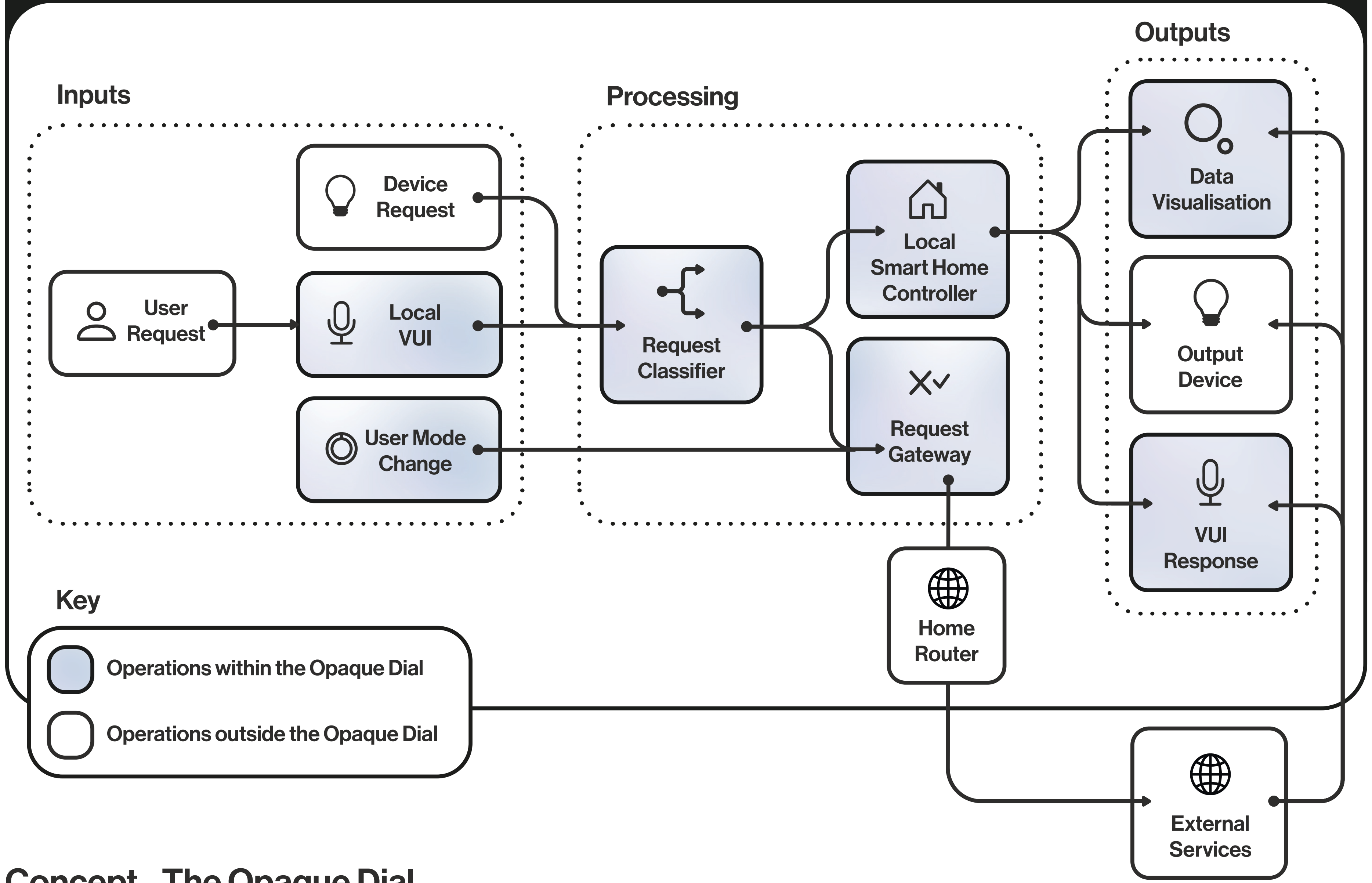
02 Control

With this understanding, the system should allow the user to control what data can and cannot leave the home - turning the complex task of controlling each of their devices privacy settings into an effortless action that can be done rapidly based on their current activities. This will give the user a sense of control over their privacy and facilitate a 'privacy detox'.

03 Minimise

The system should minimise the quantity and richness of data leaving the home. It should complete requests locally wherever possible - allowing for some of the home's utility to be maintained during a detox. If data does need to leave the home the system should apply cutting edge privacy enhancing technologies (PETs) to anonymise any request.

System Diagram



Concept - The Opaque Dial

During our ideation, we noted a single intervention would not be able to meet all of our aims. Thus, our concept is a complete smart home privacy system - with three sub-systems working in tandem to meet our requirements:

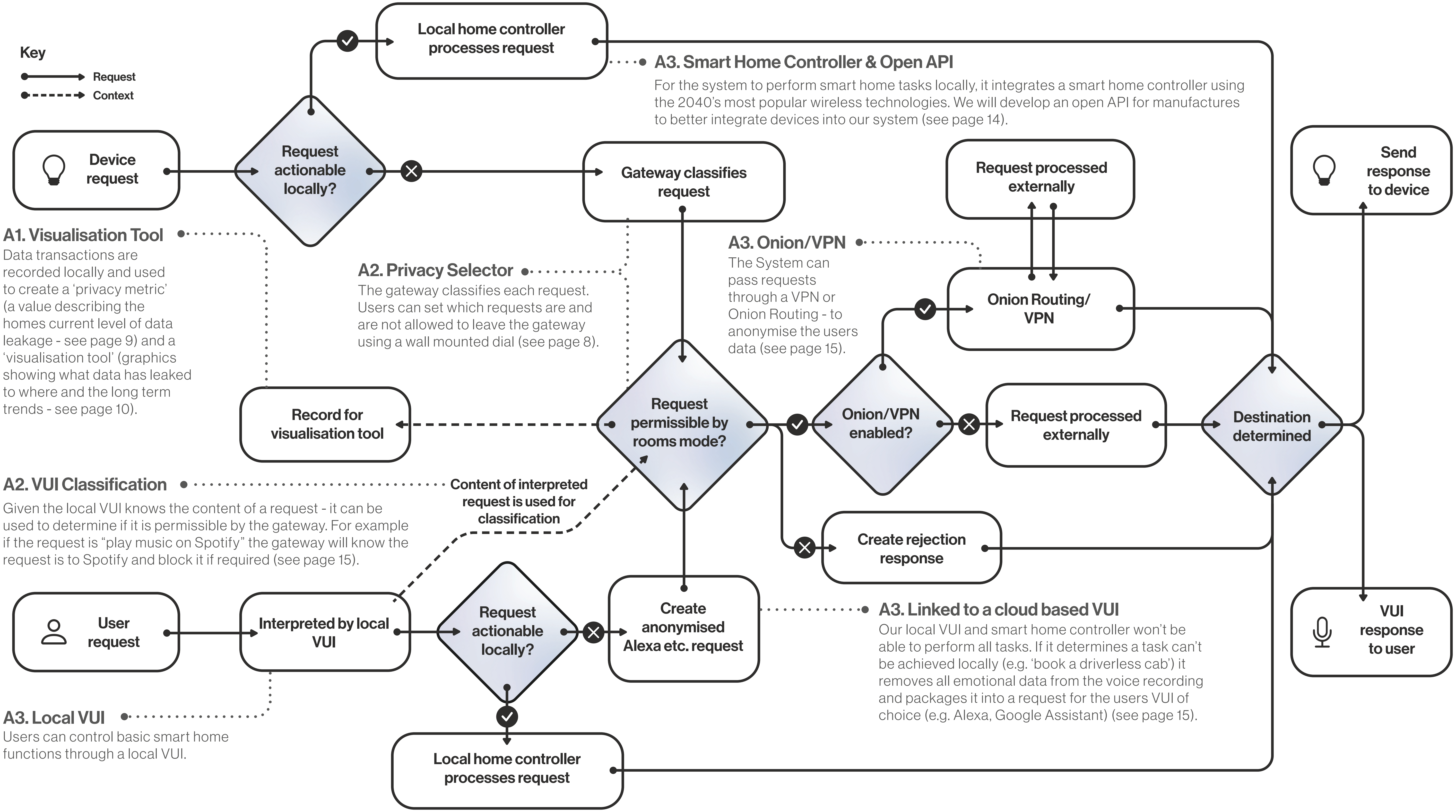
- Visualisation Tool: A system to record and display what data is leaving the home in a clear, understandable, and intuitive way (aim 1).
- Privacy Selector: A system to rapidly control what data is and is not allowed to leave the home in a single action (aim 2).
- Local Voice User Interface (VUI) & Smart Home Controller: A system to control basic smart home functions locally without data leakage (aim 3).

These three sub-systems are combined together into our concept - the Opaque Dial. The system connects to the existing home network and all other devices in the home connect to it, instead of directly to the homes network. This gives it complete visibility and control of all of the data requests occuring in the home - allowing each sub-system to work.

Data Flow

One System to Understand, Control, and Minimise Data Exposure

With our concepts features finalised we needed to consider how they could be combined into a single system capable of handling any device or users VUI request. Data leakage can be caused by both smart home devices and personal devices (e.g. AR Glasses) that users bring into the home - therefore our system must account for both. To achieve this we considered how a local VUI or home/personal device request could move through the system and interact with the various technologies when required, and created a single flow chart to map this process. This system was later validated by privacy experts Anna Maria Mandalari and David Boyle (see page 14).



Key

- Request
- Context

Device request

Request actionable locally?

✓ Local home controller processes request

✗ Gateway classifies request

Request permissible by rooms mode?

Record for visualisation tool

✓ Onion/VPN enabled?

✓ Onion Routing/ VPN

Request processed externally

✗ Request processed externally

✗ Create rejection response

Destination determined

Send response to device

VUI response to user

User request

Interpreted by local VUI

Request actionable locally?

✗ Create anonymised Alexa etc. request

✓ Local home controller processes request

Content of interpreted request is used for classification

A1. Visualisation Tool

Data transactions are recorded locally and used to create a 'privacy metric' (a value describing the homes current level of data leakage - see page 9) and a 'visualisation tool' (graphics showing what data has leaked to where and the long term trends - see page 10).

A2. Privacy Selector

The gateway classifies each request. Users can set which requests are and are not allowed to leave the gateway using a wall mounted dial (see page 8).

A3. Smart Home Controller & Open API

For the system to perform smart home tasks locally, it integrates a smart home controller using the 2040's most popular wireless technologies. We will develop an open API for manufactures to better integrate devices into our system (see page 14).

A3. Onion/VPN

The System can pass requests through a VPN or Onion Routing - to anonymise the users data (see page 15).

A2. VUI Classification

Given the local VUI knows the content of a request - it can be used to determine if it is permissible by the gateway. For example if the request is "play music on Spotify" the gateway will know the request is to Spotify and block it if required (see page 15).

A3. Linked to a cloud based VUI

Our local VUI and smart home controller won't be able to perform all tasks. If it determines a task can't be achieved locally (e.g. 'book a driverless cab') it removes all emotional data from the voice recording and packages it into a request for the users VUI of choice (e.g. Alexa, Google Assistant) (see page 15).

A3. Local VUI

Users can control basic smart home functions through a local VUI.

Concept Validation

Accreditation from the Information Commissioner's Office

What is the ICO?

Before we began our design and engineering concept development process - we wanted to validate our future scenario and system concept. Therefore, we met with Ali Shah of the Information Commissioners Office - the U.K.'s independent body to uphold information rights. The ICO has a number of roles including: assisting government in developing the U.K.'s data privacy laws, working with companies to assure they handle consumer data properly; auditing companies to see if breaches have occurred; and, if so, issue fines of 4% of global revenue [4].

Ali is the Head of Technology Policy. He is responsible for ensuring the ICO can respond to complex societal challenges presented by emerging technology developments.

Ali Shah ICO

Thoughts on our Concept

Ali agreed that our focus on securing the home as a safe space from privacy invasion was a realistic yet effective intervention to 2040's privacy problem. He believed meeting our key aims of Understand, Control, and Minimise would be key to it's success; and the privacy selector will allow users to think more critically about the privacy utility trade-off balance.

He made it clear to us that our system can't rely on support from device manufacturers. Companies with data collection based revenue streams will not want to support a system that exposed the extent of their data collection. Therefore the core of our system should work with any connected device regardless of any manufacturer support.

Ali gave us a few points to consider when developing the project:

01 He discussed the possibility about how the product could be designed to work with young children - educating them on data privacy and encouraging them to make more informed decisions.

02 He encouraged us to consider the situation of a 'guest bedroom'. Who should control the data entering and leaving the house - is it solely limited to the home owner.

03 He questioned how this system would work in a shared house setting - where members of a household may disagree on what utility should be sacrificed

04 He stressed the importance of designing our system to collect as little user data as possible. Even if it is stored locally - this would be critical to instilling a sense of trust among consumers

Thoughts on our Future Scenario

Though he remains optimistic about the future, he validated our future scenario - believing what we had scoped was realistic. He agreed with our assumption that 2040's consumers will have an inherent mistrust in organisations and their use of user data; and that it will become more common for consumers to consider the utility privacy trade off when deciding which services to use - stating that he could already see the shift towards this.

He also validated our assumption that regulatory bodies will struggle to keep up with technology companies. Stating that his small team was up against thousands of the world's top engineers and business strategists. Their current approach is to set up privacy guidelines as an architecture for companies to follow instead of guidelines to stick too - however, companies can always get around these by designing in the 'fuzzy' areas at the edge of the guides.

In conclusion, he was confident our system would be valuable to 2040's consumers as it was unlikely the privacy problem would be entirely solved by future regulation

Development Plan

With our future scenario and idea validated we felt confident to begin our design and engineering concept development process. In this document, and supporting video and web demo we aim to take the our idea and develop it into a comprehensive considered intervention to the outlined problems. Our intervention is set for the world in 2040 - addressing 2040's problems with 2040's technology. It is a highly complex product, and would require a large team of highly skilled technologists and designers to make. Therefore, we will focus on:

01 Demonstrating the potential of the system to solve the problems outlined.

02 Design the features, behaviour, and experience of the final system.

03 Embody the constituent components for the purposes of demonstrating the project and testing its proposed functionality on users.

04 Outlining what factors would need to be considered when the full product is developed.

05 Demonstrating what technologies currently in development could be used to achieve the final systems functionality.

06 Outlining how we could build a viable business around the concept.

07 Explore how we could build a brand that users could trust with their data.

[4] *Information Commissioner's Office. Wikipedia.* Available from: https://en.wikipedia.org/wiki/Information_Commissioner%27s_Office [Accessed: 11th March 2021]

Discretising Privacy I

Giving Users Control

The privacy selector is the part of the system aiming to give the user a sense of control over their data privacy. The hardware and UI are explored on pages 11-13. First we need to define how we can break down an entire home's data leakage into settings that can be rapidly adjusted with a simple interaction in a way that is intuitive, meaningful and useful to the user. Design constraints:

01 When a user adjusts the privacy settings they must understand what functions are and are not going to work. If a device critical to a consumer's routine (e.g. a smart fridge reordering groceries) stops working without their knowledge they will be frustrated and not use the system in the future.

02 The privacy settings must be useful - with realistic scenarios where users would pick one over another.

03 The privacy settings must give users complete control over their privacy - not limiting them to settle for unnecessary data leakage to keep utility as there is no setting to cover their needs.

Understanding User Need

We needed to discover what the users of 2040 would want from the privacy selector. Given we expect 2040's consumers to have a significantly different perspective on data privacy compared to today's consumers (see page 3) - we are unable to gain this information from 'normal' members of the public.

Therefore, we chose to focus on today's extreme users: those who are most aware of the extent of data collection and the implications it could have on their future prosperity; and those who are most familiar with smart home technology. So we posted a survey in the Reddit r/privacy and r/smarthome groups. These were people we didn't know - meaning our results wouldn't be swayed by acquaintance bias. In total we had 44 responses. They were shown a 2 minute unbiased video about our future scenario and asked to respond based off this situation. Questions focused around what their key privacy concerns were and what control they would want from our system. Some of our key insights include:

01 Respondents showed more concern over what type of data is being collected over who was collecting it.

02 Respondents were on average more concerned about certain types of data (e.g., audio) than others (e.g., health), but there was a large variation in response.

03 Most respondents were more concerned about data collected in certain situations than others.

04 Overall the concerns were varied, showing a need for a system users could customise.

Concept - Scenario Based Privacy Mode

Our initial concept was to use a device rating service like Mozilla's *privacy not included [5] to rate each product's privacy as a percent. Users could then set a minimum privacy percent and all products that scored lower then this would be switched off. This was quickly abandoned as it failed design constraint 1. We also considered a level system where users could assign devices/services to off after a certain level - however we dropped this as it would require users to spend a lot of time setting these up - which we felt would have been enough friction for users to abandon the system and if new devices were added they wouldn't be covered by existing settings.

The idea that offered the greatest user added value in the most initiative form was 'Privacy Modes'. We would define heuristic data categories such that users would be able to easily identify which device requests would fall into each category. These categories can then be bundled together into different 'modes' that the user can switch between based of their current context. When a given mode is on the system would block any requests that fall into the constituent categories.

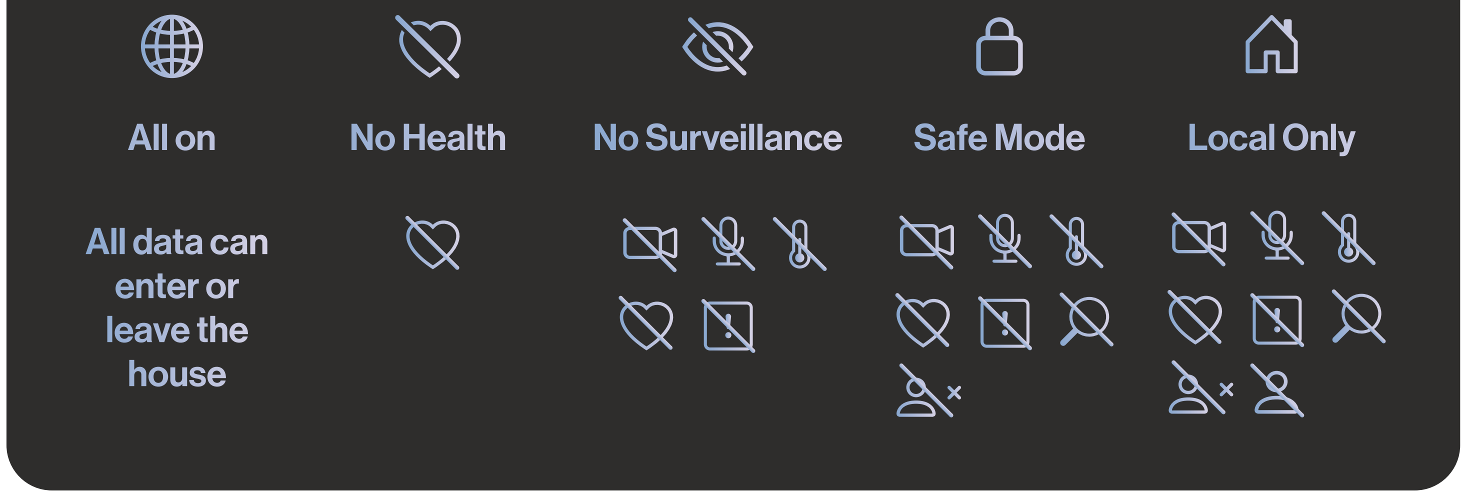
Data Categories to Build Modes

We researched what request categories it would be feasible for our gateway to classify and block (see page 8). We then used some of the findings from the survey and took inspiration from Apple's privacy labels to determine which of these would offer the greatest value to the user while being clear what requests would be permissible when activated - creating a finalised list that can be combined into modes:

Camera · Mic · Ambient · 3rd Parties · Background · User · Uncertified (see page 16) · Health

'Out of the box' Modes

We wanted our system to be useful without users having to invest significant time setting it up. Therefore we defined a set of out of the box modes by imagining what a typical 2040 day looks like - an example of this can be found on page 19. The modes were designed to be progressive - from least private to most private to give the user the feeling of turning up privacy as they scale through modes:



[5] *Privacy Not Included: A Buyer's Guide for Connected Products. Mozilla Foundation. Available from: https://foundation.mozilla.org/en/privacynotincluded/ [Accessed: 11th March 2021]

Discretising Privacy II

Testing Privacy Modes

With the privacy modes concept defined we wanted to test it on users to make sure it fit within our design constraints. With our testing we wanted to answer three questions:

01 Can the user predict which requests are and are not permissible in the different modes?

02 Are the iconography and category names clear?

03 Are the default modes useful?

To answer these we developed an online interactive demo to run through with users remotely. This demo contained a typical 2040 house with different rooms containing various devices all connected to the Opaque Dial system. Users could select various smart home device 'prompts' - e.g. "Health monitor sends message locally to smart blanket to lower temperature" and change the privacy modes to see if a given request would be permissible. Our test was run in two parts:

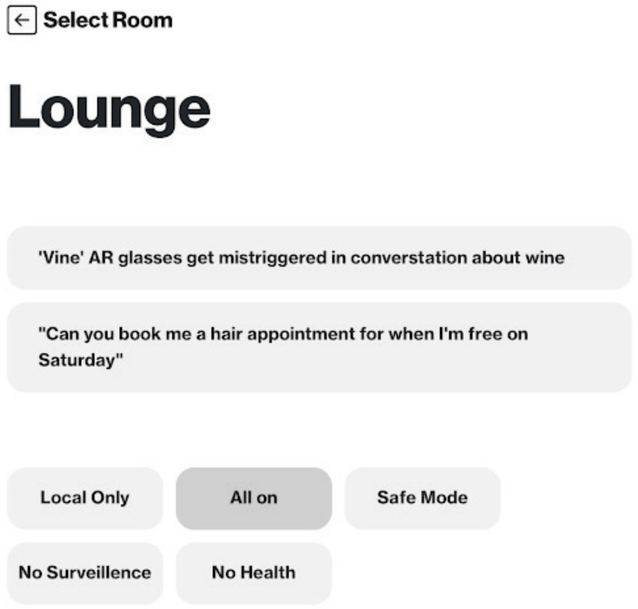
A Questions 1 & 2: Each participant was asked to go through each mode for every 'prompt' and predict whether the request will be permissible or not - a pass or fail was recorded for each case. If a participant failed, they explained their thought process to help us understand why it wasn't clear.

B Question 3: After users had explored the system, we asked them what mode the user would select for a few different typical home situations. This allow us to identify if there was a true need for all of the modes.

The results of this testing were positive, showing our concept of privacy modes is clear, useful and intuitive - meeting our constraints and overall aim of giving users control over their data leakage. Our out of the box modes and categories have shown to be useful - with only a few small changes being made to make them more clear. Ahead of product launch much more extensive user testing would be performed to assure the data categories and out of the box modes are relevant for life in 2040.

Online Demo

Link: https://opaque.house



Select Room

Lounge

'Vine' AR glasses get mistriggered in converstation about wine

"Can you book me a hair appointment for when I'm free on Saturday"

Failed Prompt	Modes	Reason for Incorrect Prediction
Health monitor communicates with smart mattress.	Local mode & Safe Mode	Users did not understand that this request could be completed locally.
'Vine' AR Glasses miss-triggered when discussing wine.	Safe Mode	Users did not understand that in 'Safe Mode' only active user requests are permissible.
"Can you book a hair appointment for Monday?"	No Surveillance	Participants failed to realise our local VUI can perform requests even when the audio category is blocked.
Kitchen helper looks online to find a recipe.	No Surveillance	Participants assumed kitchen helper would have some form of sensory technology and would be inactive in 'No Surveillance'.
Fridge uses camera and reorders what has run out.	Safe Mode	Users did not understand that in 'Safe Mode' only active user requests are permissible.
Smart mirror checks calendar and chooses an outfit.	No Surveillance	Participants assumed the smart mirror would have some form of sensory technology and would not be active.

Results

In part A only 7.53% (29/385) of cases were predicted incorrectly. A description of each failed prediction is given in the table above. The key insights gained and changes we made are:

01 Users sometimes struggled to realise when an action could be performed locally - meaning they would assume a device wouldn't work when it would. This wouldn't lead to the problems outlined in design constraint 1, and as the action is local - no sensitive information would leak as a result of this mistake. However, it means users may opt for a less private mode then necessary. Our concept for addressing this is to create certification labels to show product supports our local Smart Home system (see page 16).

02 The functionality of 'Safe Mode' was unclear - therefore it was renamed 'User Only' mode which participants found to be more intuitive.

The results from part B were also promising. It was performed in a discussion format and the participants showed clear value in all of the modes and the general privacy selector concept. Some surprising insights include:

01 When discussing an intimate dinner party respondents chose either "No Surveillance" to insure their conversation wasn't recorded or "Local Mode" but not for privacy related reasons, commenting: "I wouldn't want anyone distracted by their phones" - using the privacy selector as a 'Digital Detox' tool is an interesting use-case we would further explore in later development.

02 Some brought up the opportunity the system could have for parents - similar to what Ali was suggesting. Saying the system could be used to turn of internet access to children's rooms to limit screen time.

Visualising Privacy I

Visualisation Tool Requirements

The visualisation tools needs to display user's data leakage to help them understand how their actions affect their data privacy. To begin our development we considered how we wanted users to use the system - what information we want them to pick up and what action we wanted them to take in different scenarios. Based off this we created three 'how might we' (HMW) statements to guide our ideation:

01 HMW display a user's total current data leakage in an 'at a glance' format that allows them to determine if they need to make any changes to the privacy mode.
02 HMW break down current data leakage so users can understand which activities are particularly invasive to make informed choices when changing the privacy mode.
03 HMW show the impact of changing behaviours and switching privacy mode on long term data privacy.

HMW1 will be addressed on this page. We believed the best way of achieving this is with a privacy metric - a number that is reflective of the volume and type of data being leaked by the home. This was inspired by a smart energy meter. We defined a set of design constraints. The metric must:

01 Indicate the extent of all data currently entering and leaving the home.
02 Indicate a decrease in data leakage when more restrictive privacy modes block data transactions.
03 Be easily understood without a high level understanding of data privacy.

Ideation and Survey

To develop a metric that can be easily understood by consumers with limited privacy knowledge, we needed to know the 2040 consumer's level of privacy understanding. We used information from the survey outlined on page 7 as a foundation and ideated three potential concepts, which were tested by interviewing potential users to determine the most suitable. This testing was done with a similar group to the privacy modes testing and thus had similar limitations.

Privacy Percentage

86%

0% privacy represents a state where all data transactions are permissible - 100% represents a state where no data is being leaked.

Feedback:

Users found determining when action was needed easy. However,it failed constraint 1 as it only takes into account proportion blocked - not extent of leakage. If the system has one connected device sending data it would be 0% - but if it had 100 devices with 50 blocked it would be a 'better' 50%.

Weighted Sum of Data Transactions

1265

Each request category is allocated a weight based on it's invasiveness. Transactions are multiplied by their respective weights and summed.

Feedback:

Once shown a few examples users found it clear when overall levels were high - determining when action needed taken was intuitive. However, users felt the value wasn't heuristic - initially it appeared to be arbitrary and constantly changing and took a while to get a feel for what's high or low.

Privacy Currency

P42

Privacy displayed as a currency representing the monetary value of your data to the firms collecting it.

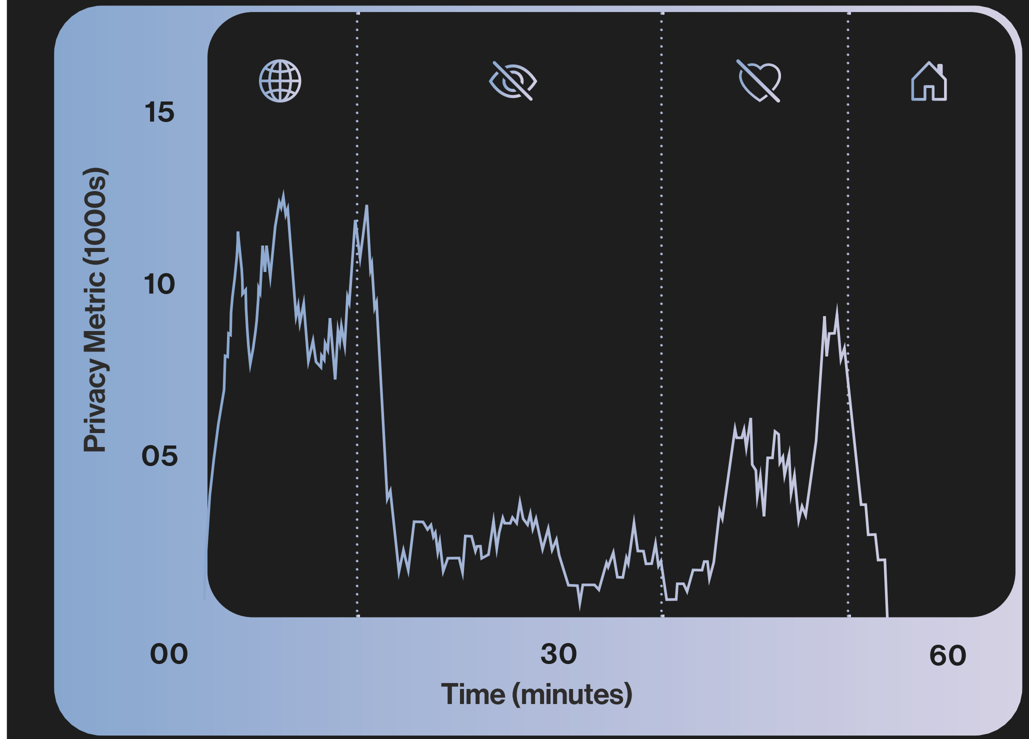
Feedback:

Provides an urgency for privacy as users equate their privacy with a monetary value. However, some users felt it counter-intuitive - the more data shared, the 'richer' they were becoming. Furthermore assigning a value to data transactions would be near impossible.

Metric Behaviour Prototyping

We believed the 'Weighted Sum' most successfully fulfilled our requirements, so was selected for further development and prototyping. Given the nature and volume of a home network's data requests will significantly change between now and 2040 developing a working model wouldn't help prove our concept. Therefore, our research focused on what metric behaviour would be the most clear and action inducing for users. To simulate the behaviour we developed a prototype of the metric coded in Python.

How the prototype works



The Python code simulates requests passing through the system. Requests are randomly assigned, at a set rate, to one of our systems categories (see page 7). We defined an initial weighting for the sake of testing, based on how invasive we personally felt the data type was. This was then all combined into a metric representing the total privacy level for a given time period. We then simulated the privacy selector - blocking the data transactions depending on which mode is set. The metric was then plotted across time.

We experimented with different time periods and weights - changing the rate of requests to test it's behaviour. We concluded a time window of 10 minutes would give a good picture of the data leakage caused by a users current activities as it wasn't heavily affected with perturbations but still fell or increased rapidly enough to give a satisfying feedback when modes are changed. Secondly we believed the weights should be tuned such that the 'average' home set to the "all on" mode should have a value roughly 10,000. This gives enough variance when new devices/transactions. Finally we felt the value should update once every one second to give the feeling of a live value without it being hectic.

Conclusion

We believe the concept and behaviour we have defined is an intuitive representation of a households live data leakage that would be action inducing in the event of a high level of data leakage. The key issue with this concept is the subjective nature of defining weights based on invasiveness. Most would agree that hospitals collecting pacemaker data to predict a heart attack is positive but Facebook collecting user data to target adverts is negative - however everyone will define the line between them at a different point. We would propose an engaging setup quiz, inspired by Apple Music, to determine where this line is for each user to assign custom weights. This would require a team of highly skilled psychologists and was beyond the scope of the project.

Visualising Privacy II

Graphically Breaking Down Data Leakage

The obvious medium to deliver HMW's 2 and 3 is through an application on the most popular 2040 personal devices (e.g. AR glasses). However, based on Ali Shah's advice, to show the user we are minimising any collection or sharing of user data, we wanted to avoid having any information shared between devices. For this reason, all visualisation tools will be displayed on the device only.

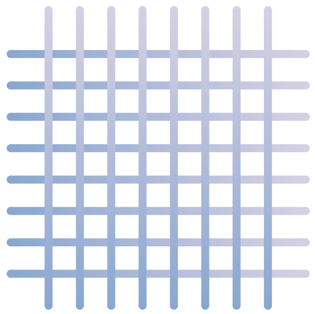
HMW2 - Ideation

To achieve HMW2 we wanted to develop a graphic to give an intuitive, actionable method of analysing data transactions. This was inspired by Apple's activity rings. Design requirements:

01 Demonstrate to users the breakdown of their data leakage
02 Encourage users to increase privacy levels when specific utility isn't required
03 Help users understand why changing levels was beneficial to user their privacy.

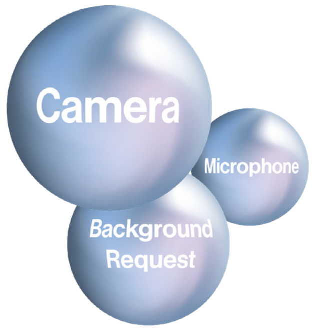
We ideated a number concepts on how we could visually break down the privacy metric into it's different data types that would allow the user to make good mode change decisions (see below). It was decided that the Volume Bubble Graphic was the most effective method of portraying both the user's overall privacy and a clear breakdown of what data categories are most highly impacting the metric. Each data category has a bubble with a volume that corresponds to the number of weighted data transactions, so the user can see relatively which specific types of data are most contributing to the privacy metric.

Filter Density Graphic



The more requests that are blocked - the denser the filter. If no data is leaking, the graphic will be a solid wall. Regions are colour coded based on data types.

Volume Bubble Graphic



Data categories are represented by bubbles. Their size represents their relative proportion of total leakage. These float around passively to build engagement.

Blur Opacity Graphic

The more requests that are blocked the more blurred the image, signifying a block in data transactions. Regions are colour coded based on data types.

User Testing Procedure

We wanted to user test the bubbles system to assure it would present all the information required to make informed choices when changing the privacy modes in a clear and intuitive way. We added in a simulation of the metric and bubbles to our online interactive demo to test it with users. Our test was to outline a typical situation (e.g. you are watching TV while scrolling through your social media) and asked participants if they would want to switch their mode and if so which mode they would switch to.

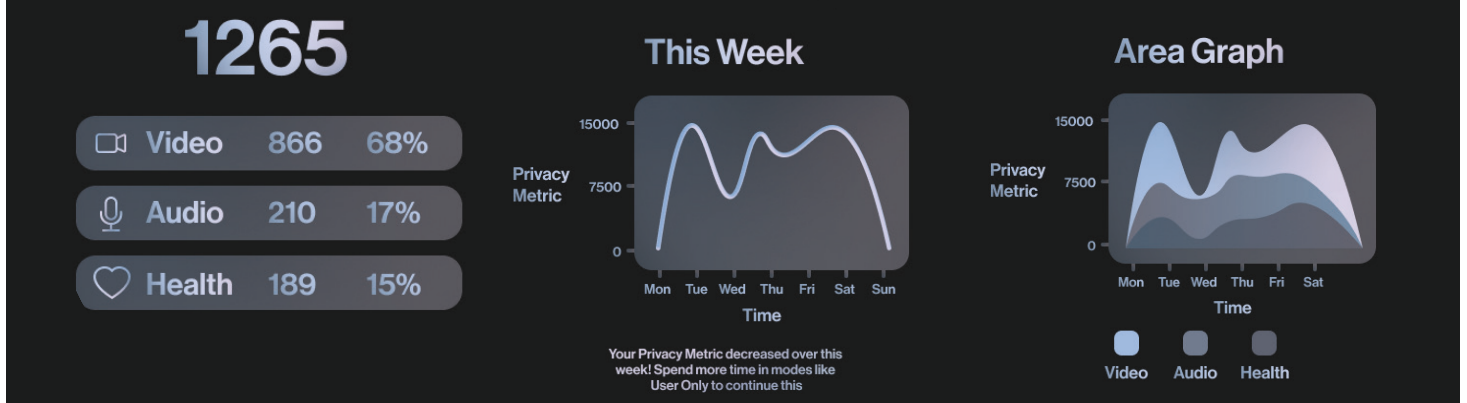
User Testing Results

We performed this with the same group as the previous demo user testing. The results were promising - in 47% of cases the user chose to change their privacy mode to the most private mode that would still allow them to continue the activity outlined in the situation. 32% choose the mode that removed the largest bubble in the graphic. However, users noted that the user request and device request bubbles weren't useful and thus weren't action inducing. Therefore these bubbles were replaced with bubbles showing were the requests were going (e.g. Facebook). This was to make the bubbles more action inducing - i.e. if Facebook is high the user knew to spend less time on Facebook.

HMW3 - Showing Trends

We felt the only way to achieve HMW3 was with relatively detailed graphs to display privacy metrics across the time span of a week. Our initial plan was to compare this with other events in the users life (e.g., the day after a high privacy score the user spends a lot on online shopping etc.). This would allow the user to see how their privacy affects their life. Based on our conversations with Ali Shah we dropped this as it would involve collecting invasive user data.

We knew from the beginning that to effectively test our trends concept we would need a working model implemented into a users home for a long period - something we can't produce. Given we had no way of validating the design - we did not perform the same detailed design process as with the other visualisation sections - instead we came up with a simple concept for the sake purpose of embodying the design



Your Privacy Metric decreased over this week! Spend more time in modes like User Only to continue this

Conclusion

With this research and development we are confident in our privacy metric concept and our data type and external service bubble concept. Together these give 'at a glance' privacy information to highlight the need to adjust privacy settings and a visual break down to inform the user which privacy mode to switch to. Any further development would require the development of the weighting model which as well as the deep packet analysis classification algorithm (see page 14).

Touchpoint of Home Privacy I

Design Constraints

01 Control privacy modes with an interaction that scores highly on the 5 factors of usability.

02 Have a flexible design that can seamlessly integrate into any users home.

03 Be able to display the privacy metric and visualisation tool visibly across a room

04 Be realistically sized in terms of the technology inside.

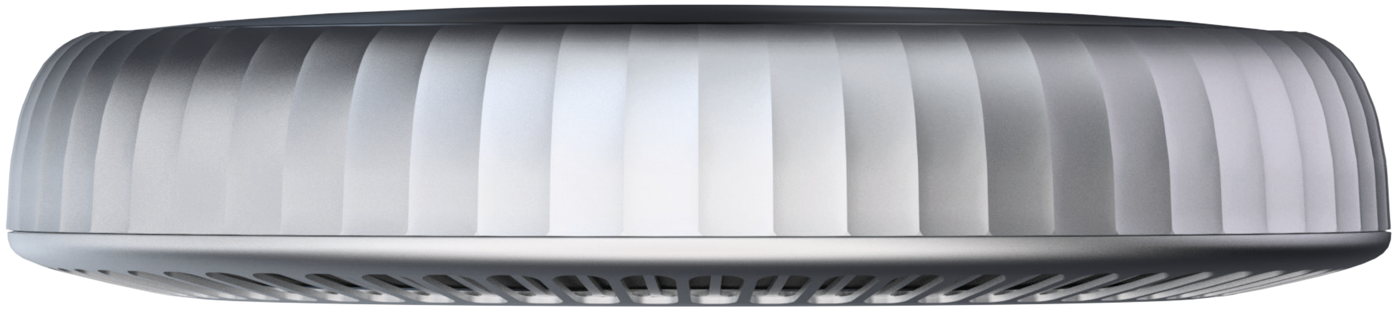
Why a dial?

When researching consumers perception of privacy for our interim report we found that though consumers desire privacy - if they encounter excessive friction when trying to achieve it they will quickly give up. This was the inspiration behind the dial form factor. Changing privacy settings is an action a user will do on impulse - based of the privacy metric and the context. With a wall mounted dial the user can control the data leakage of all of their devices in one action, meaning adjusting privacy modes becomes as easy as dimming lights. A dial interaction performs incredibly well on the usability factors - the action to highly learnable and memorable - and mapping modes to specific dial positions makes switching between them a highly efficient action with minimal errors. Finally the innately physical interaction is highly satisfying - giving users confidence the action has taken place.

One Purpose

When designing an IoT touchpoint for the home of 2040 - it's easy to fall into the trap of overloading it with features in an effort to justify it's place in a users home. However we are confident that our concept will add significant value to a users life - becoming a product they will not be able to live without. Therefore, we kept strict to our philosophy of developing a 'touchpoint of home privacy' - resisting feature creep - to create a device whose sole purpose was to help a user understand, control, and minimise their data leakage.

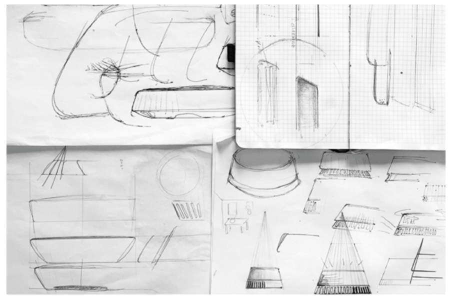
1



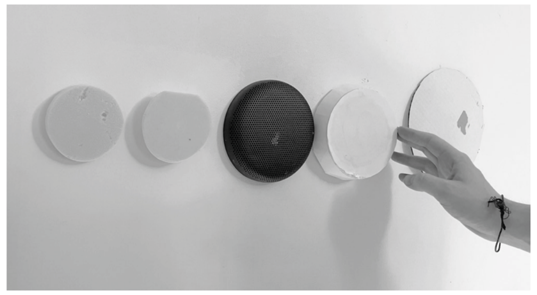
Process

An organic process - continually iterating between sketches lo-fi prototypes and CAD models - was used to develop the form of the dial. Sketches were used to quickly ideate features and ideas of the product, ergonomics were validated and size was validated with lo-fi models.

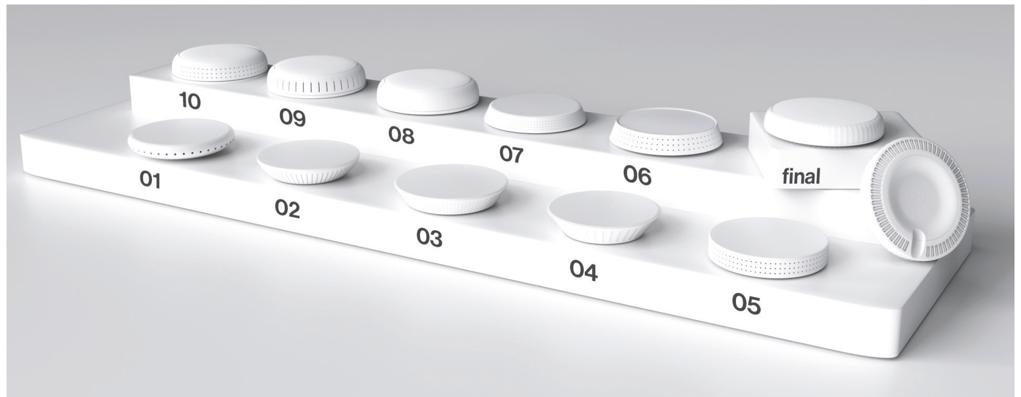
The display is the size of a CD allowing for the metric, visualisation tools to be visible from across a room, and the trend pages to be easily readable. The slight incline on the dial provides more area for the user to stroke when using and blends more seamlessly into the wall.



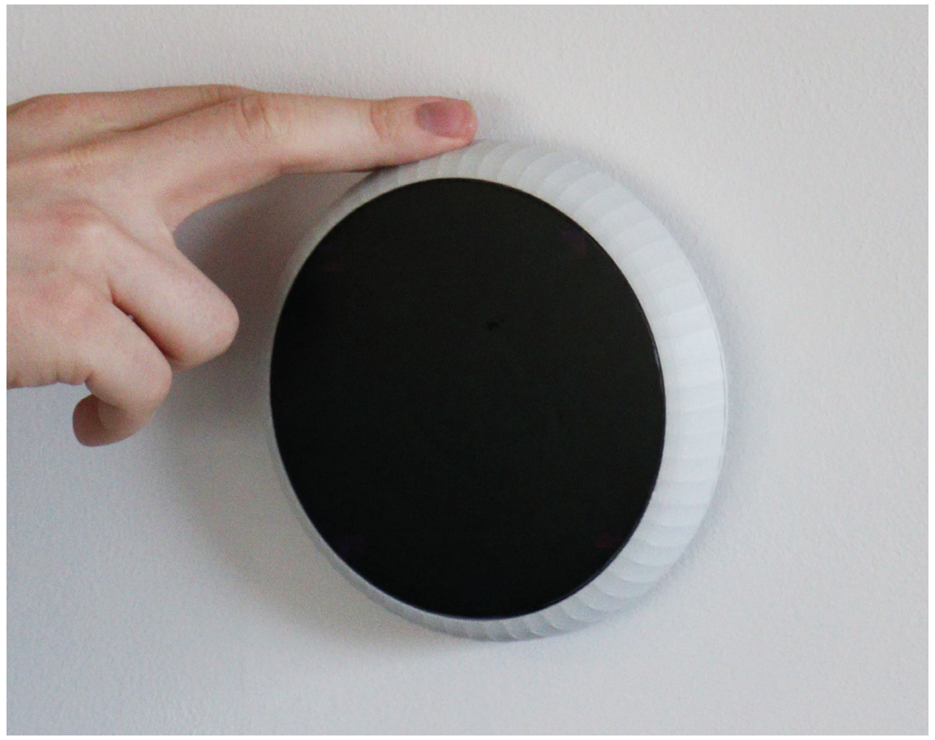
01 Sketching



02 Prototypes



03 CAD Iteration



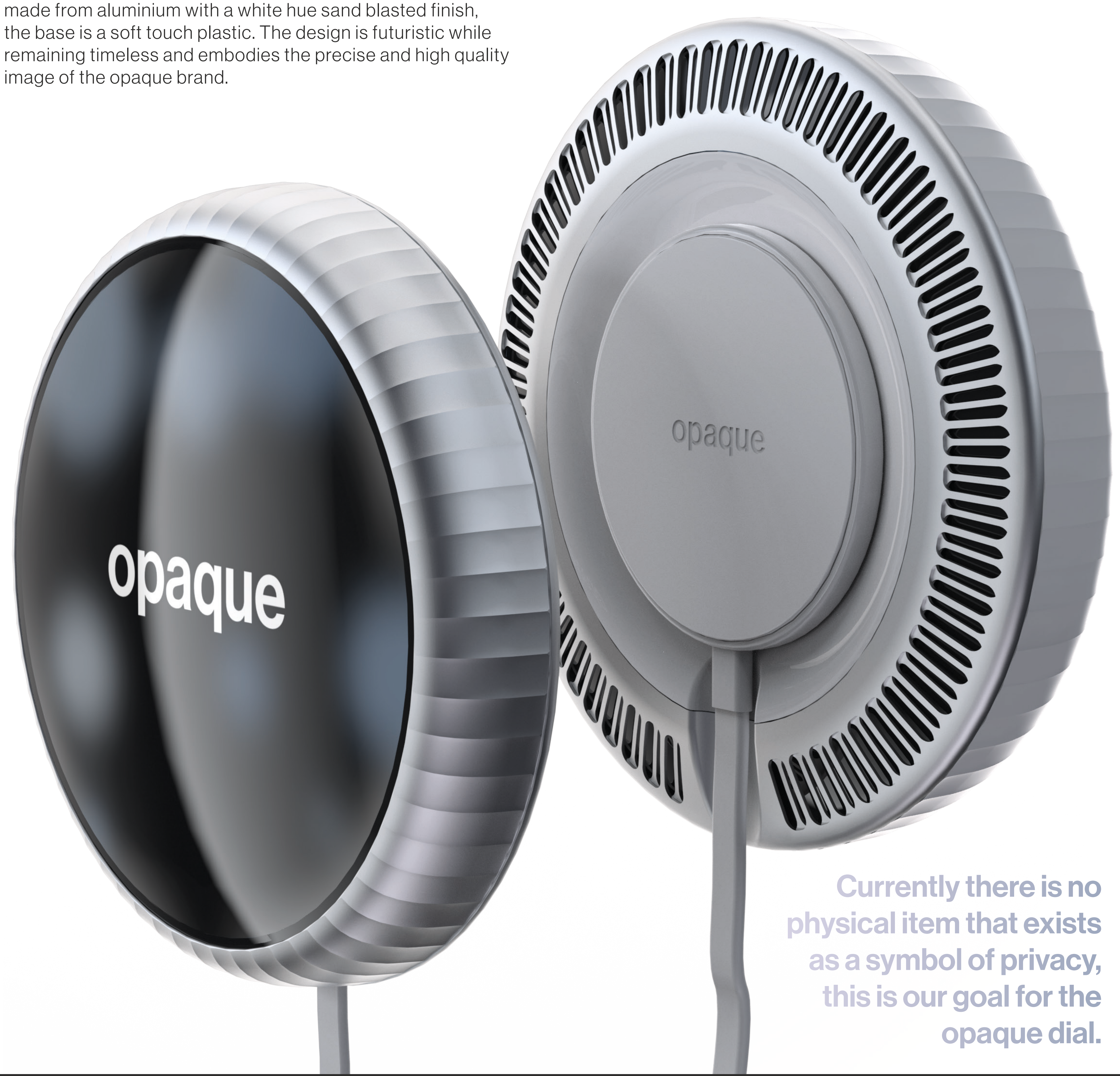
04 Final 3D Print

A dial connotes fine control providing the user with the necessary assurance that their action has been fulfilled.

Touchpoint of Home Privacy II

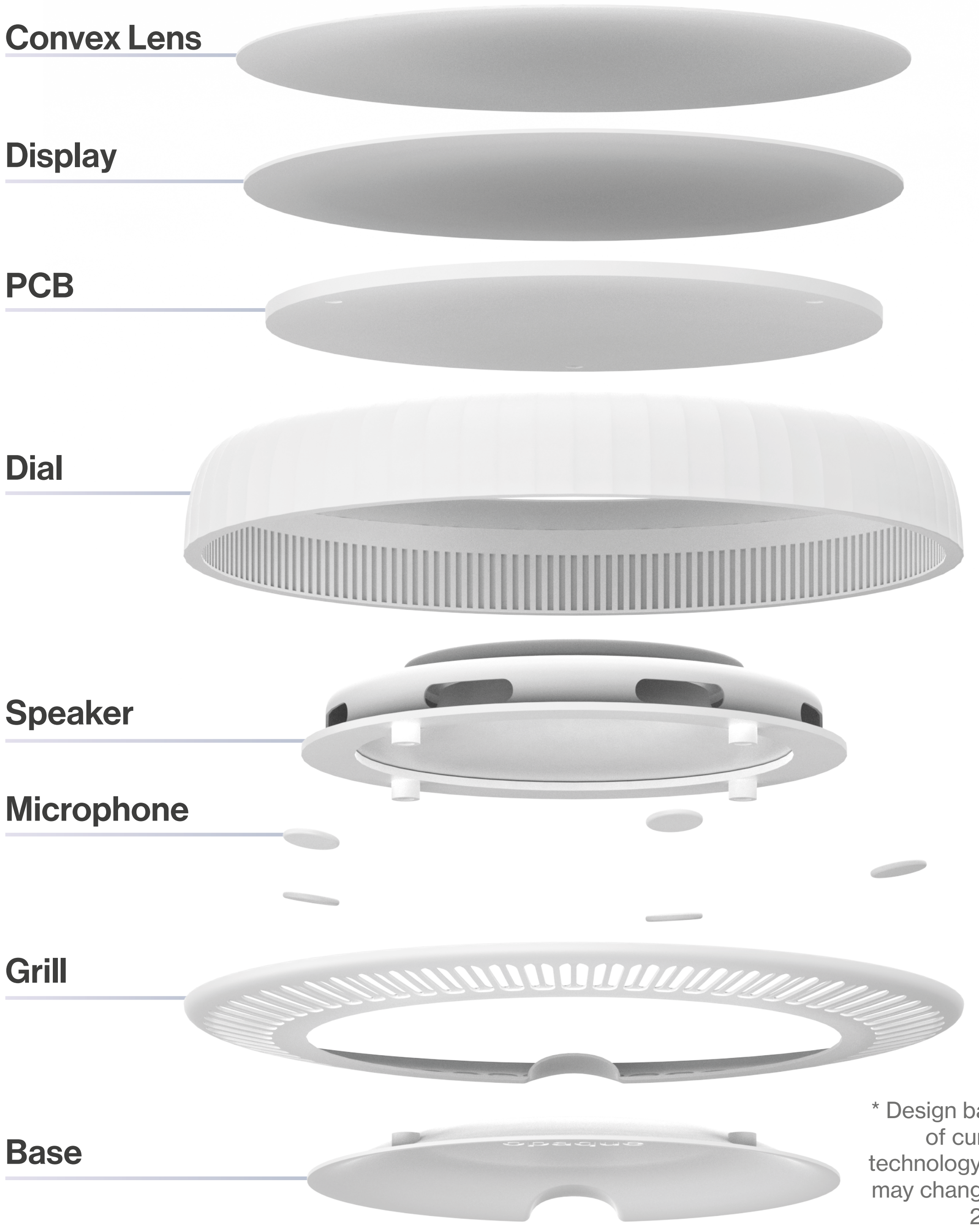
Details

The dial's design affords rotation. It's finished in with a subtle texture and a slight taper which encourages and improves the user interaction by providing a slight grip. The dial and grill are made from aluminium with a white hue sand blasted finish, the base is a soft touch plastic. The design is futuristic while remaining timeless and embodies the precise and high quality image of the opaque brand.



Currently there is no physical item that exists as a symbol of privacy, this is our goal for the opaque dial.

Component Breakdown



* Design based of current technology and may change by 2040

The Complete Package

In response to Ali's concerns of how the system would work in a shared house and his idea to make the system educate young children on data privacy control. Each Opaque Dial is equipped with the hardware and software required to create the entire system. This allows the homeowner to define regions within the home to be controlled by a separate dial. This means different parts of a home can have a different privacy mode - so if an inhabitant was working in a kitchen in 'All On' mode; another could perform a privacy detox in a bedroom in 'Local Only' mode.

Touchpoint of Home Privacy III

The Opaque VUI

The Dial is also the touchpoint for the VUI assistant. For this it integrates a microphone and speaker. The exact nature of the assistant as not thoroughly explored in this project, as we felt it was it was not critical to demonstrate or test our concept. However we did ideate a few potential behaviours - each with advantages and disadvantages. One idea is to have it completely non-personal - only replying when necessary and giving no intelligent context based suggestions. This emphasises the private non-learning approach of our system and would help create the feeling of a private 'safe space'. However, this may limit the functionality of our system. The other idea of making it a 'privacy assistant' - that guides users through and helps them make privacy decisions (e.g. "Your Ocado Fridge is sending a lot of camera data - would you like switch to anonymous"). This would help educate a user, but would require additional data to be collected which may feel invasive.

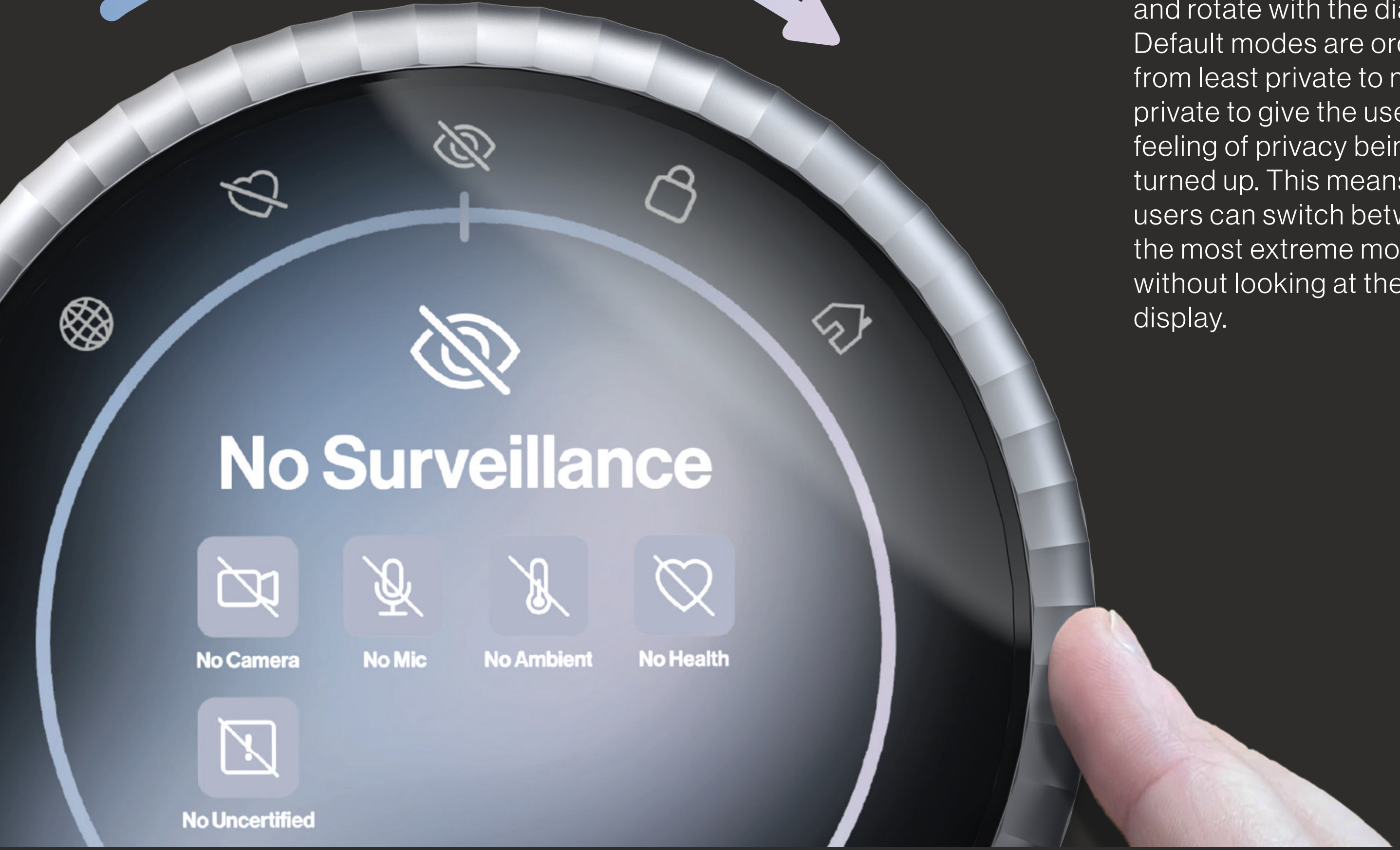
User Interface Design Constraints

01 The visual interface should only control and change data privacy within the home.

02 The privacy metric and visualisation tool should be front and centre, so the user can clearly see if privacy changes need to be made.

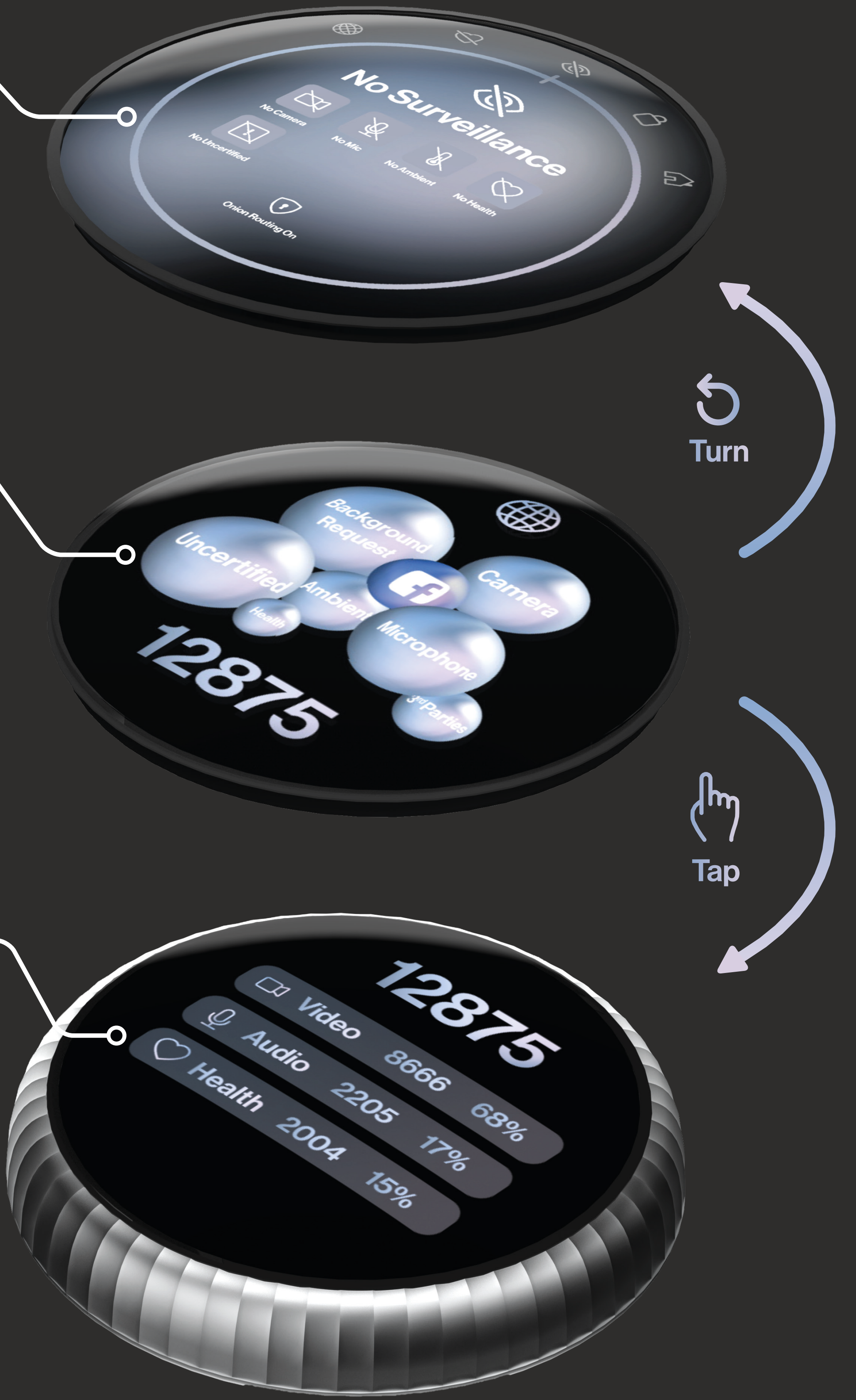
03 The current blocked categories should be clearly displayed to the user as the mode is changes.

Rotate the Dial to Change Privacy Mode



Turning Up Privacy

Modes are positioned around the top of the display and rotate with the dial. Default modes are ordered from least private to most private to give the user a feeling of privacy being turned up. This means the users can switch between the most extreme modes without looking at the display.



Mode Change

The Mode Selection screen blurs over the top of the bubbles to display modes, relevant blocked categories and whether onion routing is on. Once the user stops rotating the set mode hangs for a few seconds.

Privacy Bubble Home Screen

The Privacy Metric and Bubbles are the home screen, visible to the user at all times. This gives them instant information about current data leakage. This allows users to see the current state of household privacy at all times.

Trends: Breakdown and Graphs

The trends display gives the user in-depth information about the Privacy Metric over the last week. This is accessed by tapping the home screen. Swipe right on the first Trend page to see an overall Metric Trend Graph, and Area Graph.

Turning Data Categories Off, Not Blocking On

To make the system more intuitive the UI presents active privacy categories as 'turning off' a data type instead of turning on blocking.

Private by Design Technology I

Request Classification Algorithm

Design Constraints

Our constraints when designing the technology, and determining the possibilities of the system:

01 The system should allow a user to use any device they choose without requiring compliance/collaboration with manufacturers. As Ali Shah pointed out, our system will limit services data collection - on which their business model may rely - so collaboration shouldn't be relied on.

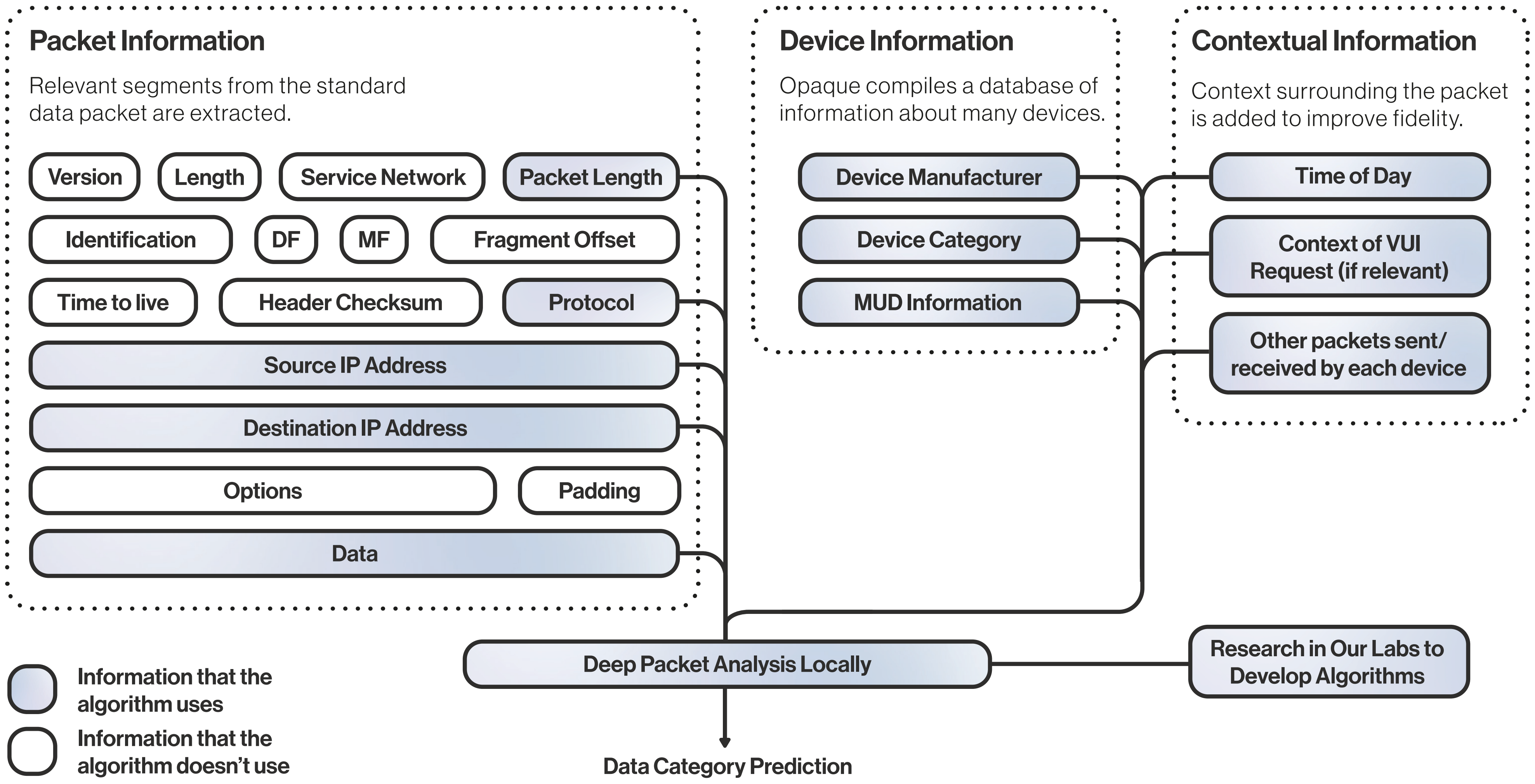
02 The technology shouldn't hinder a user's speed in any way - else they will not use the system.

03 Our device cannot require apps to be installed on a device, to avoid sharing of private data even within our system.

04 The solution shouldn't require machine learning within the home since users may be hypersensitive to the implications of this.

05 Our solution shouldn't require accounts - removing the need for any data being tied to a user or stored externally of the device.

Proposed Deep Package Analysis Algorithm



Packet Information

Relevant segments from the standard data packet are extracted.

Version, Length, Service Network, Packet Length, Identification, DF, MF, Fragment Offset, Time to live, Header Checksum, Protocol, Source IP Address, Destination IP Address, Options, Padding, Data

Device Information

Opaque compiles a database of information about many devices.

Device Manufacturer, Device Category, MUD Information

Contextual Information

Context surrounding the packet is added to improve fidelity.

Time of Day, Context of VUI Request (if relevant), Other packets sent/received by each device

Deep Packet Analysis Locally

Research in Our Labs to Develop Algorithms

Data Category Prediction

▨ Information that the algorithm uses

□ Information that the algorithm doesn't use

Classifying Requests

Depending on the current privacy selector mode, requests need to be filtered - potentially being blocked. Therefore, our device will need to classify data requests into the multiple categories. Opaque will train an algorithm to do this, using multiple sources of information and our own lab testing - pushed to the dial in regular updates. Software on the user's devices themselves would allow easy analysis of unencrypted requests, but without this the requests the dial sees will be encrypted. Therefore within the home, the algorithm will take in a combination of data packet information, device information and contextual information, as described in the diagram, to help classification. The algorithm aims to answer:

- Is the behaviour normal or unusual for that device?
- Is the packet destination a first or a third party? (manufacturer or Facebook)?
- What type of data is it (audio, video, health, ambient)?
- Is the request triggered by the user or in the background?
- Is the device certified or uncertified by Opaque?

This method of classification takes inspiration from the academic research creating IoTrimmer [6], iDetector [7], and Databox [8]. We spoke to two of these projects lead researchers, Anna Maria Mandalari and David Boyle, to understand more about the current state of the art for this technology.

Their research demonstrates the feasibility of deep packet analysis - outlining a system to categorise or 'finger print' devices and their behaviour locally (at the edge). However, as it stands there are a few key limitations. The quality of the classification decays rapidly - and requires the continuous collection of user activity data to regularly retrain the model, at the edge - something we believe is unacceptable for a privacy by design system. Furthermore, even at its peak the system isn't totally accurate - meaning devices may stop working unexpectedly, or continue to work when they shouldn't - which again we believe is unacceptable.

However the research noted that these are problems that they hope to address with future research - and the experts we spoke to agreed that with 20 years of development in computing, machine learning, and network technologies the proposed system will be viable.

> **"What's in the labs today will be commercial in 20 years"**
> **- Prof. David Boyle**

[6] Maria Mandalari A, Kolcun R, Haddadi H, Dubois D J and Choffnes D. Towards Automatic Identification and Blocking of Non-Critical IoT Traffic Destinations. Available from: https://arxiv.org/abs/2003.07133.
[7] Maali E, Boyle D, Haddadi H. Towards identifying IoT traffic anomalies on the home gateway. *Proceedings of the 18th Conference on Embedded Networked Sensor Systems. 2020.* Available from: doi:10.1145/3384419.3430414
[8] Zhao Y, Haddadi H, Skillman S, Enshaeifar S, Barnaghi P. Privacy-preserving activity and health monitoring on databox. *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking. 2020.* Available from: doi:10.1145/3378679.3394529

Private by Design Technology II

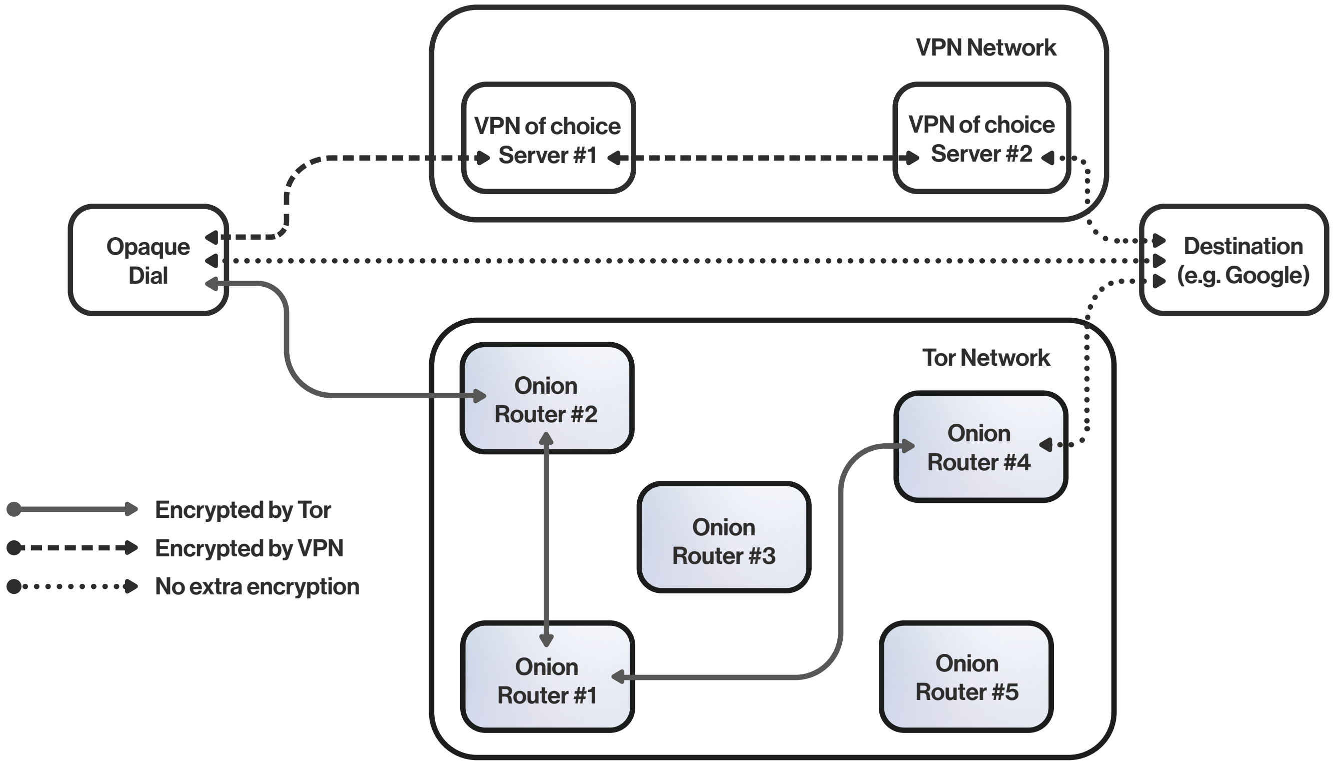
Anonymised & Locally Processed

Online & Anonymous

The Opaque Dial allows a user to further limit the data able to be collected by companies, by anonymising their data - directing requests through a Virtual Private Network (VPN) or through an Onion Routing network such as Tor.

The Tor network acts as a middleman between the home and an external service, similar to a VPN - however by using onion routing it makes data virtually un-traceable. Onion routing works by adding several layers of encryption then sending it between several routing servers - each one able to remove one layer of the encryption [9]. The final router sends the now unencrypted request to the destination server (e.g., Google). Each routing server can only see the server directly behind it and in-front of it, and only holds the key to one layer of encryption - meaning a packet cannot be interpreted and fully traced by anyone looking into a single point of the onion network. Onion routing is currently slow - however we expect by 2040 improvements in network technologies will mitigate this problem.

To provide full flexibility users can add their preferred VPN, select Onion routing or use no additional encryption. These routes are shown in below.



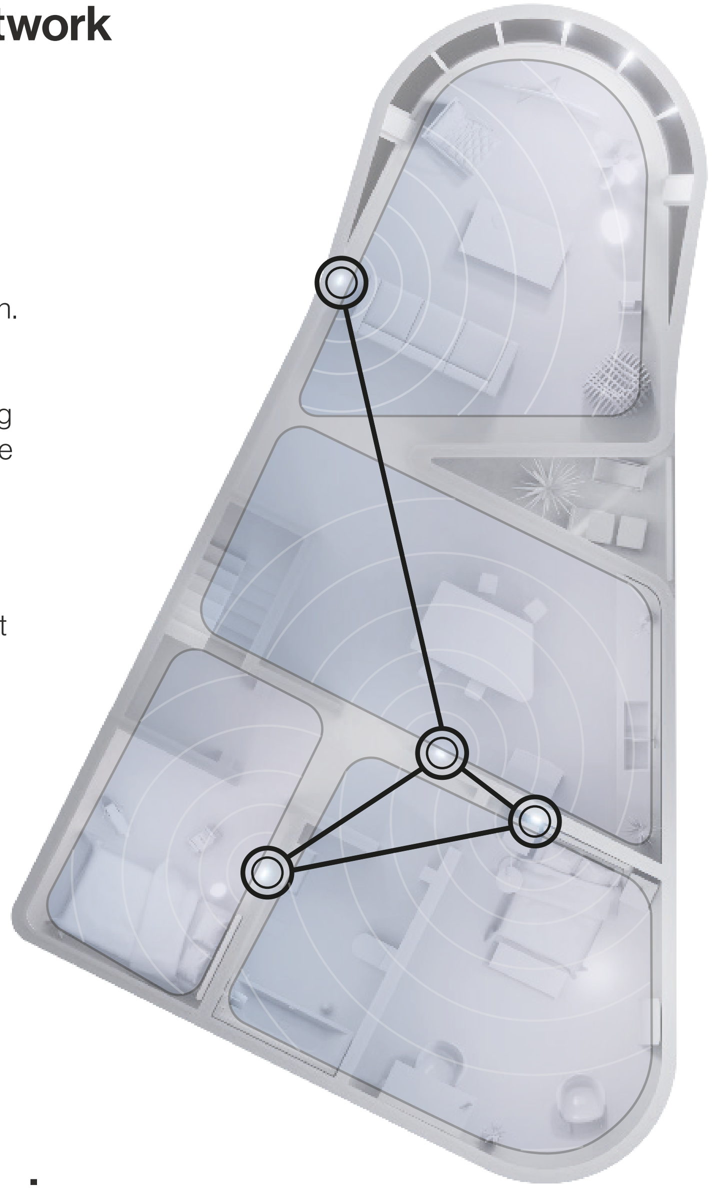
Using either the VPN or Tor, the origin of the data (the user's home) is not able to be determined and tracked by the destination - i.e. the requests are being made anonymously. This protection is lost however if the user signs into an account, since the requests can then be attached to that user. This is a severe limitation of this method for many services, however if a better anonymity solution is developed in the next 20 years it would be used instead.

For each mode the user is able to easily toggle the VPN/Onion routing on or off. This is needed in certain situations where the location/identity of the user is required. E.g. a regional service such as BBC iPlayer or an institution (e.g. an employer) requiring a proprietary VPN to access it's network.

The Opaque Regional Mesh Network

Each Opaque Dial connects to the home's existing router then creates its own sub-network for a user defined region of the house (e.g. a bedroom) - all these sub-networks mesh together creating a single network for devices to connect to - for ease of use. Which specific region a given device is in is found intelligently by finding the closest connection. What data a device is and isn't allowed to transmit is controlled by the mode set in its current region. Although this system is proposed based on existing mesh WIFI technologies, it would be updated to use 2040's state of the art technologies.

The Dials are able to send local requests between each other through secure encrypted connections within the mesh network. The Dials initially connect through a simple passkey exchange (no accounts required).



Minimise Through Local Processing

Local processing is used to minimise the amount of unnecessary data leaving the home and allow for basic utility during a privacy detox.

The Opaque Dial's built in local VUI assistant allows the user to control basic home and privacy functions. Our system achieves this without using voice recordings to improve its accuracy - limiting our own data collection and on device learning. Although local natural language processing is currently limited, by 2040's we expect this technology to be sufficiently accurate and reliable for our application. If the user makes a request that can't be processed locally (e.g. ordering a takeaway) - the system will remove any emotional data from the voice recording and forward it on to the users external VUI of choice (e.g. Alexa).

The dial also integrates a smart controller using 2040's state of the art wireless technologies (similar to Zigbee, z-wave etc. [10]). This takes load off the main wireless network and enables these devices to interact locally. We would develop an open API to allow manufacturer's to integrate their devices with the controller for extra functionality. E.g. a health monitoring device control the room temperature entirely locally. The local VUI will also be able to control devices within this network.

[9] *Onion Routing.* GeeksforGeeks. Available from: https://www.geeksforgeeks.org/onion-routing/ [Accessed: 11th March 2021]
[10] *Z Wave Vs ZigBee: Which Is Better For Your Smart Home?* The Smart Cave. Available from: https://thesmartcave.com/z-wave-vs-zigbee-home-automation/ [Accessed: 11th March 2021]

Business Planning

Creating Trust

The key non-technical challenge our company will have to overcome is building trust with consumers. Our system is designed for a future scenario where consumers understand the value of their data and have an inherent mistrust in large technology companies. We, a technology company, are presenting a solution to this problem that will have access to all of the household's data - and the consumer will be savvy to this. Therefore to be successful we have to gain the consumers trust. We believe we can do this by achieving three things:

Business Model

Our business model must be profitable without data harvesting, and creates an incentive to not collect user data.

Technology (see 13-14)

We need to demonstrate that our system is private by design and our technology is not used to collect user data.

Branding (see 17)

Our branding and marketing materials must position Opaque as a privacy first technology company.

To achieve point 1 our system needs to be monetised and premium. To cover the cost of continuously developing and updating the classification algorithm the service is going to require a monthly fee - and to justify a high monthly fee the hardware needs to look and feel premium. This high monthly fee should demonstrate a 'privacy premium' to the consumer. They will recognise that subscriptions fees make up the majority of the companies revenue, and therefore it is disincentivised from collecting data - because if it is 'caught-out' users will cancel subscriptions.

All this works to build trust in our service. However, this premium price point means we are creating a 'privacy privilege'. Thus, once we have demonstrated that we are a trustworthy brand we would introduce a lower tiered model to 'democratise privacy'.

Certification & Accreditation

In our meeting with Ali Shah we discussed the opportunity of having opaque notarised by the ICO. This would allow us to develop a certification scheme to 'badge' products as having been approved by regulators as data secure. This is an opportunity that no other company has leveraged - and it would allow our firm to build up it's legitimacy. Doing this means consumers will recognise us as the company that decides if devices are or are not private – so when we launch the Dial they will not question its privacy credentials.

We would create two levels of certification - the first if the product is private by design, as a general privacy standard to build our image as the privacy company. A second level of certification could be achieved if the product supports our open source smart home API - helping to solve the problem identified during our privacy mode testing that users didn't know which devices would work locally.

Business Plan

Customer Segments

Finance & Opportunity

Concerned their actions will effect their future finances and opportunities.

Sensitivity

Worried about specific sensitive data leaking (e.g. if work is confidential).

General Discomfort

Find data collection anxiety inducing and want to preserve their 'privacy health'.

Value Propositions

01 Understand what data is leaving the home.

02 Control what data is leaving the home rapidly.

03 Minimise the data leaving the home.

Key Partners

Information Commissioners Office

The ICO needs to approve and acknowledge our testing and certification program.

3rd Party Research Organisations

Data from organisation like MUD and Mozilla will be used to develop data classification algorithm.

Key Activities

01 Developing the Data Classification Algorithm

02 Development of Hardware Products

03 Certifying Devices

04 Developing Local VUI & Open API

Customer Relationship

Local VUI

Allow user to control their smart home devices.

In-Person Assistance

No data is collected & devices can't be controlled remotely, so help & support needs to be performed in person.

Channels

Device Certification

Device certification markings listed on approved products

2040's Channels

The relevant channels of 2040

Key Resources

Smart Devices to test

Required to develop classification algorithm

MUD / Regulator Product Information

Required to develop classification algorithm

Cost Structures

Manufacturing

Hardware & Software Development

Device Certification

Opaque will not charge for this as it's a branding project. The cost of testing and approving devices will need to be covered by revenue

Revenue Stream

Hardware Cost

The premium hardware will be sold at close to cost price to encourage adoption

Monthly Subscription

To cover the cost of keeping the classification systems up-to-date and generate profit.

Branding

“Opaque: Understand, Control, and Minimise your Data Exposure”

Understand, control and minimise your data exposure

Demonstrating the Product, not the Problem

The brand’s messaging shouldn’t centre around the extent of the user data collection, the malpractice of other firms, or the effects these factors have on users lives. It shouldn’t paint a dystopian picture of the world of data collection to scare consumers into buying a patchwork solution. Instead it should present the system as a highly effective and desirable tool no modern home is complete without - giving the consumers understanding and control over their and their families ‘privacy health’. It should be described as a product designed from the ground up to do something new rather than a ‘patchwork’ temporary fix trying to solve an impossible problem.

Private Now, and Always

The message of absolute data privacy must be conveyed through every interaction with Opaque, as our concept hinges around consumer trust. Currently, public perception is becoming increasingly sceptical of major technology companies; Opaque must make an effort to differentiate from those companies by instilling a core message of trust. For example, service hot-lines shouldn’t be able to see any user data remotely and ‘remote connect’ to the hardware - instead if problems occur technicians should be sent.

Assets Representing Data and Privacy

Our branding assets need to speak to our branding messages. There is no colour of privacy - thus we have defined this as pale blue - a calming colour that promotes tranquillity to support the products aim of creating a safe space from invasive data collection. The colour connotes trustworthiness and reliability - key pillars our brand.

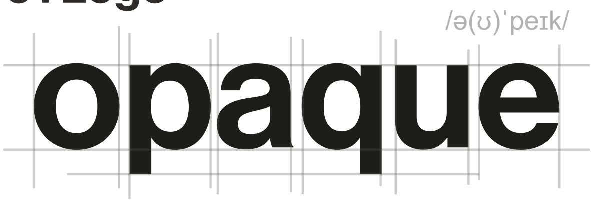
The ‘orbs’ used throughout the UI and the branding are a visual manifestation of a users data. They appear alive - floating and colliding on the UI to engage the user. Their size represents their proportion of data - the way images are applied shows the data bulging almost bursting out.

Opaque to the World, Transparent to You

The message of absolute data privacy must be conveyed through every interaction with Opaque, as our concept hinges around consumer trust. Currently, public perception is becoming increasingly sceptical of major technology companies; Opaque must make an effort to differentiate from those companies by instilling a core message of trust. For example, service hot-lines shouldn’t be able to see any user data remotely and ‘remote connect’ to the hardware - instead if problems occur technicians should be sent.

Branding Iceberg

01 Logo



‘Not able to be seen through; not transparent’

The logo is well balanced, simple and clean to reflect Opaque’s approach to the future scenario. Using a dictionary word allows for the opportunity for Opaque to naturally develop into a household name for privacy.

02 Visual Identity

Neue Haas Grotesk Display Pro

03 Offering

All Opaque’s products are privacy focussed

Above Surface

Below Surface

04 Market Strategy and Positioning

Opaque is a privacy company, not a Smart Home technology company that considers privacy - certifying devices as private by design will solidify Opaque’s position as the first major privacy company.

05 Personality and Voice

Opaque portrays a helpful, open and honest outlook; a respite from the current data farming culture encouraged by companies that profit off data collection.

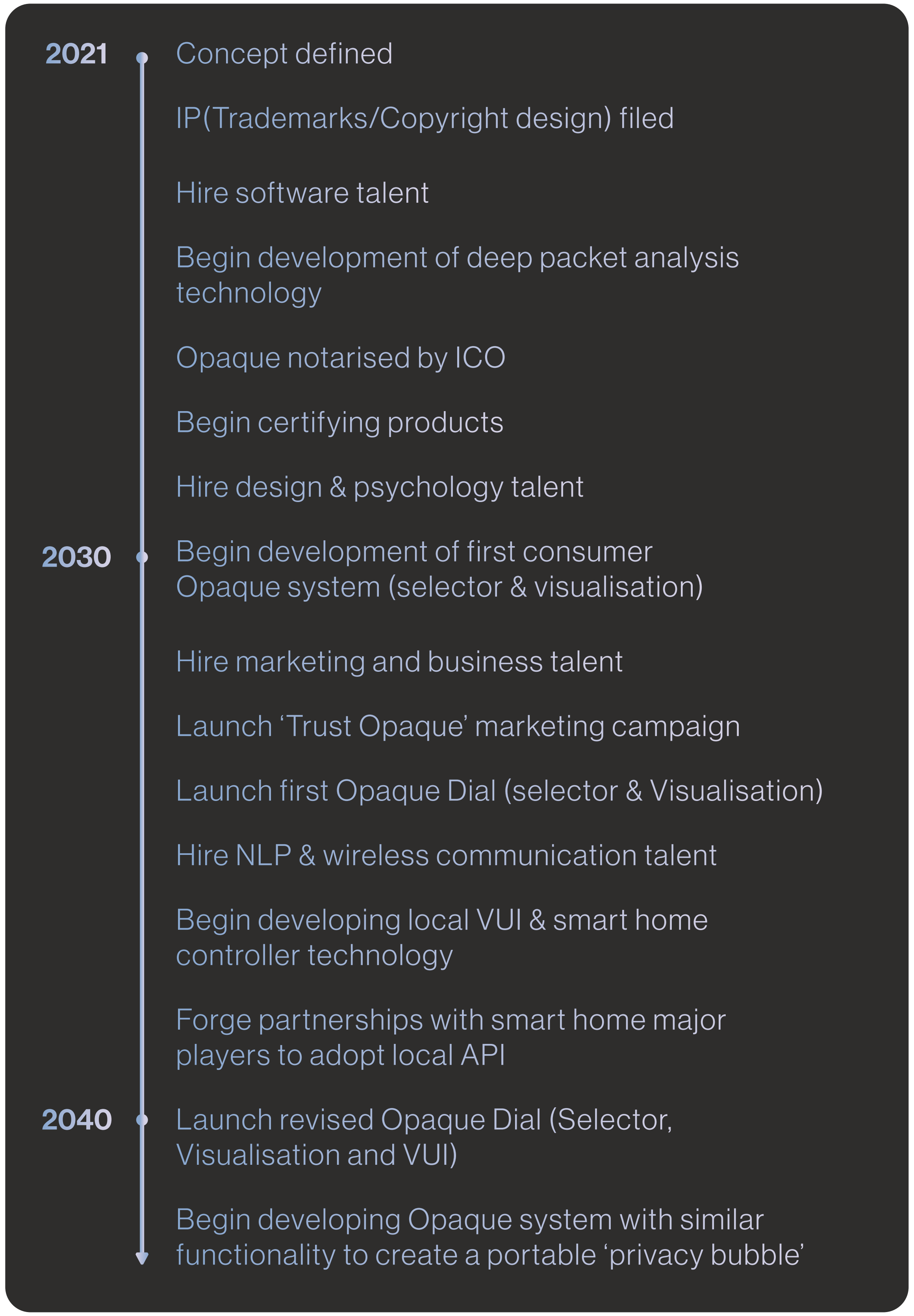
06 Brand Mission and Promise

Understand → Control → Minimise

The key aims provide a clear brand message as single missions, but more importantly provide a chronological progression in the users interaction with their data. Interacting with the brand Opaque and the Opaque Dial allows the user to develop an understanding of their data exposure. This expanded knowledge prompts a desire to change data exposure, and the Opaque Dial represents a means of control. Over time, this understanding and control leads to a minimisation of your data exposure.

Development Roadmap & Project Limitations

Technology Roadmap



2021 Concept defined

IP(Trademarks/Copyright design) filed

Hire software talent

Begin development of deep packet analysis technology

Opaque notarised by ICO

Begin certifying products

Hire design & psychology talent

2030 Begin development of first consumer Opaque system (selector & visualisation)

Hire marketing and business talent

Launch 'Trust Opaque' marketing campaign

Launch first Opaque Dial (selector & Visualisation)

Hire NLP & wireless communication talent

Begin developing local VUI & smart home controller technology

Forge partnerships with smart home major players to adopt local API

2040 Launch revised Opaque Dial (Selector, Visualisation and VUI)

Begin developing Opaque system with similar functionality to create a portable 'privacy bubble'

Limitations

This project is designed for the world in 2040 - however, our design and engineering process was limited to the means available during the 2020-21 COVID-19 pandemic. The limitations of our approach to developing our concept was discussed throughout this portfolio - however, they are summarised here:

01 The lack of a working prototype meant the 'dial' based form factor to change privacy modes has not been fully tested with users.

02 The privacy selector hardware is purely for the embodiment of the concept, and does not consider the technology it would contain when released.

03 The privacy metric and visualisation tools are solely concepts for visualising privacy. The model for measuring data would need to be developed and weights assigned which is heavily subjective.

04 When trying to understand the wants of people in 2040 - we reached out to today's extreme users. The respondents won't be a perfect representation of the average 2040 consumer and we did not record the ages, genders, or socio-economic status of respondents so there may be a sample bias

05 The functionality of the home in the demo may not be a good representation of a smart home in 2040

06 When testing our demo, we only had access to family and friends, leading to a potential acquaintance bias

07 Our business model and strategy for developing user trust are only our thoughts, and have not been fully tested

08 It is assumed that future homes will still use local Wi-Fi style networks and not just 5G/6G.

09 It is assumed that deep packet analysis will be reliable enough for accurate classification by 2040.

10 2040's consumers may be more comfortable with data collection then we expect - negating the desire for our service

Conclusion:

We believe this document, and associated video and demo have demonstrated how our concept could help to solve some of the problems associated with data privacy in 2040. However - this is a huge problem to solve - and we recognise our limitations. Developing this concept would take a highly-skilled multidisciplinary team including: software engineers to develop deep packet analysis and locally processed VUI and smart home controller; designers and psychologists to develop intuitive UI's to make their data privacy easy to understand and action upon; philosophers to decide when data collection becomes invasive and wrong; and branding and business leaders to create a profitable yet trustworthy technology company.

Use Case Breakdown

5:31 PM Yazmin returns home, stressed out from work. She switches to 'No Surveillance' mode and completes her yoga routine to de-stress

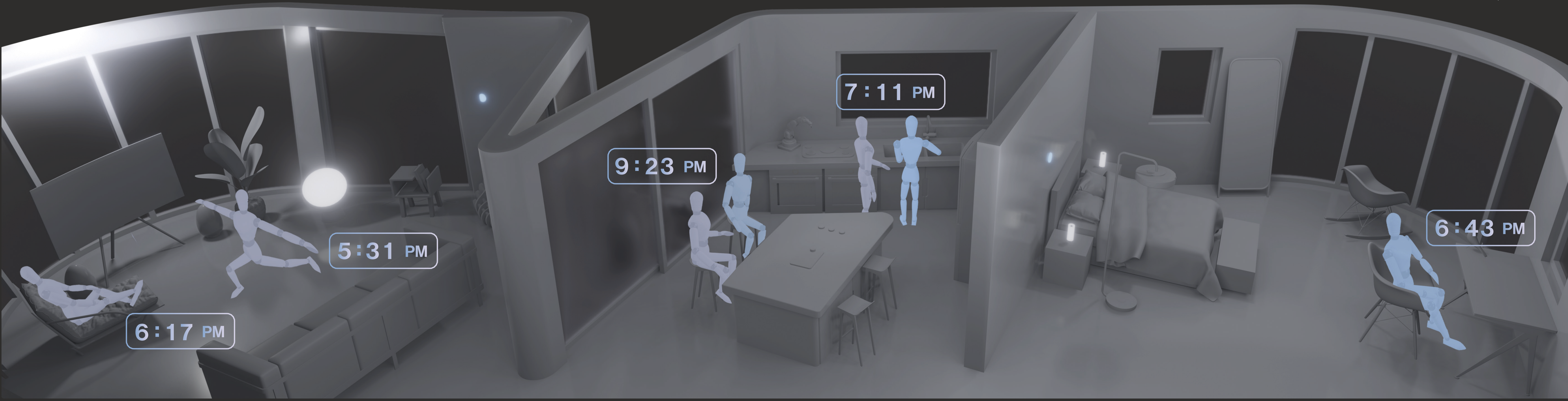
6:17 PM After she's cleared her mind from the yoga she decides to look for new jobs online. She switches to 'User Mode', to search with onion routing, so her employer will not find out.

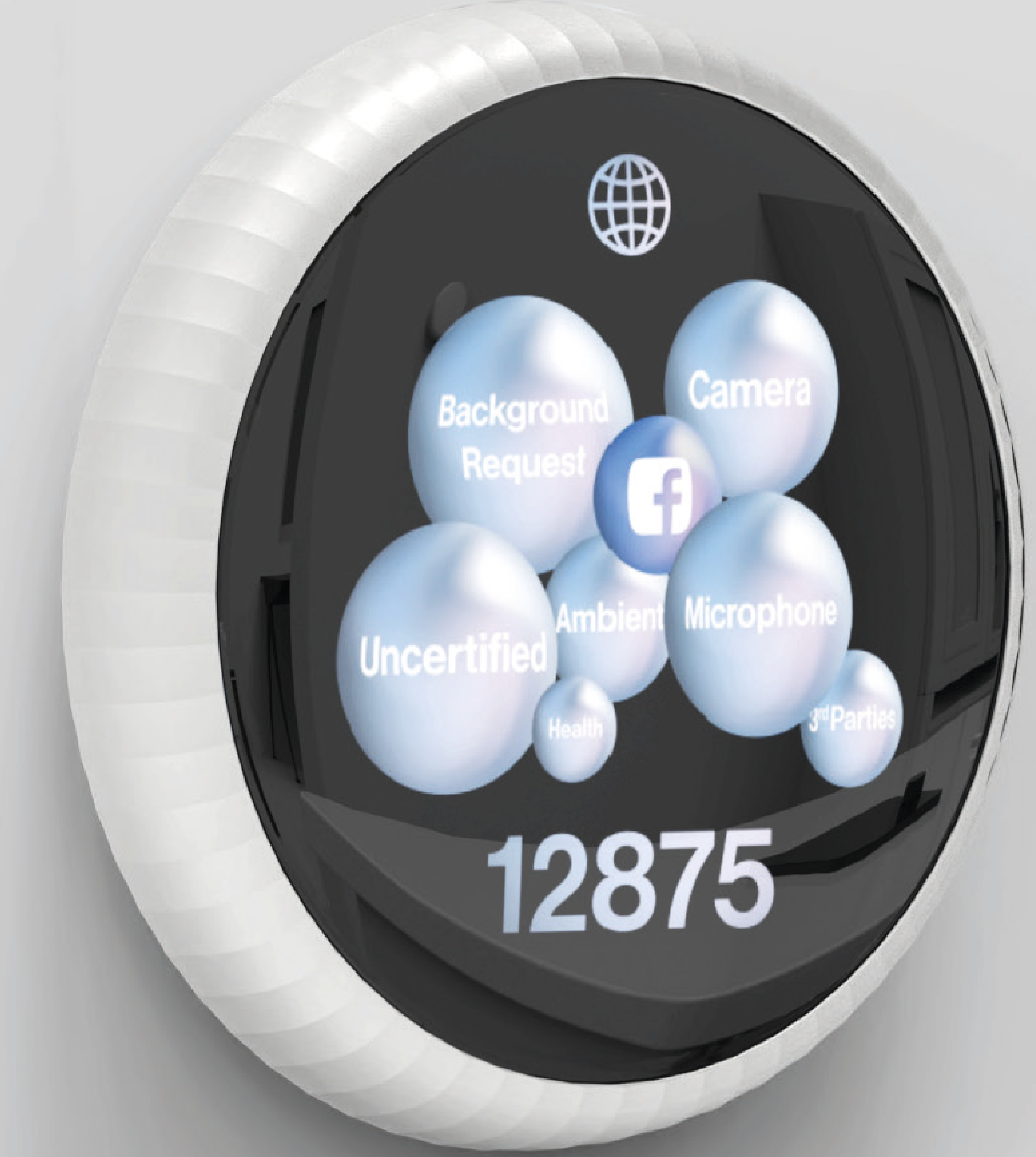
6:43 PM Her boyfriend Leo comes in from work and needs to finish a few tasks on his employers company network. This isn't compatible with onion routing but Yazmin is still searching, so he moves into the bedroom region which he sets to all on.

7:11 PM Leo and Yazmin decide to cook a meal together and need to use the kitchen helper's camera function. They want to enjoy a glass of wine whilst cooking but are concerned about their health insurance premiums increasing. Therefore they switch to no health mode.

9:23 PM They sit down for dinner and Leo glances at the privacy metric seeing it is now very high. They decide to have a privacy detox and switch to local only mode for the rest of the evening.

* Yes Yazmin and Leo are Mannequins

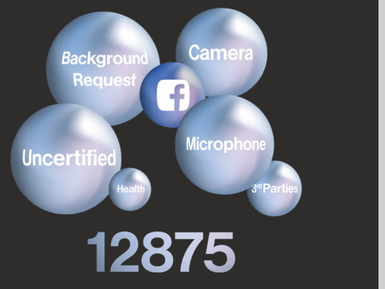




Understand

How: The privacy metric provides an "at a glance" view of total data leakage. The bubbles break which data types and services are contributing most to this.

Why: Gives users peace of mind if data leakage is low and highlights what steps should be taken if it is high.



Control

How: The privacy selector allows instant control of what data is and isn't allowed to leave each region of the home.

Why: Turns the multi-hour long task of changing every devices privacy settings into a one second action done on impulse This provides the user with sense of control and facilitates a privacy detox.

Minimise

How: Local processing is used to minimise the amount of data leaking from the home; while PETs reduce the invasiveness of data that must leave.

Why: To minimise the quantity and quality of data leaving the home.

request
actionable
locally?

Project Management

Tools & Workflow

Throughout this phase of the project we used shared platforms for our planning, research and development. We created a Onedrive to store specific deliverables for the demo, portfolio, video, and presentation, and a Onenote file to store documentation for any additional research. A shared Miro was the primary tool we used for the concept ideation and development - the live updating whiteboard was a highly effective method of presenting our ideas, while also providing a clear macroscopic picture of our overall progress.

Continuing our approach from phase 1, we set up weekly Microsoft Teams meetings with our project tutors Dr Nejra Van Zalk and Dr David Boyle, where we discussed the development of our ideas. In these meetings our tutors shared content to further guide our development, and provided expert contacts for us to meet with to validate our concepts.

In order to ensure we remained on track we created a Gantt chart to plan our development. After every weekly meeting, we set targets of individual work, referencing and updating the chart to track each others progress. This created an individual accountability and ensured everyone was aware of what they needed to achieve across the next week.

The first key deliverable we developed was the online demo, as this was required for testing the privacy selector and visualisation tool. The concept for this was defined early on in the project as we knew it would be the most effective method of user testing our ideas remotely. We later found that it was a highly effective method of demonstrating the product, so it was redesigned to be submitted as a deliverable. Most team members contributed to creating this - planning it's design, creating the assets, or developing the site itself.

Once this was done, each team member lead the development of a specific feature of the concept. Great care was taken to assure the work we produced was highly aligned to the overall concept to avoid the project becoming disjointed. We used a group chat to do this - planning and setting frequent and informal meetings between group team members. Here, short feedback loops were achieved - where members were able to post a quick glimpse of ideation or development and receive near immediate feedback or guidance from other members. This was a highly effective and dynamic method of development.

We developed a highly efficient workflow for preparing the final deliverables. An 'undesigned' portfolio was created on Google Slides so that the team members who managed each section of development could write up their individual pages. McGuckian, Kane, and Gibson filmed the live video footage as they live in one household so could do so COVID-19 safe. Once this was finished the group was divided into two sub-teams. Colebourne & Polturak edited the video footage while McGuckian, Kane, and Gibson converted the 'undesigned portfolio' into a final branded document and created the presentation.

A particular phase during the project where management could have been improved was when all development had been completed and team members were adding their content to the portfolio slides. Here we found that there were multiple repetitions of research insights and the content did follow a clear narrative from start to finish. Re-structuring the content in clearer format was time consuming and we could have avoided this issue by investing more time in planning the portfolio format. Furthermore, when the 'undesigned portfolio' was converted a final branded document - Gibson and Kane worked on pages independently and thus when it was put together their were design inconsistencies meaning time needed to be spent unifying the design.

The project budget was managed by McGuckian and was spent on acquiring royalties for video assets and 3D printing the privacy dial.

Teamworking

Our team dynamic closely followed the Tuckman "Stages of Group Development" model. In the early stages of phase 2 there was a brief "storming phase" as team members were trying to find a section of the project they could take ownership of and work on with some autonomy. As multidisciplinary Design Engineers, each team member would have been capable of leading each section, meaning their were a few minor disagreements on how it should be managed. These problems may have been accentuated by four of the group members having 'Intuition Thinking' MBTI personality types - meaning most of us typically tend towards leadership roles. However we quickly moved into a routine where each team member lead the section of the project that best aligned with their skills and interests. This took longer than expected however it was important to ensure everyone was content with their responsibilities for a rewarding and productive experience.

With this defined, each member could take their own initiative in the research and development of their own section, often leading to milestones being met ahead of schedule and work being of higher quality.

Jack Polturak

I lead the development of the privacy mode categorisation, this is due to my existing skillset and interests in digital and experience design. In this role I learnt the importance of maintaining clear communication channels with my other project leads, this is mainly due to the privacy modes being incredibly dependant on technical development (led by McGuckian and Colebourne), hardware and form development (Ted Kane) and branding & user interface (Alex Gibson). In reflection, when editing the video, I could have been more open suggestions to changes to first draft.

Ted Kane

I lead the hardware and visualisations for the project. I also produced the portfolio with Alex. I produced the visualisations and design of the product externally and internally. I designed the house seen throughout with the aim of embracing a realistic home of 2040 and conveying Opaque's mission. I brainstormed the visual identity of Opaque with Alex, together we had a extremely constructive teamworking dynamic continually bouncing ideas of each other. In reflection I could have avoided some of the conflict during the project by taking some time to think, furthermore taking time to let others speak in meetings could increase productivity and diversity of thought.

Alex Gibson

I ideated and developed the visualisation tool, conducting research and creating prototypes to develop a metric and bubble data representation that was human centred. I also lead the visual identity and UI development for both the brand and product, which allowed for the cohesive design of the portfolio and presentation slides. I worked with Ted, Oliver and Patrick when developing the UI, as their work in hardware form and technology influenced the design and structure of the UI. Reflecting on the work, I think that i could have increased collaboration with team members on important decisions in the section of work that I was covering, so that all team members had an impact and were updated with developments equally.

Oliver Colebourne

In this project myself and Patrick led technology development, due to our interest in developing technical products. I led the website demo due to my experience with React web development. I also produced the video with Jack due to past video development experience. Reflecting on the project, overall I was happy with the sections I was involved in. With technology I could've kept clearer communication with other subteams particularly levels, to save time - since the technology offered several constraints to their work which needed identifying earlier.

Patrick D McGuckian

In this project I co-lead technology and lead business planning; and due to my interest in systemic design I took a leading role in the development of the system diagram and data flow chart. This meant I had a holistic view of the project so worked with other members of the team to assure all the features complemented each other and met our aims. With this view I was able to lead the refinement of our future scenario and system aims. In general I believe I worked well in this role, however upon reflection at times I may have been overly forward with my opinions in an effort to assure progress was being made - this is something I will work on in the future.