ICO Data Lives

Ethnographic Research

Final Report

October 2023

Executive Summary

Background

The ICO wanted to build a foundational understanding of the UK public and its attitudes, behaviours and beliefs around data and privacy. This research is intended to offer the ICO an empathetic view on how real people interact with their data. This understanding can be used to identify fruitful avenues for future research, as well as bring the voice of the customer into the heart of the ICO's decision-making.

Method

Ethnography is the study of people and cultures in their natural settings. It differs to qualitative research, which aims for a detailed understanding of conscious behaviour and opinion, and from quantitative research, which deals in statistical representation and breadth of understanding. We use film to understand what the UK public say, see and do when it comes to data, both consciously and unconsciously.

Sample

We spoke to 30 members of the UK public. Eight of the participants took part in the ethnography and spent 5-7 hours with a trained ethnographic filmmaker, observing their daily lives. The remaining 22 took part in a shorter, qualitative interview, which took a more deliberative approach. The research sample skews, deliberately, to more vulnerable members of the public, who are typically underrepresented in quantitative research.

The findings

Priorities and Lifestyle:

Culturally, people do not think explicitly about their rights, but rather base their assumptions on common sense and the social contract. In this context, decisions around data are not always taken by individuals, but rather by social networks, inner circles, and consensus. Our data lives are both digital and physical, and the public does not always make a distinction between the two.

Personal rights, data rights, and privacy

People do not always identify with their data risks; people who could experience harm may be unaware of these latent or "abstract" harms. As a result, there is no straightforward hierarchy of "more private" or "less private" data, but rather a wide array of situations in which a given piece of data might need protecting. When asked to think about their relationship with organisations, the public's data rights can feel conditional. People assume that organisations can simply argue back or ignore an exercise of these rights altogether. In this sense, the dense jargon of terms and conditions can be seen as a show of force from an organisation rather than a consensual agreement.

Understanding the future

The future is difficult for the public to grasp. Adoption of tech is a passive process: people may think about the technology they have to adopt, rather than want to adopt. As a result, people feel a lack of agency over the pace of change, and, as a result, the privacy implications of future innovations.

Table of Contents

A guide to reading ethnographic research

This report is predominantly based on findings from ethnographic research which is not intended to be representative.

Instead, it provides in-depth insights into the lives of a small group of participants. Their stories speak for themselves, but also hint at more universal experiences, both around data and around our culture. The reader may recognise aspects of these participants' lives in their own, or in other people. The reader can come away from this report feeling more connected to the UK's data users, with a more intimate understanding of their challenges, hopes and needs.

Throughout, the report we will use case studies to illustrate points made. A case study is a descriptive portrait of a participant who embodies a broader idea; they aim to turn broader, strategic insights into concrete, human stories.

This report will raise further questions and areas for analysis: it does not contain straightforward answers to the challenges the public face with their data. However, this research is longitudinal which will help monitor views over time and it will articulate those challenges as well as suggest future avenues for research.

Project Background

Project Background

Upholding the United Kingdom's public's information rights requires an **evidence-led approach.** The pace of social, economic and technological change means that the threats and opportunities around how people use, protect and share their data are changing in kind.

The **ICO25 strategic plan** outlines the purpose, objectives and values that the Information Commissioner's Office embodies. It calls on the ICO to continue safeguarding and empowering the public, enabling responsible innovation, and promoting openness in how data is used.

To achieve this, the ICO needs to develop interventions and actions based on **lived experience.** This report outlines the insights from the Data Lives Ethnography. It is a first step towards a comprehensive understanding of data users in the UK. It offers a foundational, **empathy-led** picture of what the UK public are thinking, feeling and doing about their data. It highlights where problem areas lie, and where further research would be valuable.

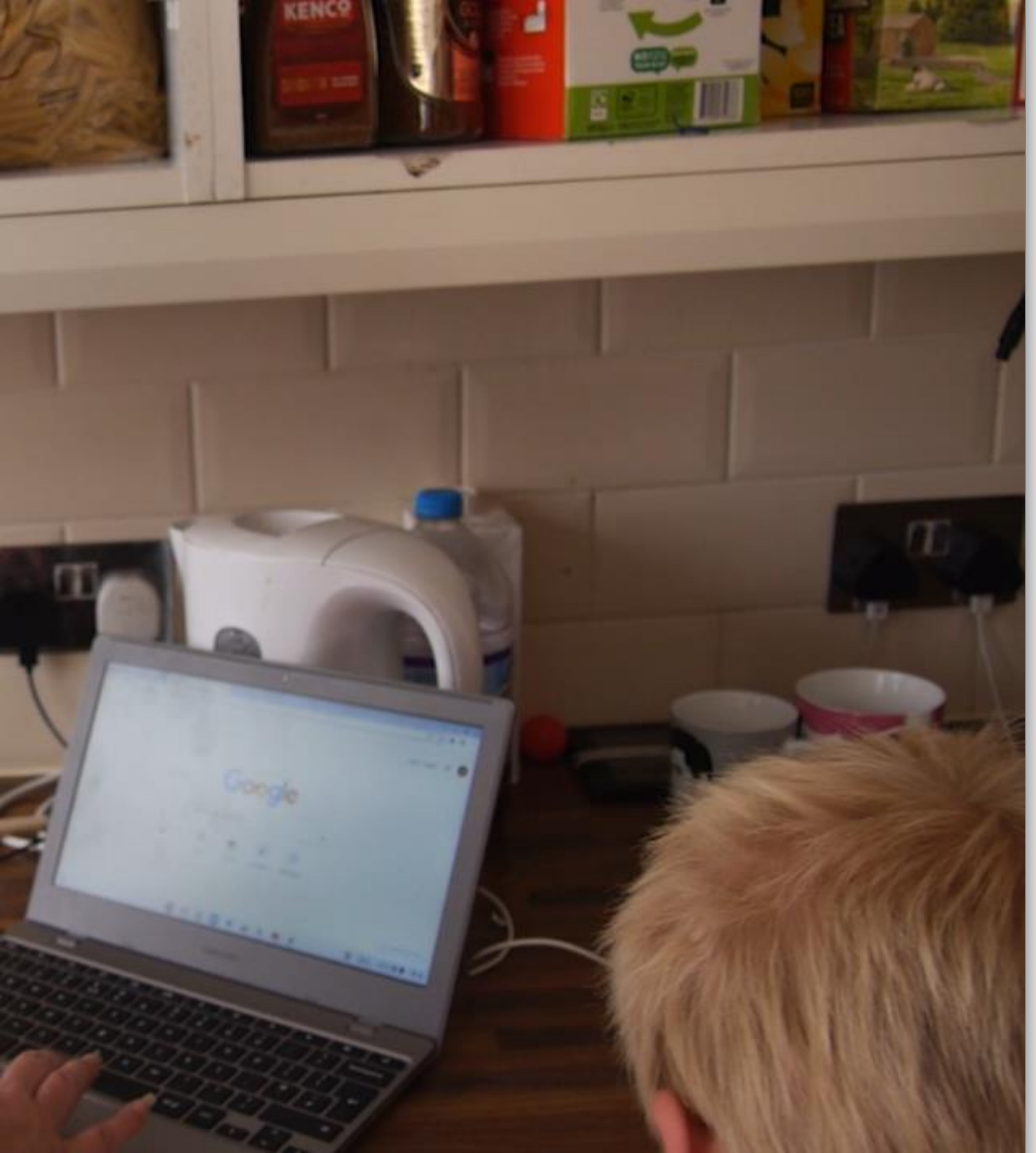
OBJECTIVES

1 To bring to life, through film, people's views and experiences of how they use personal information

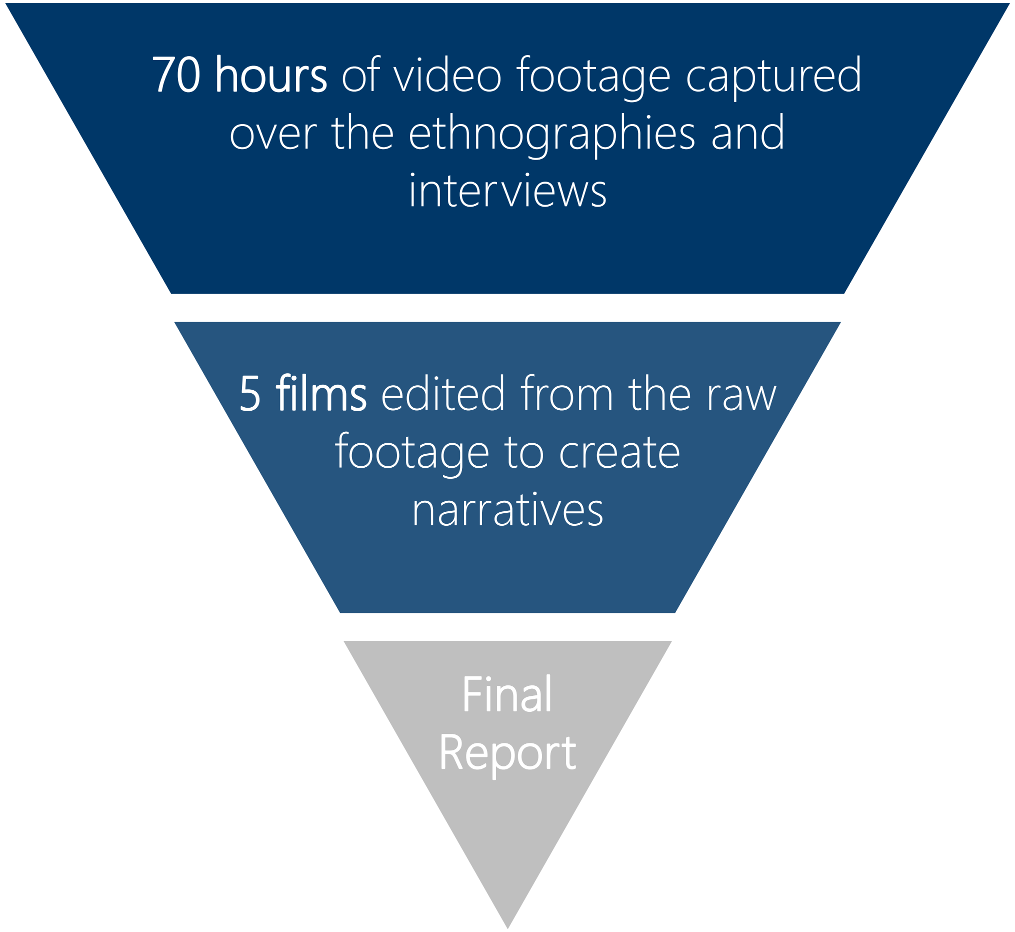
2 To learn the role that personal information plays in daily life, and how this differs demographically

3 To observe, through longitudinal research, how behaviours and understanding change over time

4 To establish unmet needs and sharpen the focus for future research conducted by the ICO



Using Film in Data Analysis



70 hours of video footage captured over the ethnographies and interviews

5 films edited from the raw footage to create narratives

Final Report

Methodology

Ethnography for empathy and depth

Ethnography is the study of people and cultures in their natural settings. Ethnographic researchers learn about human behaviour through direct observation, relying less on what people *say* they do, and more on what people do in practice as well as the context of their lives.

Ethnography's core strengths lie in the participant-led nature of the research method. Participants were given the space to show us what matters to them within the confines of the research topic. A great deal of time was spent with each participant, between 5 and 7 hours, meaning that their data lives could be explored both holistically and in depth.

In-depth interviews for deliberation and breadth

In-depth interviews were also conducted to understand consciously-held beliefs. What do people claim about their data usage? What are their opinions and perspectives about how organisations use their data?

The shorter time frame allowed for a greater number of interviews to be conducted. This meant that we could generate hypotheses about how different demographic characteristics influence beliefs and behaviours around data.

It should be noted that neither ethnography nor in-depth interviews are quantitative methods and therefore not statistically representative. As a foundational piece of research, our goal is to uncover the array of ideas, beliefs, behaviours and contexts that exist around data, not to assign prevalence to them.

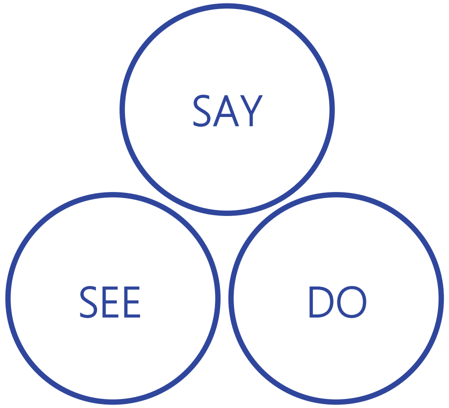
Ethnography: The observational study of people and cultures in their natural settings, bringing unconscious ideas to life

In-depth interview: A shorter, more direct conversation where explicit and conscious ideas are captured through discussion

All interviewers in this research are expertly-trained anthropologists and filmmakers. As researchers, they aim to empower participants to speak their mind and share their experiences openly.

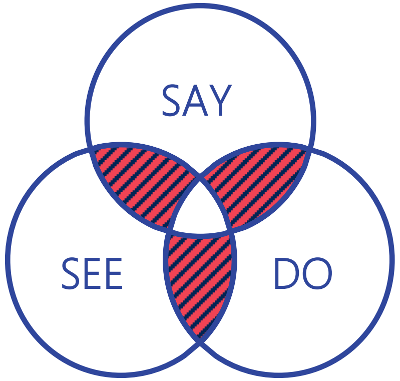
Analysis

Fieldwork



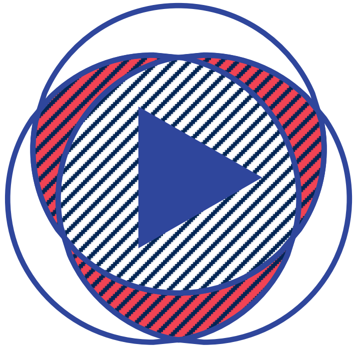
The research materials focussed on what people say, do and see. Film was used to collect data on how they behave, what they believe and what their cultural context looks like.

Analysis



Insights came from the crossover between what people say, do, and see. This meant identifying gaps or conflicts between what people say they do and what they do in practice, or exploring how what people see influences what they say and do.

Bringing insight to life



The insights were shared through storytelling, using edited films to provide a comprehensive narrative of each participant. **In this report, no stock photography is used:** imagery of real people interacting with their own technology and data is used to illustrate the insights and build empathy.

The process of ethnography

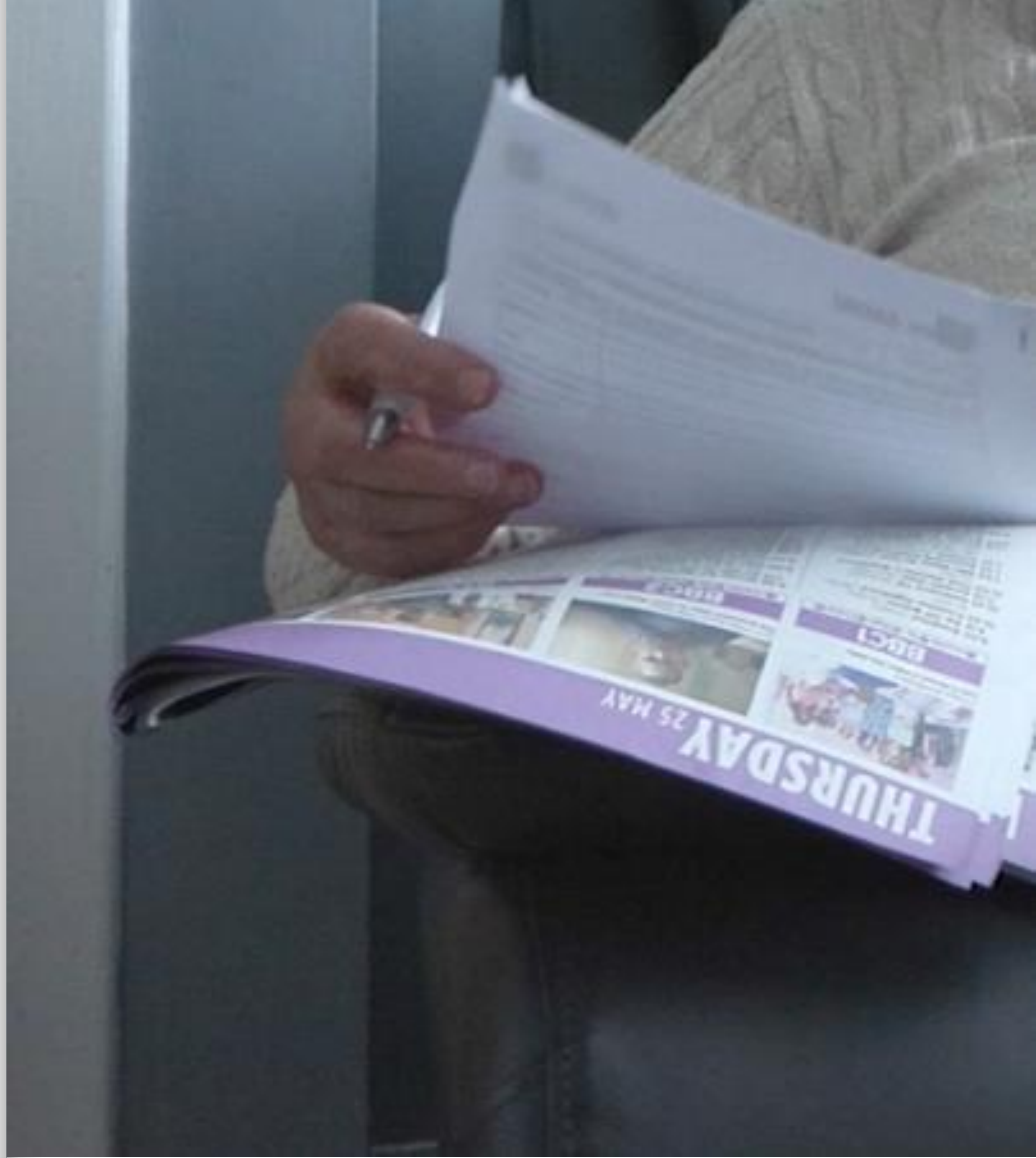
1 **Preparation:** A kick-off workshop was used to align on research objectives and define the scope and sample of the research. Thematic briefing guides were created to align on the most important questions to ask, and observations to gather in the field.

2 **Collection:** A trained researcher spent a day with each ethnography participant, or 90 minutes with each interview participant, using film to capture as much data as possible. In total over 70 hours of video data was collected.

3 **Thematic analysis:** Themes were identified through reviewing raw film to identify people's values and beliefs, observe how they interact with data, security, and privacy, and how context influences these values and actions.

4 **Analysis workshop:** The ICO were immersed in the footage and stakeholder expertise was leveraged to identify new themes versus existing knowledge.

5 **Final outputs:** This report, as well as five edited films, represent the final analysis of the data, and includes indications for where further research could be conducted.



A note on vulnerability:

This research sample includes multiple participants that self-identified as at risk of harm, such as a health condition.

These members of the public are often under-represented in quantitative studies. To understand the un-met needs of the public at large we need to amplify the voices of its most at-risk members. Qualitative research prioritises diversity of voices over statistical representation.

This research's definition of vulnerability drew from the FCA (Financial Conduct Authority) definition, which recognises vulnerability as a fluid, multi-layered state, rather than a fixed one. The definition is a starting point: there is no established rubric for "data vulnerability", but a definition that incorporates risk of harm from organisations in a holistic way is a valid place to begin.

In screening participants, we included circumstantial, medical and socioeconomic vulnerabilities, as well as indicators of compromised decision-making, such as addiction, in our quotas.

In addition to those who self-identified as vulnerable during the recruitment process, during the fieldwork some additional participants disclosed information that would class them as currently or previously at risk of harm.

In situations where a participant has requested, or it was felt appropriate to do so, pseudonyms have been given.

> "A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care" –– FCA, 2021

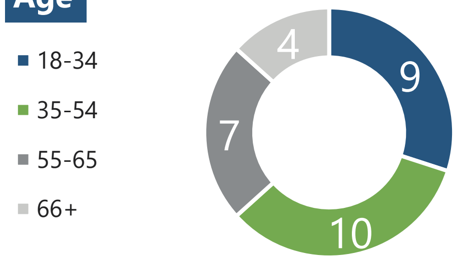
Our sample

30 Members of the UK public

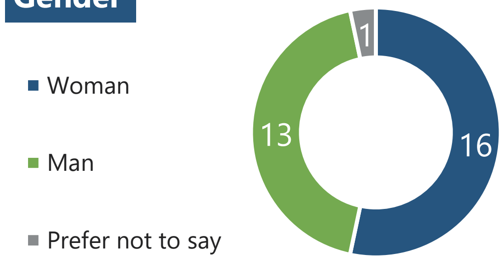
08 Filmed ethnographies

22 Filmed in-depth interviews

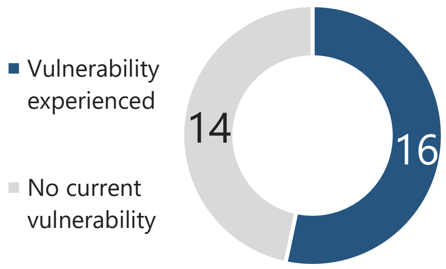
Age



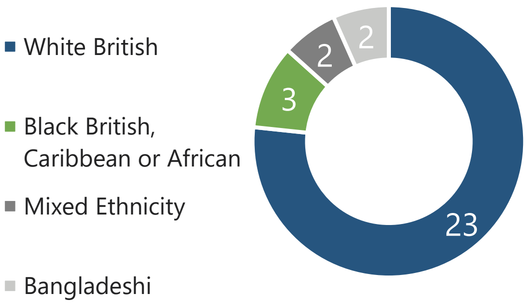
Gender



Vulnerability



Ethnicity



A minimum of four interviews took place in each of London, Belfast, Manchester, Scotland, Wales and Bristol. We recruited a spread of awareness of data protection, and a spread of usage of technology. Vulnerabilities included physical health conditions, economic precarity, mental health concerns and unpaid caregiving.

Meet the data user:

Some foundational notes about the UK public

The cultural context

The UK is a constitutional monarchy with an uncodified constitution. Our rights comprise both written laws and unwritten customs.

The public does not have an easy frame of reference for understanding **what their rights are**, or how to exercise them.

Unpicking "common sense"

Instead, as a culture, we expect most functions of organisations and government to operate according to **common sense and good faith.** This can make the comprehension and exercise of data rights feel unusual.

These understandings of reasonable behaviour can be highly personal: they may range from assuming that the company is processing no data at all, to simply assuming it is never transferred to a third party.

The tension arises when companies do not live up to the user's understanding of reasonable behaviour. Even if a company is acting within its privacy policy, the user may still feel let down or violated.

> A big company like Admiral, **of course** they're going to take care of your information, but they've never said that to me. I've just made that presumption
>
> - Tracy, 59, Stirlingshire

Competing priorities

The participants in this research – whether vulnerable or not – were under stress. Cost of living pressures, childcare responsibilities, difficulties with work-life balance all compete for attention with an individual's rights, data-related or otherwise.

We found that the challenge is that in multiple cases, data rights need to be asserted actively: this requires time and attention from the data holder, which many struggle with. **Data rights can be subsumed by competing priorities.**

> I'm saying all these things like 'security, security', but then I've used a PC for shopping where the antivirus has run out. Just because it's run out you don't think 'I'm not buying anything anymore.' **You want it, you're still going to put your details in.**
>
> - Desmond, 41, Manchester

Priorities & Lifestyle

Priorities and Lifestyle

Data privacy sits within a broader social context. How people live, work, play, care and study all influence their data lives.

Key Points

1 Culturally, people do not think explicitly about "rights". We rely on common sense to decide what is, and is not, proper behaviour from organisations.

2 Decision-making around data is not made by individuals, but by families, communities and neighbourhoods. This can mean conflict as much as compromise.

3 Our data lives are both physical and digital. The public do not make a distinction between "online" and "offline" privacy; the norms are the same and their goals draw from the same source.

4 Adoption of tech is a passive rather than active process. Participants in this research talked about technology they *needed* to adopt rather than technology they *wanted* to adopt.

> Facebook, Instagram, TikTok, but just **whenever the kids are asleep**, that's like a bit of me time rather than doing something more sociable.
>
> - Clara, 32, Manchester

The UK public has a diverse set of orientations towards technology

On the furthest end of the spectrum, one participant had never sent an email before, but in the main, **technology was strongly embedded in participants' lives.** Technology, along with the data sharing that comes with it, felt compulsory.

> You *can* live a life without technology... but it would be a **hard one.**
>
> - Drew, 65, Cardiff

> It's probably not great but it's just the way we live now. The only way to not have it like that is to live **off grid.**
>
> - Gwen, 44, Belfast

High tech usage

Sayeda (18, Manchester) is a young adult studying Nursing. She is a digital native and has developed a series of **workarounds** to keep her privacy safe. Sayeda creates spare email addresses to avoid spam in her main one. She is a frequent user of social media and is particularly careful about information she shares in the professional space of her nursing course.

Sayeda, 18, Manchester

Medium tech usage

Anna (41, Belfast) is a school assistant from Belfast. She's active on social media, partly driven by her many friends who live abroad. Her social media are set to **private** and she recently decided to stop posting photos of her son. Her son is a gamer, and is getting tech savvier than her, making it harder to protect him online.

Anna, 41, Belfast

Low tech usage

Caroline (59, London) doesn't use social media because she's worried she will accidentally upload photos from her phone or have her financial details stolen. She is very cautious and will give up on online shopping if she suddenly feels a surge of **anxiety.** She suffers from epilepsy and feels most at risk of being left behind because of technology advancement.

Caroline, 59, London

Technology is primarily intended for individual use, but within trusted circles, data is highly communal

Family dynamics and trusted circles

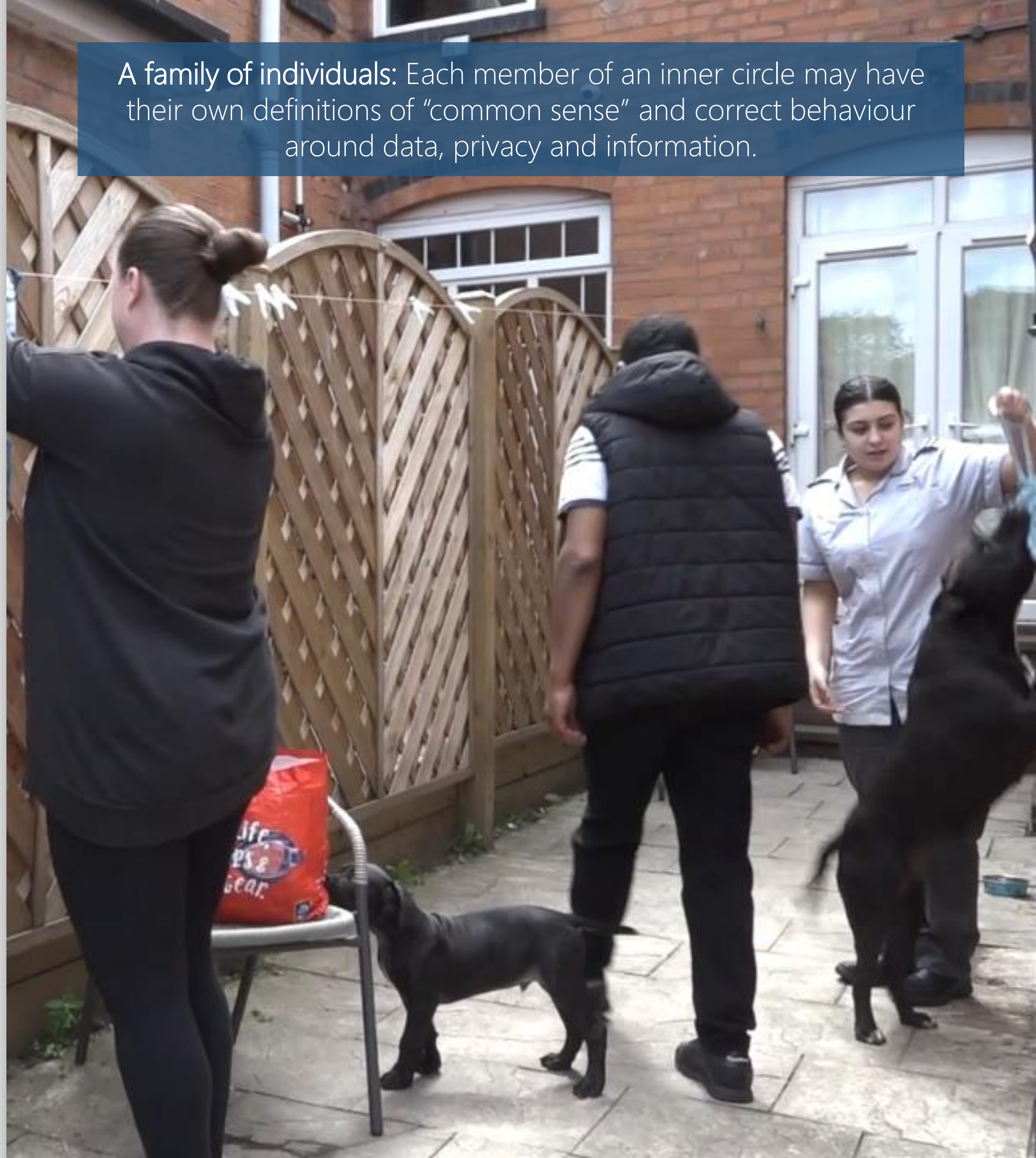
Across the public, passwords, devices, email addresses and logins are shared between parents, children, friendship groups and extended families. Families are an inner circle and trust each other implicitly, unless and until this trust is broken.

On the more at-risk end of this inner circle are **proxy users;** people whose data sharing and tech usage is mediated through another person. Again, because of this implicit trust, they do not recognise proxy usage as a vulnerability *per se*.

Inner circles look out for their more vulnerable members: children and those with a disability or set of adverse circumstances. They can differ on the best ways to go about protecting those in their care, but fundamentally want their loved ones to be safe and to have their dignity maintained.

In this context, families' relationship to online services, which often assume a single, autonomous user, can be strained. Participants have had children logging into Amazon accounts without their knowledge, or parents asking about embarrassing adverts on their children's streaming services.

Data services do not always recognise that behind each user sits a family or inner circle, which may have distinct and unique priorities for that service.



A family of individuals: Each member of an inner circle may have their own definitions of "common sense" and correct behaviour around data, privacy and information.

Beyond the trusted circle, participants share aspects of their lives more cautiously

Nosey neighbours, friends and employers

People are noticing when their neighbours install Ring doorbells or other surveillance tools. Participants talked about conflicts over "nosey" neighbours, or friends who take Snapchat videos of them without their consent.

While ideas around privacy are culturally-informed, "common sense" is not a settled concept, and people differ about the right ways to respect privacy. The same neighbour who gets accused of "curtain twitching" in one moment could be praised for spotting a burglar the next.

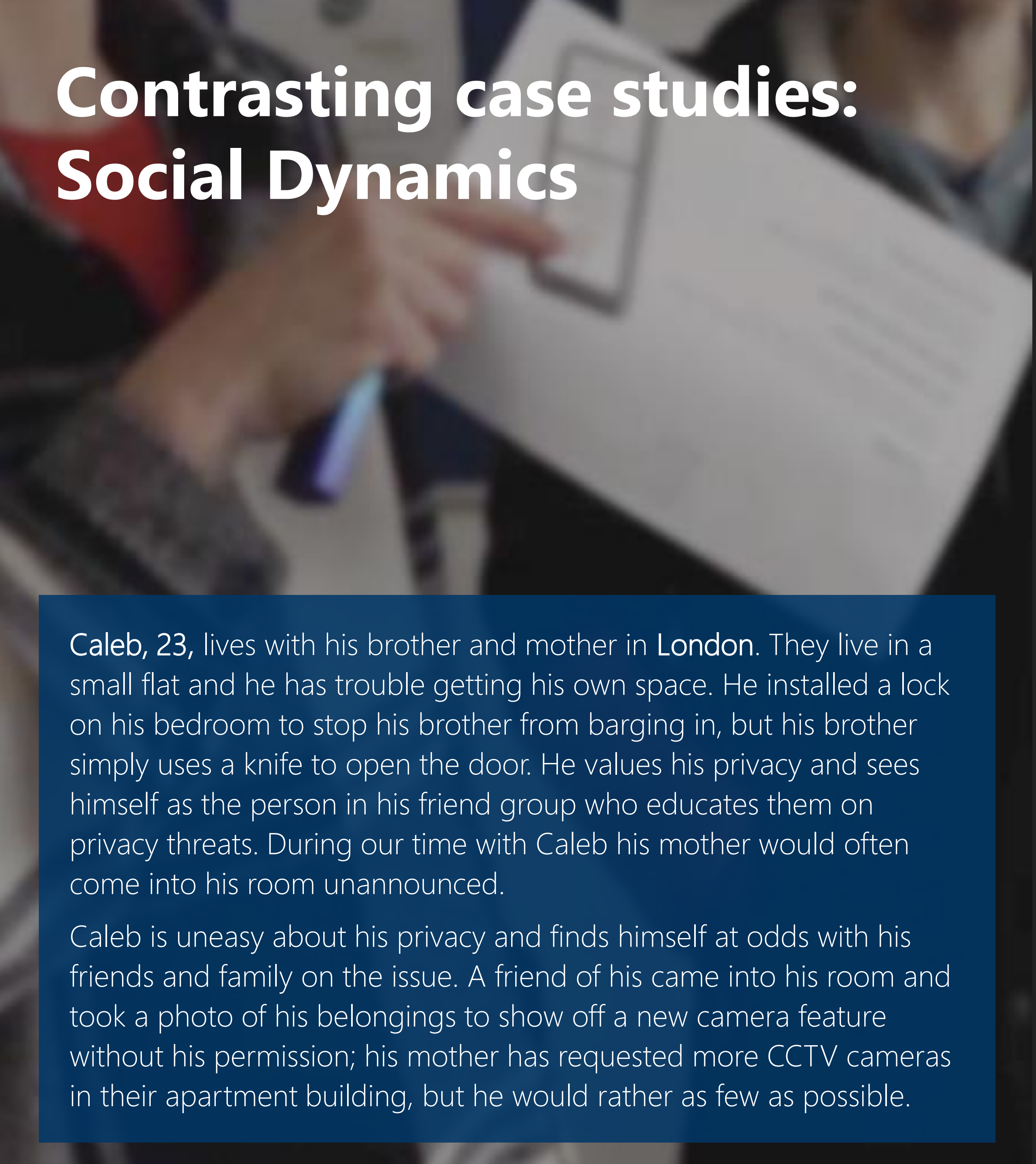
Data is communal but everyone brings their own set of assumptions to the table, as well as their own trade-offs around safety versus privacy. These don't always work in tandem.

Participants were particularly aware of privacy in the **workplace.** They argued that employers sit in a position of both care and authority and worry about the prospect of information being "used against them".

> That's my choice. That's because I want people to know without me telling them.
>
> \- Walter, 59, Bristol

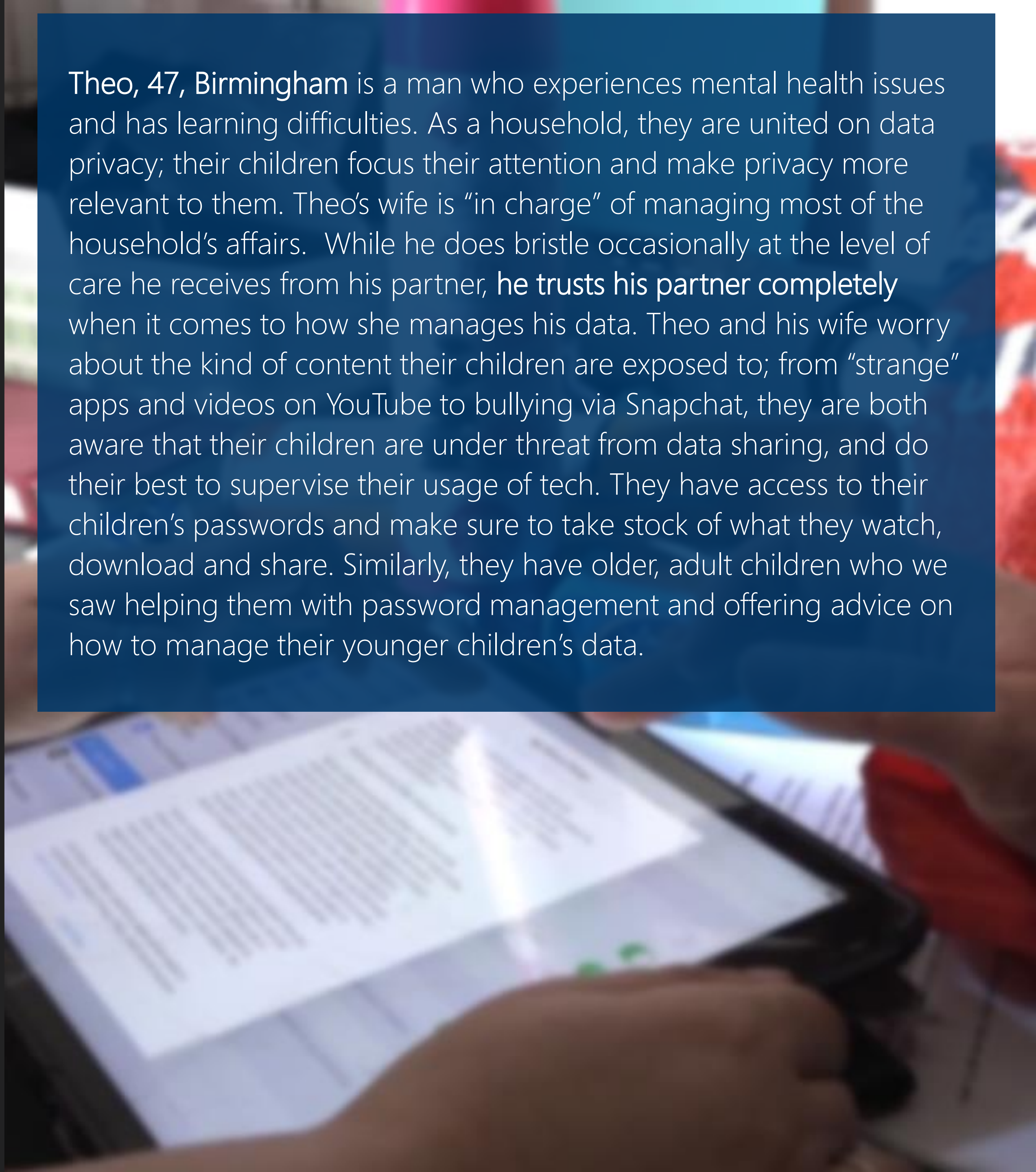
Walter, 59, Bristol, shares information about his political beliefs through flags. In doing this, he can let people know that he supports LGBTQ+ rights, as well as the monarchy, without having to disclose any further detail. He is cautious about how he shares information with those outside of his inner circle. His neighbours know the essentials of his political beliefs, while his family and friends may know about them in further detail.

Contrasting case studies: Social Dynamics



Caleb, 23, lives with his brother and mother in **London**. They live in a small flat and he has trouble getting his own space. He installed a lock on his bedroom to stop his brother from barging in, but his brother simply uses a knife to open the door. He values his privacy and sees himself as the person in his friend group who educates them on privacy threats. During our time with Caleb his mother would often come into his room unannounced.

Caleb is uneasy about his privacy and finds himself at odds with his friends and family on the issue. A friend of his came into his room and took a photo of his belongings to show off a new camera feature without his permission; his mother has requested more CCTV cameras in their apartment building, but he would rather as few as possible.



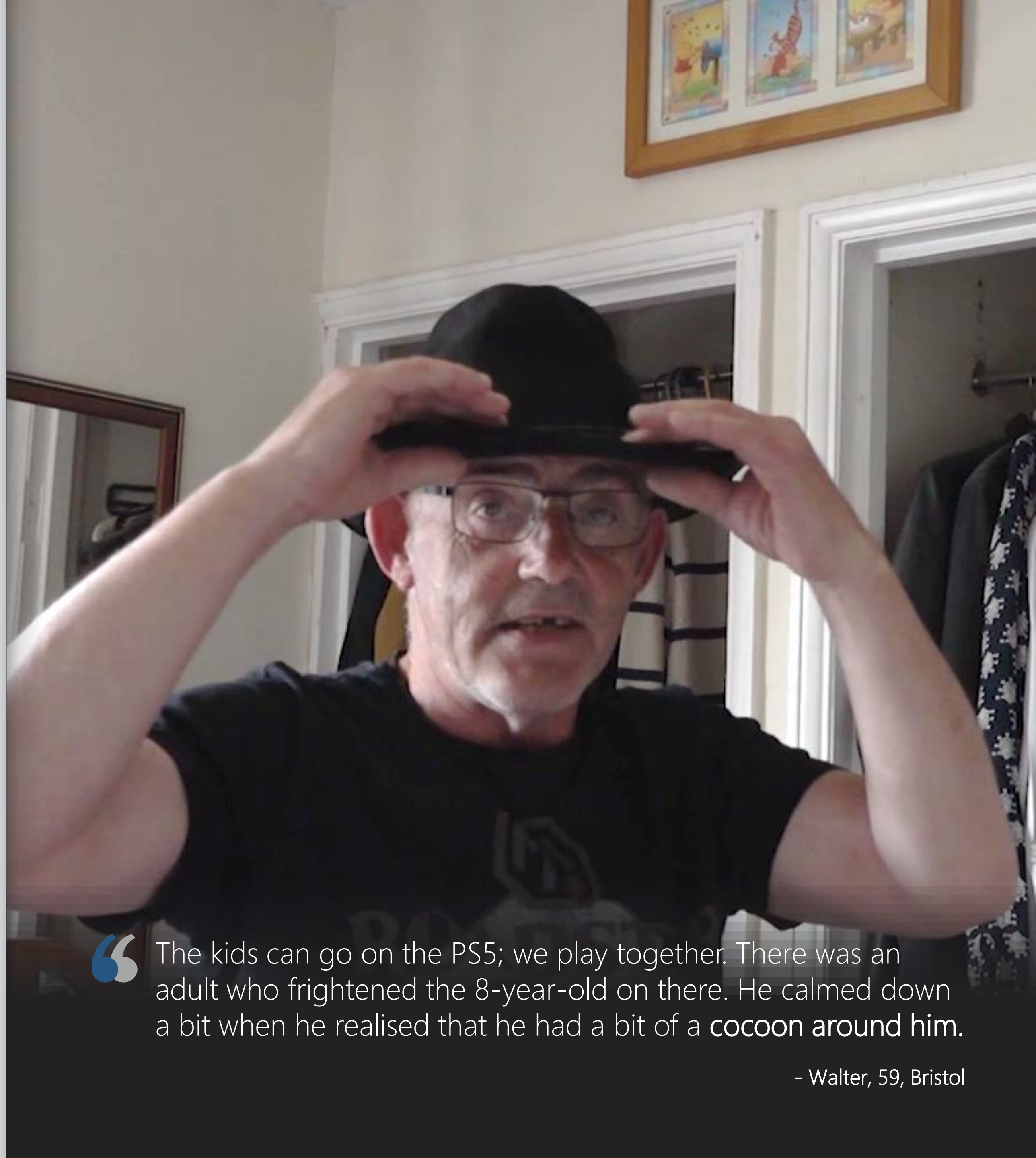
Theo, 47, Birmingham is a man who experiences mental health issues and has learning difficulties. As a household, they are united on data privacy; their children focus their attention and make privacy more relevant to them. Theo's wife is "in charge" of managing most of the household's affairs. While he does bristle occasionally at the level of care he receives from his partner, **he trusts his partner completely** when it comes to how she manages his data. Theo and his wife worry about the kind of content their children are exposed to; from "strange" apps and videos on YouTube to bullying via Snapchat, they are both aware that their children are under threat from data sharing, and do their best to supervise their usage of tech. They have access to their children's passwords and make sure to take stock of what they watch, download and share. Similarly, they have older, adult children who we saw helping them with password management and offering advice on how to manage their younger children's data.

Children are the primary focus of people's concerns; they want to protect them, but don't always feel equipped to do so

Parents struggle to keep up with the threats children face in 2023. Participants tended to find workarounds, rather than systematic solutions to a given problem. This is a reactive process, rather than a proactive one, and can leave parents and carers worried that there are unknown threats on the horizon.

After their son encountered a disturbing video on ***YouTube Kids,*** *Marcus (38, Cardiff) and his wife disabled the "child-friendly" version altogether; their son now browses the all-ages version of YouTube.*

Walter (59, Bristol) plays PlayStation with his younger grandchildren to supervise them as they interact with other people during their game. However, this is more around ***responding*** *appropriately to online trolls rather than preventing negative interactions to begin with.*



> The kids can go on the PS5; we play together. There was an adult who frightened the 8-year-old on there. He calmed down a bit when he realised that he had a bit of a **cocoon around him.**
>
> \- Walter, 59, Bristol

Data is rarely thought of exclusively in online terms, and people's goals and hopes for privacy are often drawn from their physical and social lives

Physical and digital lives

Our "real world" lives are conspicuous and tangible. Participants instinctively noticed when their homes were visible to a neighbour, or when their conversations were audible through a wall.

The privacy of the home is sacrosanct, and the privacy toolkit for physical space is more readily comprehensible: we know how to close blinds, cover laptop cameras, or how to spot CCTV in the street.

Skye (66, Stirlingshire) recently suffered a break-in and knew that CCTV could be reviewed to find the culprit (although ultimately this did not happen.)

A common battleground for physical privacy was the GP's waiting room. Participants were aghast that their health complaints were being disclosed by staff in a public forum.

However, while the physical world's privacy challenges are more apparent, this does not mean that digital privacy is any less valued. Its threats and potential harms are simply less clear.

> People get asked personal information at the [GP's] desk. **That isn't right.** I don't' believe they should be asking, and they certainly shouldn't be shouting it across the room."
>
> - Skye, 66, Stirlingshire

Data selves

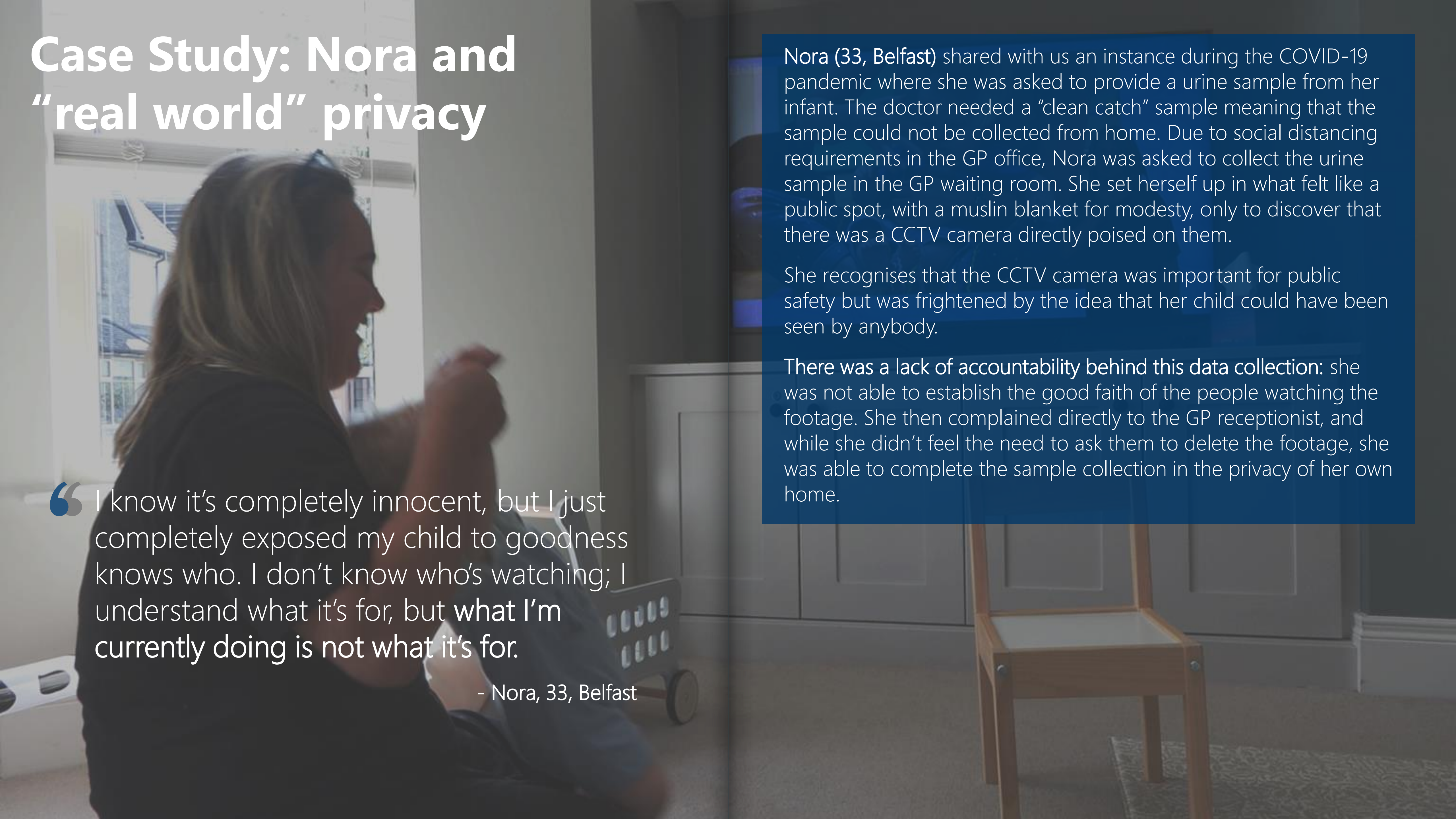
Participants did not talk about their privacy and data as segmented into "physical" and "online" territories. To the public, it is one coherent concept **drawing from the same set of underlying assumptions.**

In a sense, **people do not have "data lives"** - they have aspects of their lives that are (often reluctantly) transformed into data. Data is an abstraction of the self: it can be commoditised and mishandled, or it can be an accurate and meaningful reflection of the data owner.

When participants talked about being empowered through data, they referred to sharing information in order to be understood (or rewarded) meaningfully and **on their own terms.**

> I share information online about myself in the sense that I give other people **my experience** of living with Lupus, I'll recommend different clinics or ways to look after myself.
>
> - Darren, partner of Simon, 65, London

Theo (47, Birmingham) data lives in both digital and physical spaces. Both in his kitchen cupboard and across devices like his phone and iPad.



Case Study: Nora and "real world" privacy

> I know it's completely innocent, but I just completely exposed my child to goodness knows who. I don't know who's watching; I understand what it's for, but **what I'm currently doing is not what it's for.**
>
> \- Nora, 33, Belfast

Nora (33, Belfast) shared with us an instance during the COVID-19 pandemic where she was asked to provide a urine sample from her infant. The doctor needed a "clean catch" sample meaning that the sample could not be collected from home. Due to social distancing requirements in the GP office, Nora was asked to collect the urine sample in the GP waiting room. She set herself up in what felt like a public spot, with a muslin blanket for modesty, only to discover that there was a CCTV camera directly poised on them.

She recognises that the CCTV camera was important for public safety but was frightened by the idea that her child could have been seen by anybody.

There was a lack of accountability behind this data collection: she was not able to establish the good faith of the people watching the footage. She then complained directly to the GP receptionist, and while she didn't feel the need to ask them to delete the footage, she was able to complete the sample collection in the privacy of her own home.

Data empowerment is not (consciously) on people's radar.

People are aware that they are *benefitting* from data sharing, perhaps through convenience, discounts or a well-tailored advertisement, but they don't feel empowered. The data collection model they experience day to day feels transactional at best, and invasive at worst.

Some don't particularly *want* to be empowered through data: it is sufficient that they use technology to access daily necessities like banking, food, or employment.

Achieving the ICO25 goal of empowering people through data will require a closer understanding of what "empowerment" means for the public and to the ICO as a regulator. A few promising threads emerged from this research:

1. Authenticity

We are social animals. People are willing to share data about themselves in ways that reflect how they see themselves and their values. We saw people filming TikTok's of their children, sharing stories of illness on forums, or expressing their political opinions through flags.

2. Transparency

Transparency precedes any empowerment from data sharing because people need to know, upfront, how data is being used and why. This may be why people did not mention feeling empowered by data, or knowing what it would look like if they were. They simply did not feel equipped with the requisite knowledge.

3. Reversibility

People's circumstances change. Some people have been sharing data through the internet since childhood. We observed that some people do not always stand by their decisions. It can feel as though it's too late to take control of one's own data profile, as though all the major decisions have already been made.

> Sometimes I feel more in control when I *don't* share things about myself, although that's not really in my nature.
>
> \- Ben, 56, Birmingham

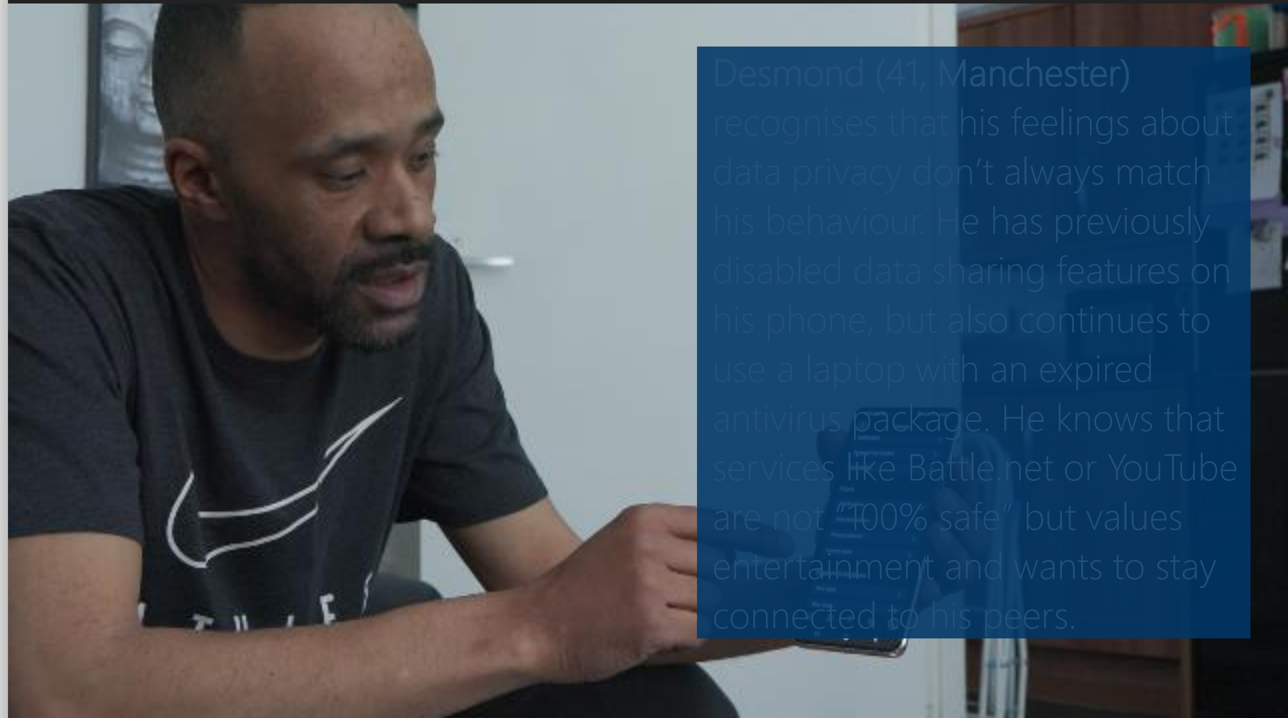
People currently do not feel in control of where technology is going

People tend to think about what they ought to use technology for, not what they would like to be using technology for.

This is not to say there are not positive examples of proactive and meaningful usage of technology. We saw people derive a lot of value from a range of things including the simplicity of 'unwinding through scrolling', using "BookTok" (getting book recommendations from TikTok), and Instagram parenting channels that offered childcare advice that aligned nicely with the participant's values.

The challenge for safeguarding the public's data rights is that much of the data being shared is done on "autopilot". **How might the UK public engage with technology and data with more intent and purpose?** And furthermore, what can be done to make this engagement simpler and more frictionless?

Nora (33, Belfast) takes a lot of pleasure from watching parenting content on Instagram; she sees this as an active, purposeful process of learning. It's something she wants to do, and she researches and vets the best content to watch.



Desmond (41, Manchester) recognises that his feelings about data privacy don't always match his behaviour. He has previously disabled data sharing features on his phone, but also continues to use a laptop with an expired antivirus package. He knows that services like Battle.net or YouTube are not "100% safe" but values entertainment and wants to stay connected to his peers.

Personal rights, data rights & Privacy

Personal Rights, Data Rights & Privacy

Talking about rights did not come naturally to participants. This section is about the assumptions and behaviours that underpin how we keep data safe.

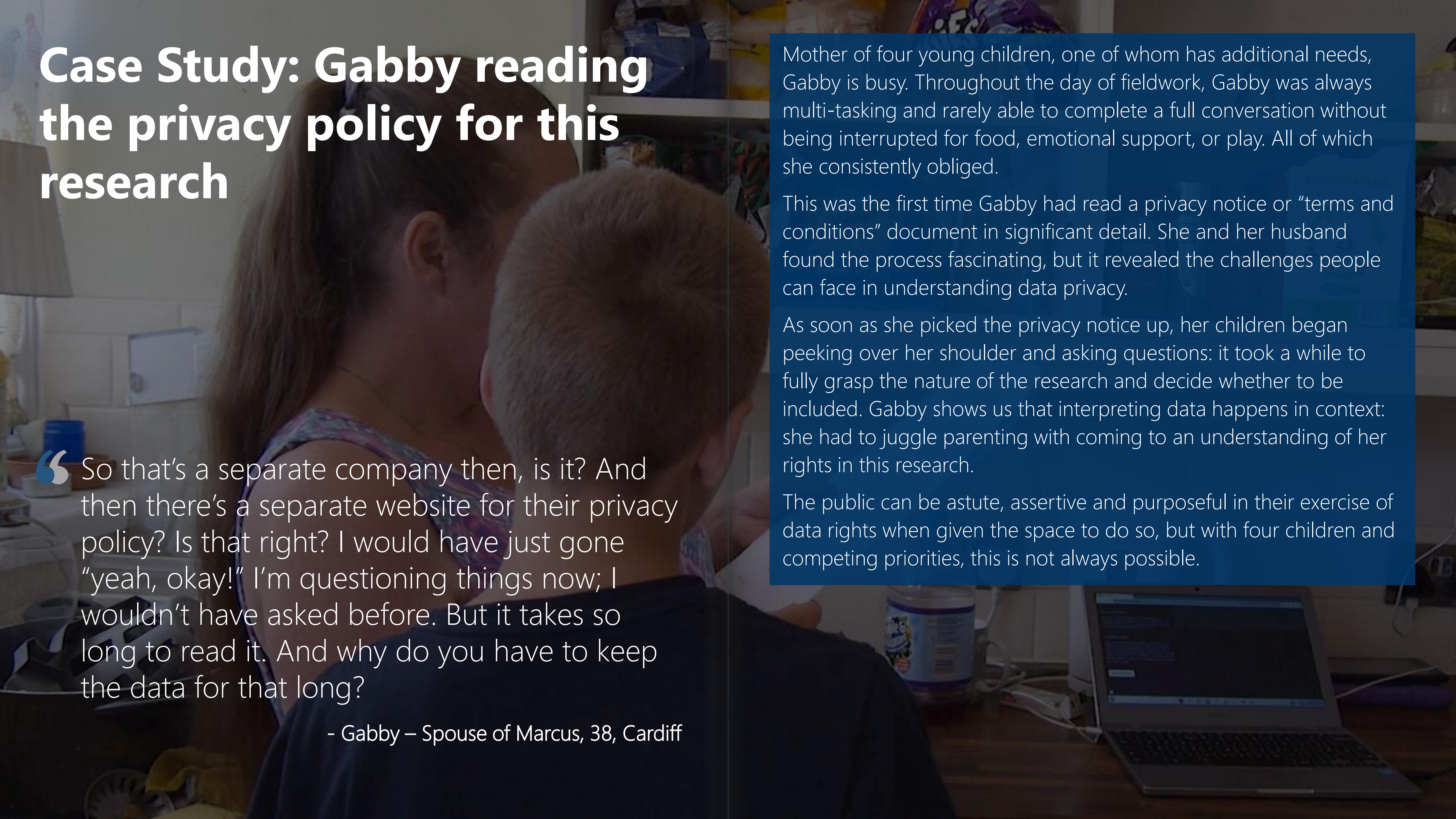
Key Points

1 **The public draw their expectations for privacy from cultural and social norms, not the law.** Tensions emerge when legal rights clash with "common sense" assumptions.

2 **People do not always identify with their data risks.** People who *could* experience harm due to a particular life circumstance or vulnerability may be unaware of latent or "abstract" harms.

3 **Privacy driven by context.** There is no straightforward hierarchy of "personal" versus "public" data, but rather a wide array of situations in which a given piece of data might need protecting.

4 **Data rights feel conditional.** Participants assume that organisations can argue back against an exercise of data rights or ignore one altogether.



Case Study: Gabby reading the privacy policy for this research

> So that's a separate company then, is it? And then there's a separate website for their privacy policy? Is that right? I would have just gone "yeah, okay!" I'm questioning things now; I wouldn't have asked before. But it takes so long to read it. And why do you have to keep the data for that long?
>
> - Gabby – Spouse of Marcus, 38, Cardiff

Mother of four young children, one of whom has additional needs, Gabby is busy. Throughout the day of fieldwork, Gabby was always multi-tasking and rarely able to complete a full conversation without being interrupted for food, emotional support, or play. All of which she consistently obliged.

This was the first time Gabby had read a privacy notice or "terms and conditions" document in significant detail. She and her husband found the process fascinating, but it revealed the challenges people can face in understanding data privacy.

As soon as she picked the privacy notice up, her children began peeking over her shoulder and asking questions: it took a while to fully grasp the nature of the research and decide whether to be included. Gabby shows us that interpreting data happens in context: she had to juggle parenting with coming to an understanding of her rights in this research.

The public can be astute, assertive and purposeful in their exercise of data rights when given the space to do so, but with four children and competing priorities, this is not always possible.

People hold organisations to moral rather than legal standards of propriety

Trust and its limits

People fall short of trusting organisations wholesale, least of all those that collect and use data for marketing or analytical purposes.

It is a social norm to be sceptical of data processors. Caleb argued that TikTok was being monitored by the Chinese government; Malcolm went further, telling us that social media was "the devil." But, from Drew's perspective, an organisation would have to act with actual malice in order to harm him or breach his data rights.

As a culture, we trust these organisations to a point, but no further. A repeated theme among participants was the idea that organisations will not go "too far" with their data collection. Despite what can sometimes feel like cynicism towards organisations and their data ethics, the public does assume that there are lines they will not cross.

However, the question of what "too far" means in practice was unclear in people's minds. They assume that organisations will act within the limits of the law, but awareness of these legal obligations was low. The public does not always know what respect for privacy they are owed, where their rights end or organisations' responsibilities begin.

> I don't think there is anything on Google that could harm me really. **Why would they?**
>
> \- Drew, 65, Cardiff

Professionalism and data

In the absence of a clear understanding of rights and responsibilities, people defaulted to heuristics around how certain organisations might be handling their data.

There was a strong sense that more established organisations behaved with more decency around data. Homebase is a household name, and for Gwen, the idea that they would be sharing data with any third party felt unlikely.

The challenge here is that this trust is untested and fragile as a result: Gwen does not know what Homebase do with her information, and as such, she cannot assert her own needs for how it is treated.

> **I trust professionalism**. That's why I tend to use bigger firms and reputable companies; they give me security and make me feel a bit safer.
>
> \- Raleigh, 34, Birmingham

People's stances towards personal data vary according to what feels private in a particular moment and context

Contexts and contradictions

We found that there is no straightforward hierarchy of importance for personal information. "Special category" data like a person's political views can be public knowledge or a private matter, depending on the social context they inhabit. For some, these beliefs might attract ridicule, whereas others might be celebrated.

Organisations did not seem to account for this context. While the public struggle to understand how organisations amalgamate their data, they do have a sense of what *could* happen if certain data was shared at the wrong time and place.

But people can lose track of their intentions in the complexity of the data sharing landscape. Malcolm may say that social media is the devil, but he has enjoyed sharing TikTok's of his children in the past.

For much of the public, their data lives may feel uncomplicated; there are no past mistakes to conceal or vulnerabilities to mask, whether in the context of a job interview or in online forums. Sometimes, *any* data can be weaponised: a participant's daughter was bullied over Snapchat using whatever data they could find on her as ammunition.

To say we have "nothing to hide" is sometimes a function of **privilege**, or of a context that makes their data sharing feel straightforward and low-stakes.

In differing contexts on the same data, a person's name can be freely known or deeply private

NPCC
ACRO Criminal Records Office
Home About Services Publications Contact News
Search
Subject access
Access your information

Ben (56, Birmingham) has tried to have his name taken off the police national computer following a criminal conviction. In multiple contexts, he is cautious about having his name associated with his past, particularly now that he has started a small business.

Gabby, spouse of Marcus (38, Cardiff) did not consent to the use of her name in this research and has been given a pseudonym. She uses her true name when shopping online, and on social media, but did not want her name used *either* in public or private presentations of the research.

Argos | Order online today for fa
argos.co.uk
Shop
Trending
Shop our latest voucher codes

The daughter of Theo (47, Birmingham) did not take issue with her Apple Watch having access to her name, even in association with her email address and health information collected by the device. She feels as though there is little to hide here; nothing is exploitable or "of interest" to someone else.

Those with vulnerabilities don't always identify as "at-risk" from data

Who are the data vulnerable?

Decisional vulnerabilities:

We spoke to people whose Internet usage was mediated through another person, whether in helping them to set up their device, or in using the device on their behalf altogether. Participants in this research were happy with the arrangement; it did not occur to them that their relationship with their proxy could change, or that the proxy – though well intentioned – could be exposing them to data harm.

Reputational vulnerabilities:

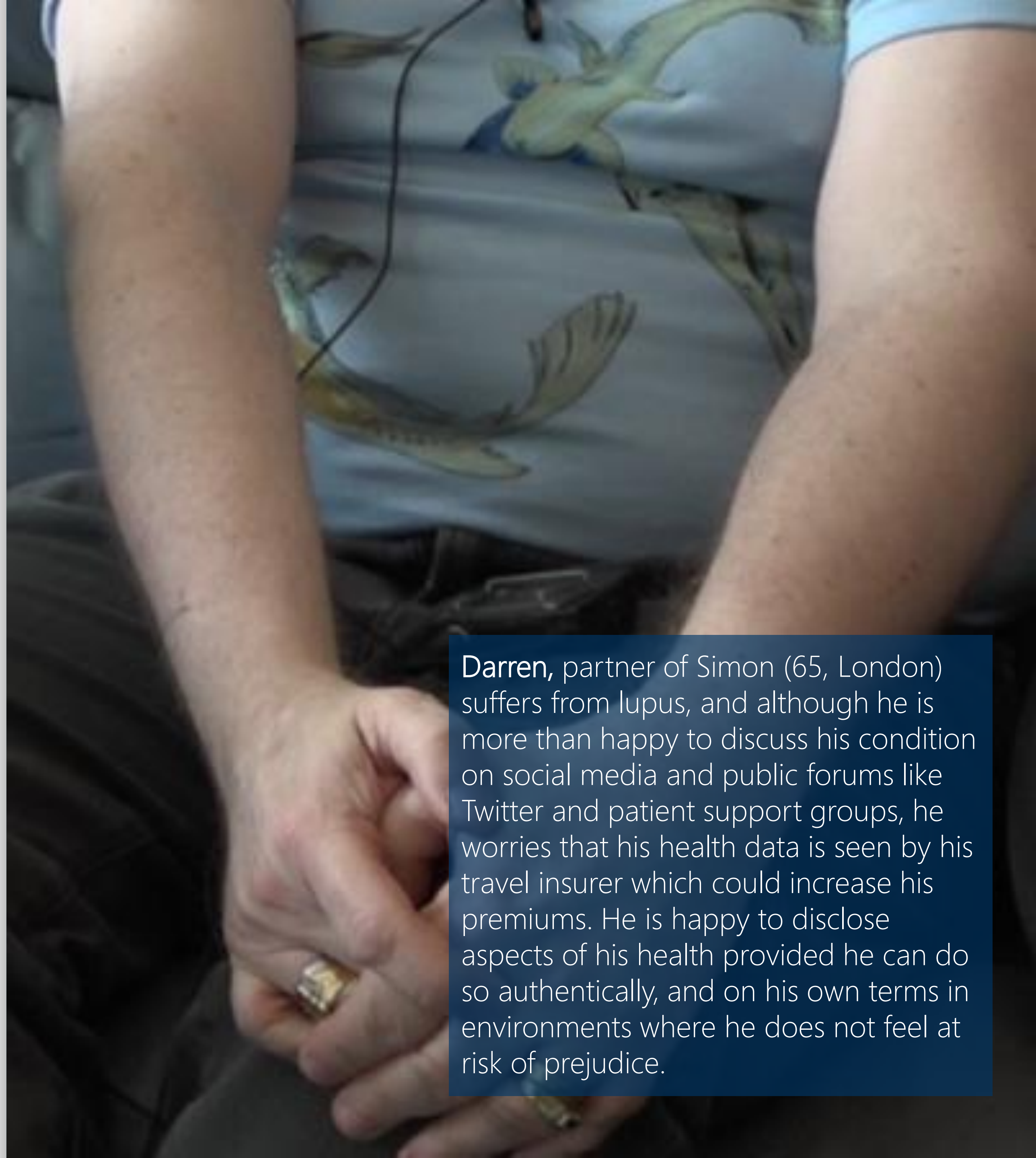
We met people with pasts they would rather forget, or aspects of their lives they would rather keep private. One participant was particularly worried about the prospect of other people discovering chat histories with friends where, as a teenager, they would share "off-colour jokes."

Group vulnerabilities

Participants had experienced discrimination and prejudice as a result of their health conditions, although a wider analysis of the public will highlight other instances of marginalisation. For one participant who suffers from Gilbert's Syndrome, he feels he has no choice but to disclose this in his CV, in part due to the requirements of his Universal Credit arrangement and the need for accommodations in his working environment, even though he worries about discrimination.

Vulnerable by victimisation

Participants in this research had fallen victim to active attempts to use their data against them such as fraud, bullying and relationship abuse. In each case, the impact was devastating and the role of their personal information in their victimisation was entirely unexpected.



Darren, partner of Simon (65, London) suffers from lupus, and although he is more than happy to discuss his condition on social media and public forums like Twitter and patient support groups, he worries that his health data is seen by his travel insurer which could increase his premiums. He is happy to disclose aspects of his health provided he can do so authentically, and on his own terms in environments where he does not feel at risk of prejudice.

> **In a way, I don't feel protected,** because I know things still go to my previous address that I haven't lived in for 15 years. Where is the cut-off point for things to feel safe? It's worrying.
>
> - Clara, 32, Manchester

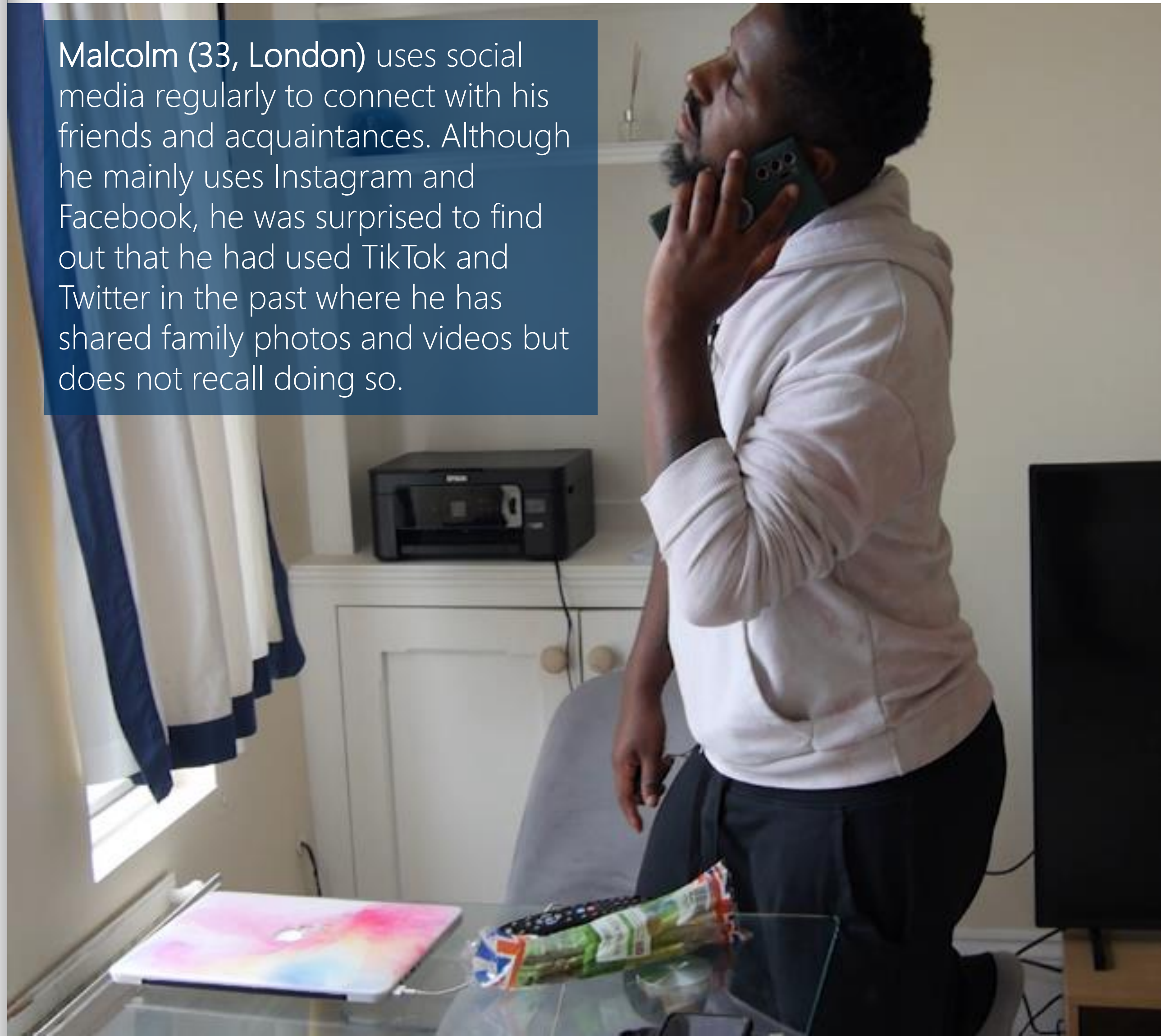
Being at risk of harm is a fluid state, but data feels fixed and immutable

We observed that people don't always feel that they are risk of harm, rather it is dependent on their life stage and current situation.

People at different life stages reflect on their past, wanting to hide personal information that they may have once shared, and there is a sense of tension between their intentions at the time and their values. However, with the convenience that technology offers, it overran their values at the time. For example, we observed people regretting their decisions to accept cookies or marketing emails from long ago and struggling to correct the situation later.

Even decisions made during moments of decisional vulnerability (including childhood) feel difficult if not impossible to rectify. For example, we observed how some participants had shared personal information on social media such as location check-ins that they have forgotten about and don't know how to delete.

People are also experiencing challenges where some are unemployed and are spending more time online as a distraction therefore oversharing at times. Meanwhile, others who are busy balancing parenthood and work life rely on the convenience of online shopping to save them time resulting in their banking information saved on various websites.



Malcolm (33, London) uses social media regularly to connect with his friends and acquaintances. Although he mainly uses Instagram and Facebook, he was surprised to find out that he had used TikTok and Twitter in the past where he has shared family photos and videos but does not recall doing so.

The public struggle to understand the nuances of data protection law

Overestimation and underestimation

People have noticed the implementation of the GDPR in their daily lives, primarily by observing that their permission is being asked for data collection.

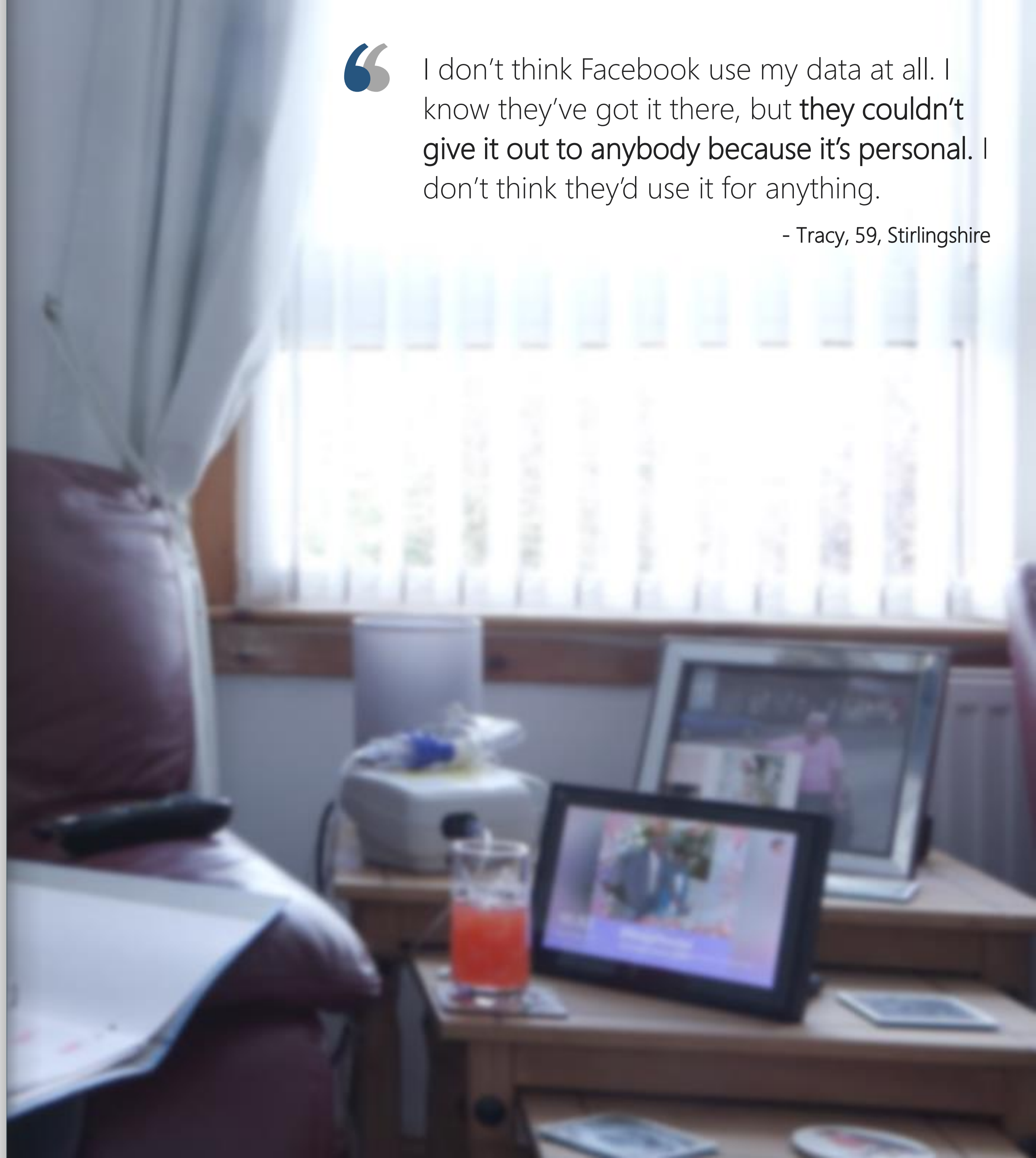
However, we observed real differences in how people interpret the dynamics of consent under the GDPR. People talked about not having a choice but to accept cookies in order to access their favourite websites.

There is significant confusion in what the GDPR means for people in practise. Participants, including those who reported a stronger knowledge of data protection, tended to overestimate or underestimate the extent of protection they were afforded under the law.

On the underestimating side, there was a stubborn belief that organisations can, fundamentally, do what they like. People described the possibility of organisations ignoring consent processes altogether and simply taking the data they felt they needed.

Others overestimate the degree to which the GDPR has protected them. There is a strong assumption that the law outright prohibits certain forms of common data collection whether consent is given or not. People told us that Facebook is not allowed to share their personal information at all, and when faced with the reality that they are, they are alarmed.

There is a difficult intersection here between our common sense and the law. Common sense and the social contract tell us that organisations cannot act against what we feel are our interests. The law tells us that they can, if permission is given.



> “I don't think Facebook use my data at all. I know they've got it there, but **they couldn't give it out to anybody because it's personal.** I don't think they'd use it for anything.
>
> - Tracy, 59, Stirlingshire

In this context, data rights feel fragile, as though they can be signed away with a click

The pessimism problem

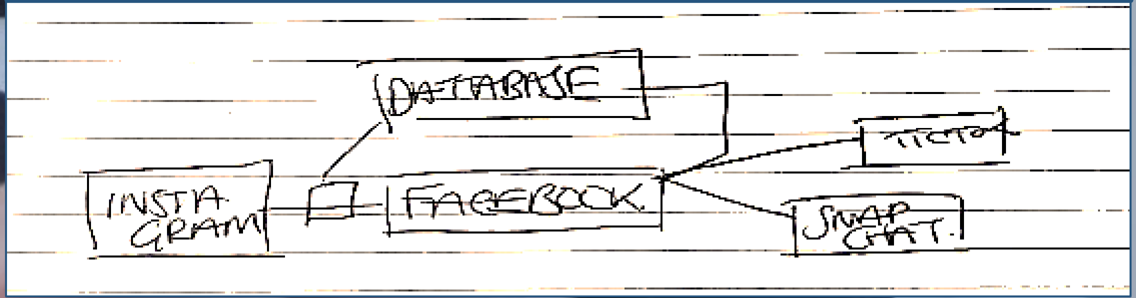
An important theme in speaking to participants was **the say-do gap** around organisations and data sharing.

People *say* that organisations can be indifferent towards their data privacy needs. *In practice*, we saw those same people continue to engage with the organisation and supply data to them on request. Mistrust of an organisation does not always lead to action to re-take control; pessimism can lead to inaction rather than data empowerment.

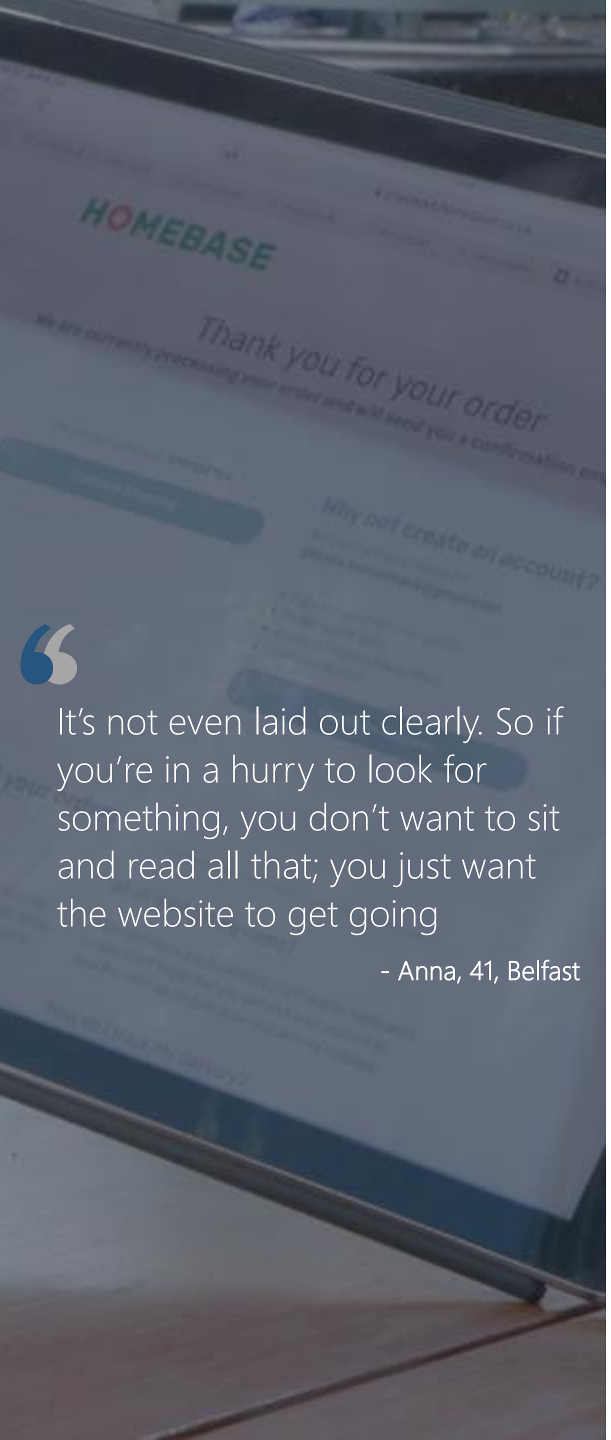
Participants would continuously refer to "third parties", "the database", or "the system", taking their information and sharing it with other third parties, or other systems. A consent process that could feel empowering can instead feel disheartening. Tailored advertising on social media becomes an unpleasant reminder of data shared while the children took over the iPad, or while the user was simply too busy to double-check what they were signing up for.

We observed participants personal information including their bank details on different websites or having 'autofill' options. Some did not know how their data appeared, how to 'undo' it but also found the convenience and simplicity outweighed what felt like a lot of work to understand and undo. This is where the moral code of sensibility steps in: people hope that organisations will keep their details safe.

"The Database" - People struggle to understand where their data lives once it's been shared



> Yes, it's important that everybody looks after their personal information, but you don't really know who has it…you're not under control of it!
>
> - Gwen, 44, Belfast



> It's not even laid out clearly. So if you're in a hurry to look for something, you don't want to sit and read all that; you just want the website to get going
>
> \- Anna, 41, Belfast

Convenience is currently driving people's online behaviour

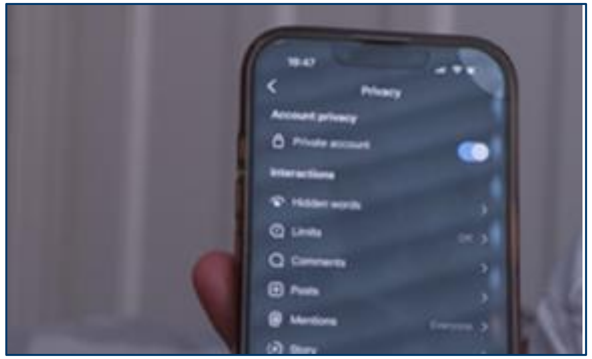
People are leading busy lives and are reliant on online services to serve their needs – and with technology constantly advancing, the convenience that is offered to people will continue to develop.

People do feel that the responsibility falls to them to keep their data private, but they wish it didn't need to. Convenience overpowers this responsibility, and once people have shared their data with an organisation, their sense of control over it feels lost.

People feel powerless after sharing this data with organisations. We observed a strong sense of despondency in the face of frequent requests for data sharing.

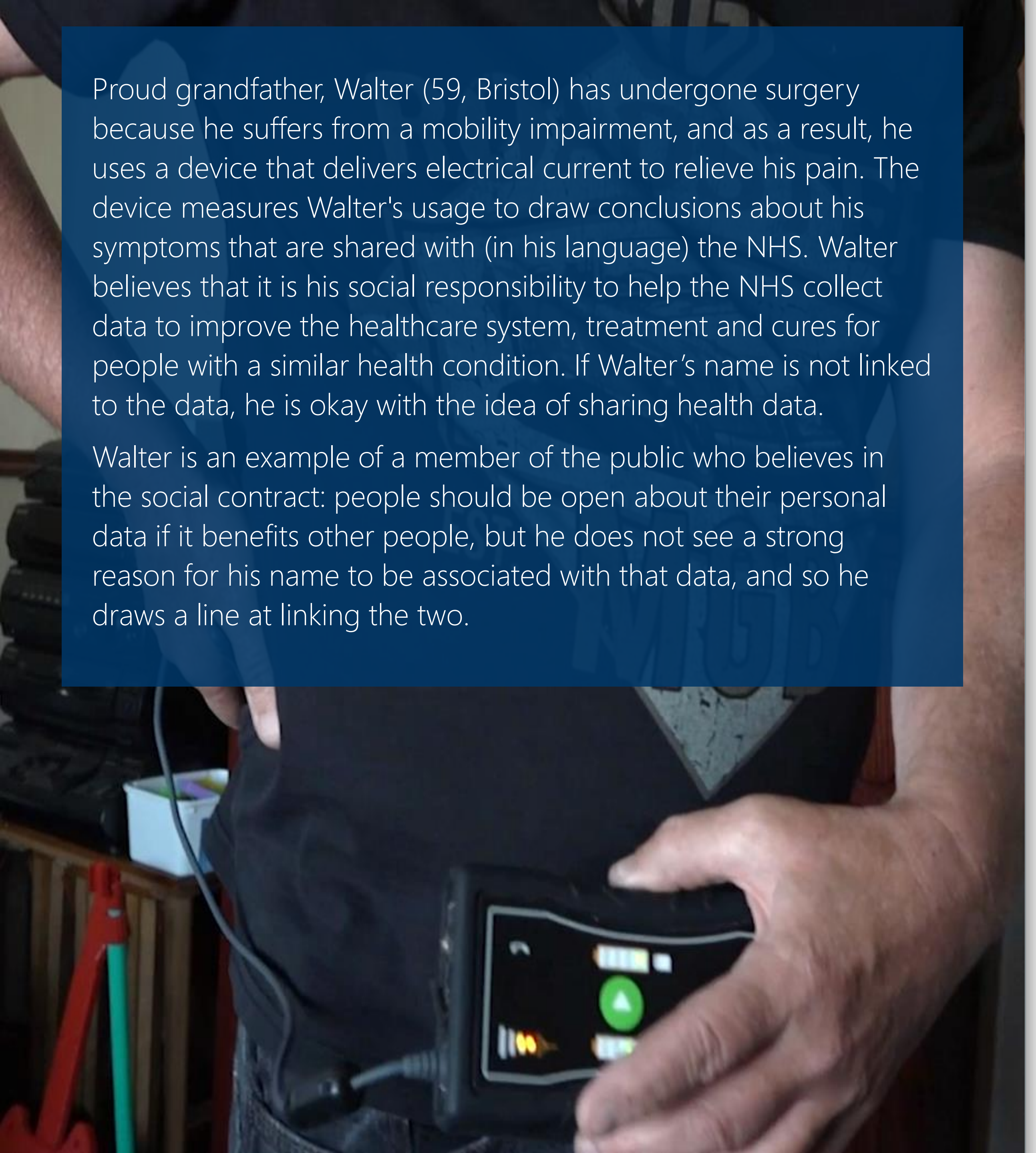
Some experiences observed that are leading people to give their information easily:

Feeling forced to accept cookies on websites in order to use it, which results in people sharing personal information. For example, Anna (41, Belfast) does not fully understand what cookies are for, how to reject them, or if she can even proceed to the website without accepting them. She feels that organisations deliberately make it harder for you to reject cookies to access personal information and she does not know what to do to change this.



Agreeing to terms and conditions without reading them because the language used lacks clarity, is difficult to understand, and is lengthy. Instead, people choose to simply scroll quickly to accept and proceed to the website. For example, Ella (22, Cardiff) uses Snapchat daily but has never read the T&C's because it is overwhelmingly long.

Registering an email on e-commerce websites to receive discounts on first purchases. For example, Clara (32, Manchester) used to share her email in exchange for discounts, however, this resulted in being spammed with emails and advertisements from unfamiliar websites. Now she is reluctant to share her email because she does not understand how other retailers have received her information.



Proud grandfather, Walter (59, Bristol) has undergone surgery because he suffers from a mobility impairment, and as a result, he uses a device that delivers electrical current to relieve his pain. The device measures Walter's usage to draw conclusions about his symptoms that are shared with (in his language) the NHS. Walter believes that it is his social responsibility to help the NHS collect data to improve the healthcare system, treatment and cures for people with a similar health condition. If Walter's name is not linked to the data, he is okay with the idea of sharing health data.

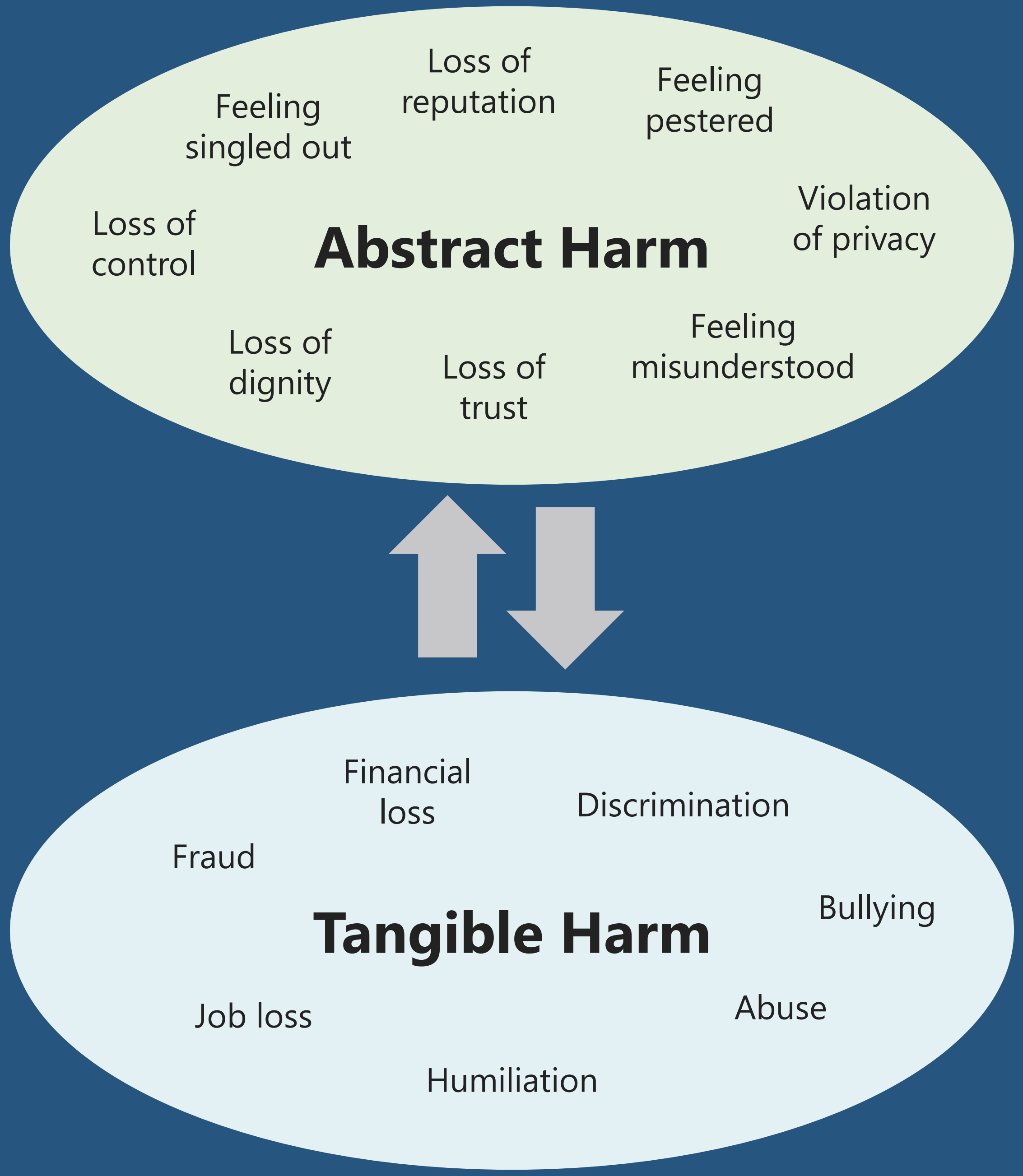
Walter is an example of a member of the public who believes in the social contract: people should be open about their personal data if it benefits other people, but he does not see a strong reason for his name to be associated with that data, and so he draws a line at linking the two.

People are concerned about linkages drawn between data as much as individual points of data

People discerningly share their personal information, choosing which organisations they want to share with or not. For this reason, it can feel unacceptable for organisations to share data on a person's behalf. We observed this across multiple participants where they explained that they use various social media platforms but share specific information on one and not the other.

Malcolm (33, London) showed us how on Facebook he shares minimal information, whereas on Instagram he feels more comfortable sharing more personal photos of himself and his life. However, Malcolm noticed that his information on Facebook appears on Instagram and struggles to understand how his data transferred from one platform to the other. He wonders if this is what happens across all organisations that he's given his personal information to.

On the contrary, when the data being shared is for the greater good, such as sharing health data, people are comfortable doing so. People feel this is their social responsibility. However, there is a worry when health data are combined with their name and date of birth. For example, we observed in multiple participants that they look at the bigger cause when it comes to health data, and as long as there is no reference to who they are, they willingly share their medical data.



Data harms are not always tangible: they range from the abstract to the tangible, and we saw participants worry about both

Participants in this research expressed concern over "linkages" being drawn between different aspects of their data. Identifiable information combined with behavioural, health or financial information, for instance, was felt to create the risk of both concrete and abstract harms.

Tangible harms are those which impact a data user in an immediate and acute way. This is not, however, to say that participants did not worry about more latent forms of harm, such as loss of dignity, reputation or control.

These **abstract forms of harm** were simply more difficult to conceptualise:

- Are the data processors mocking or thinking less of the user based on the data they shared?
- Is the organisation singling their data out compared to other customers?
- Did the organisation listen to them or surreptitiously act against their wishes?

The public do wonder about these questions, but competing priorities can push them to focus on the most readily obvious, concrete harms.

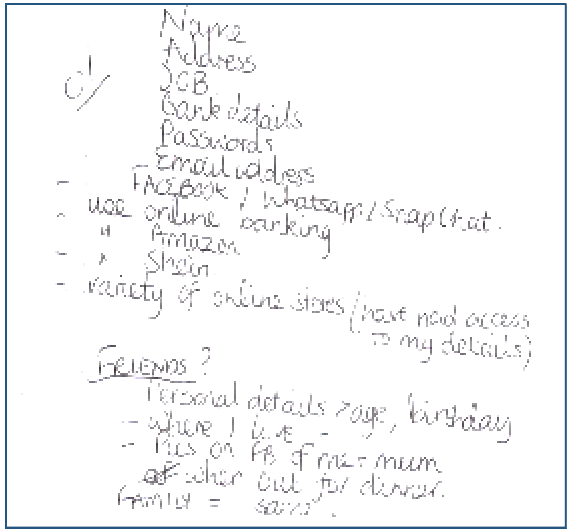
The border between abstract and tangible harms is permeable. Tangible harms can feel distant if the data user is not immediately at risk of them, and abstract worries can become very real when they occur.

A major challenge for people is “undoing” their previous data sharing

Participants were asked to recall the different places they previously shared their personal information. When realising the extent of data they have provided to different organisations, people worry about how to undo it.

Accounting for all the personal data people have shared is difficult work: it takes time and effort that people simply do not have.

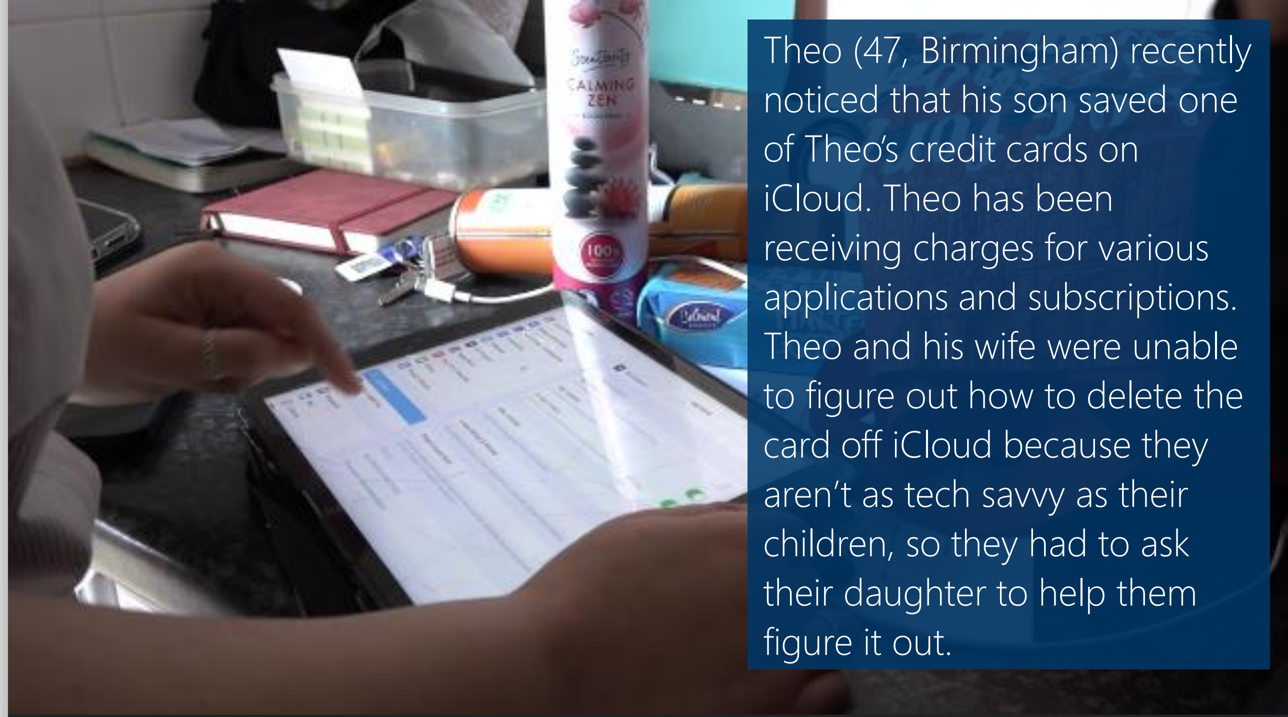
There was a common theme whereby people remembered several examples of when they have shared data unintentionally, or a member of their family has done so – but figuring out how to undo that sometimes seems impossible. We observed across multiple participants instances where they have saved their bank account details on websites with no recollection of doing so but were unable to go back and change that. Participants who shared devices amongst their inner circle also experienced similar situations where their personal information was saved in places they weren’t aware of and became anxious figuring out how to undo that.



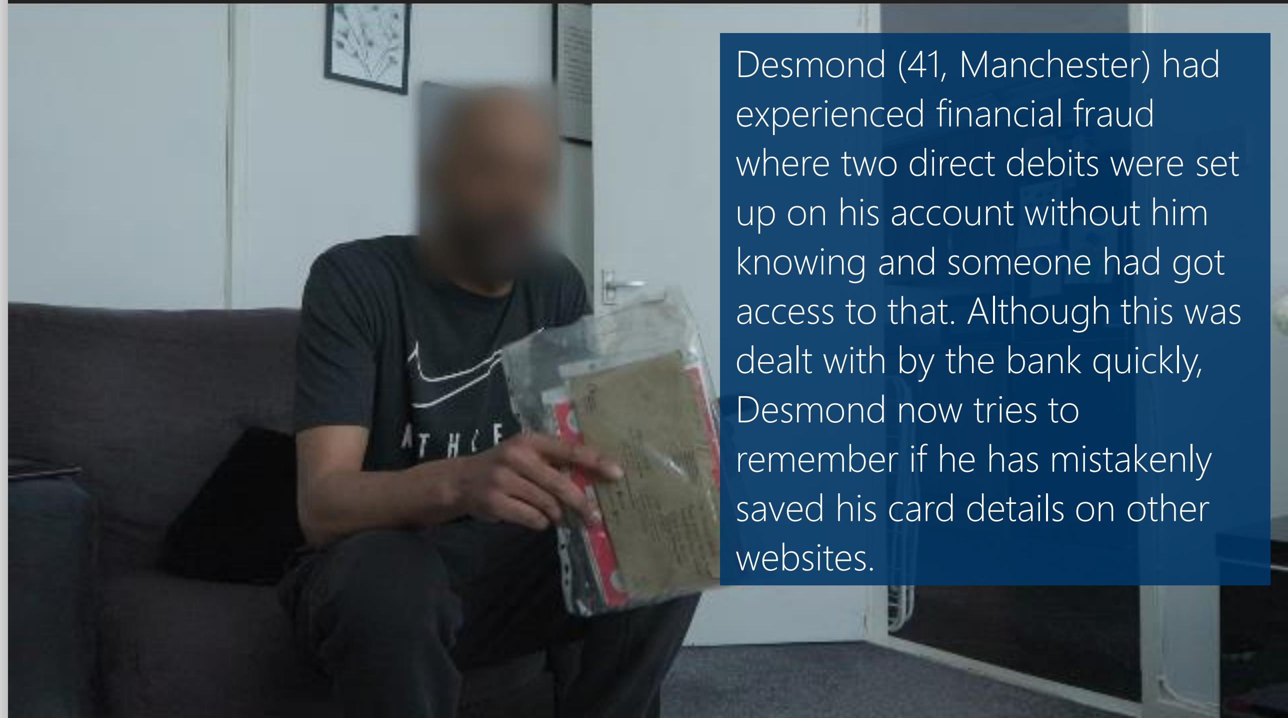
Name
Address
DOB
Bank details
Passwords
Email address
- FACEBOOK / Whatsapp / Snapchat.
- use online banking
" Amazon
- " Shein
- variety of online stores (have had access to my details)

FRIENDS ?
Personal details > age, birthday
- where I live -
- Pics on FB of me = mum
~~of~~ other out for dinner.
Family = same.

Data map of where one of the participants think their data is at



Theo (47, Birmingham) recently noticed that his son saved one of Theo’s credit cards on iCloud. Theo has been receiving charges for various applications and subscriptions. Theo and his wife were unable to figure out how to delete the card off iCloud because they aren’t as tech savvy as their children, so they had to ask their daughter to help them figure it out.



Desmond (41, Manchester) had experienced financial fraud where two direct debits were set up on his account without him knowing and someone had got access to that. Although this was dealt with by the bank quickly, Desmond now tries to remember if he has mistakenly saved his card details on other websites.

Exploring terms & conditions with participants revealed a lack of knowledge, but also a lack of trust

In the main, participants felt *able* to read and interpret terms and conditions around data sharing; the challenge is more around a lack of desire to do so, and a lack of faith that reading the information will empower or help them.

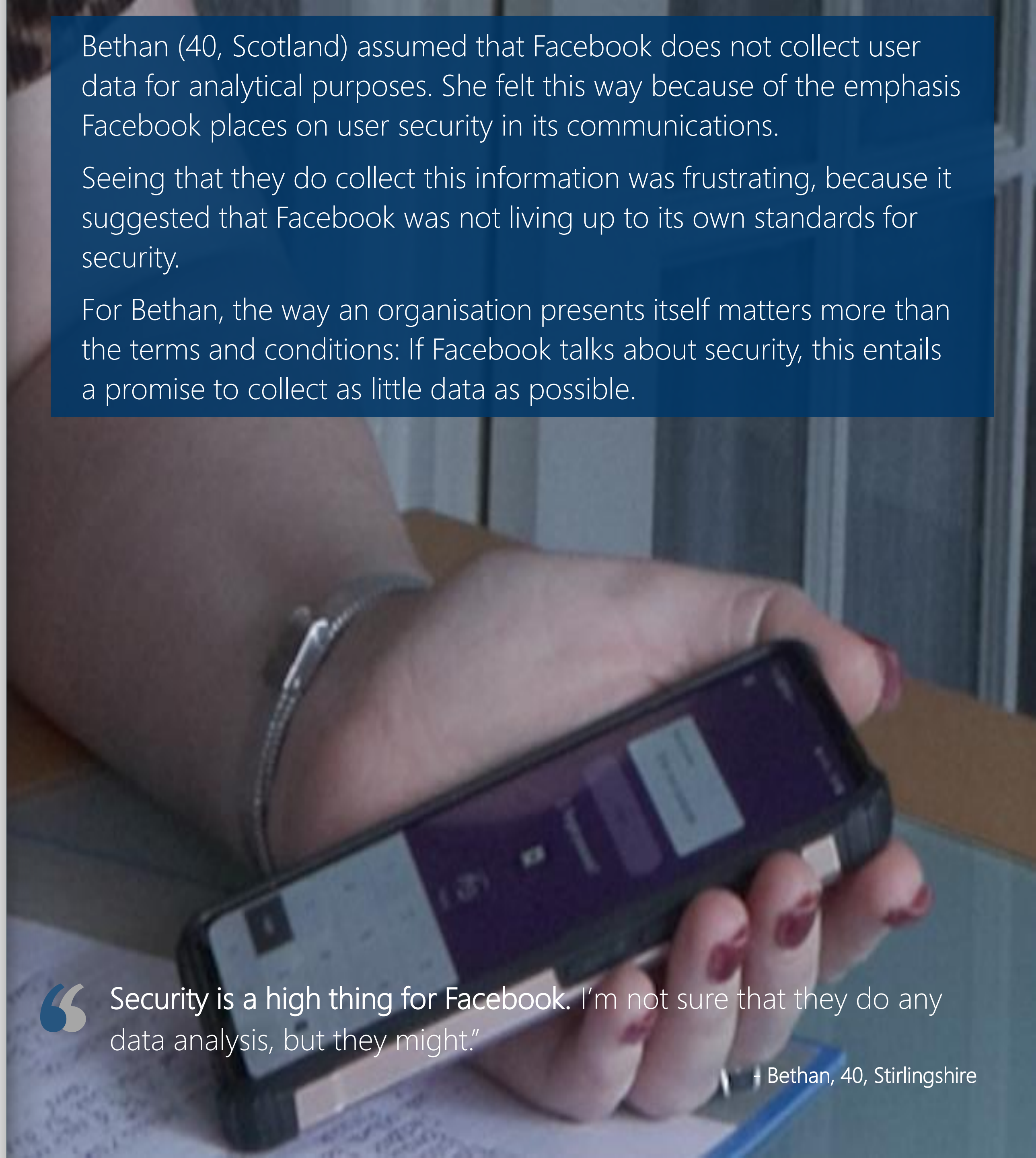
Terms and conditions feel more like a show of force from an organisation; a statement of what the organisation *will* do (or, perhaps, what it already has been doing) and what the user must simply accept. In participants' view, reading privacy notices and terms and conditions felt less like a request for information and more of a demand. The relationship feels hierarchical: reading privacy notices did not create the impression of a partnership of equals.

Indeed, reading the "fine print" in these terms and conditions shook participants' faith in companies they trusted: not for any passage in the text, but because an organisation that they assumed operated on goodwill was in fact relying on "legalese".

As a result, participants struggled to unpick exactly what data compromises or trade-offs they were signing up to. People expect organisations to collect information with restraint and consistency. The phrase "need to know" was a common one in this research. They expected organisations to have a valid and intuitive purpose for each form of data collected, taking no more and no less than what they need to provide a good service.

While this can include analytics and marketing information (with sufficient transparency), fundamentally the public worry that organisations are collecting data they want, or might want, rather than data they need.

> Fine prints should be banned. Anything that's important, that's where they put it."
>
> - Desmond, 41, Manchester



Bethan (40, Scotland) assumed that Facebook does not collect user data for analytical purposes. She felt this way because of the emphasis Facebook places on user security in its communications.

Seeing that they do collect this information was frustrating, because it suggested that Facebook was not living up to its own standards for security.

For Bethan, the way an organisation presents itself matters more than the terms and conditions: If Facebook talks about security, this entails a promise to collect as little data as possible.

> Security is a high thing for Facebook. I'm not sure that they do any data analysis, but they might."
>
> - Bethan, 40, Stirlingshire

Understanding the Future

Understanding the future

As people work to reconcile and maintain control over their data in the present, understanding future threats or opportunities feels overwhelming

Key Points

1 **The public expect the ICO to predict and signpost abstract or difficult-to-predict harms**. They do not always have the time or knowledge to anticipate the worst-case scenario.

2 **In the absence of specific information about future tech innovations, people default to first principles.** Public good, clarity of purpose and good faith are important proof points.

3 **Trade-offs in data privacy are made with incomplete information.** Predicting the long-term consequences of data sharing can feel overwhelming if not impossible.

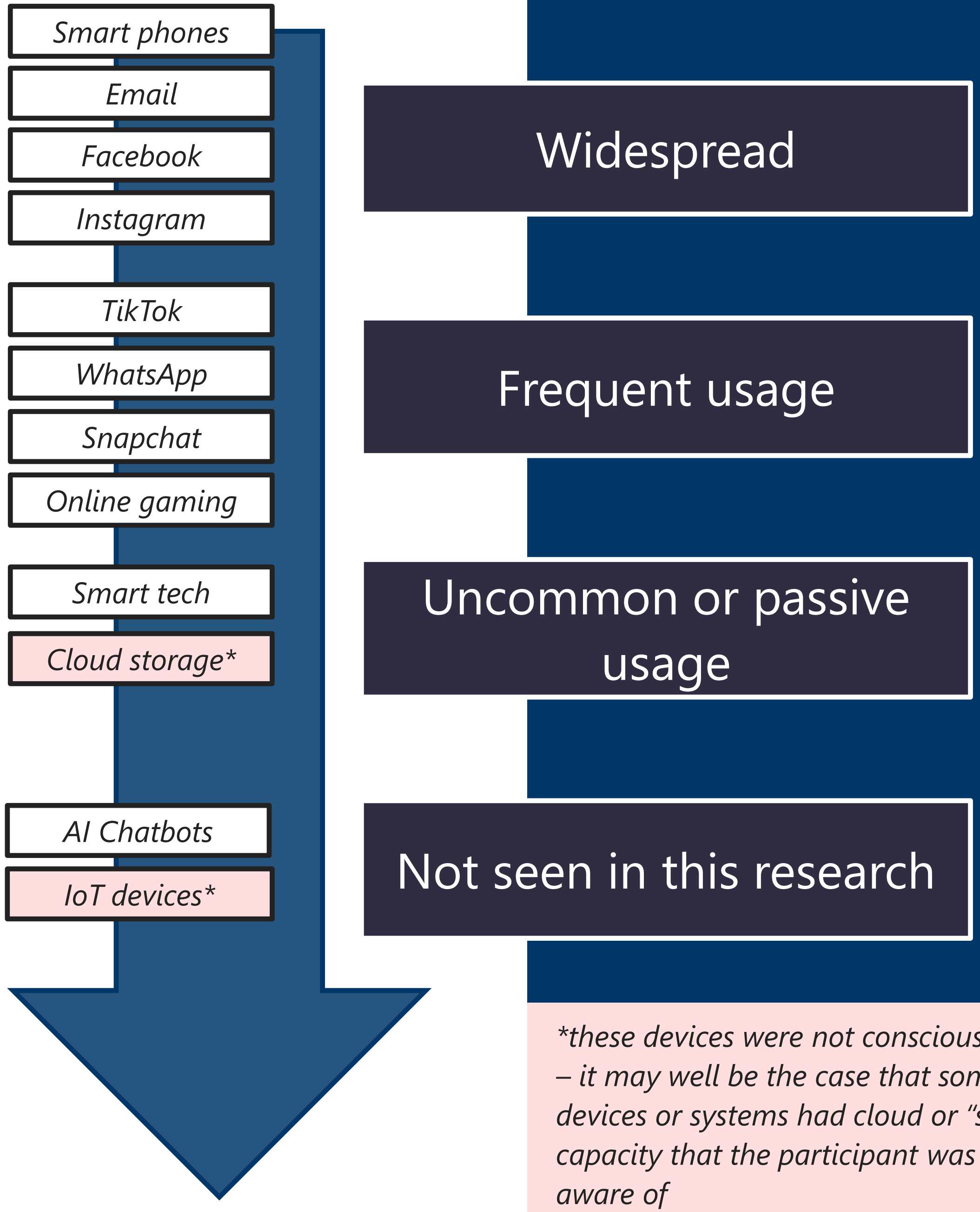
Participants in this research were primarily mainstream in their tech usage; they were not early adopters, and some were very late adopters.

New forms of data collection or usage are developing faster than the public can readily understand or adopt.

Participants did not express a particular interest in being on the cutting edge; they are mainstream adopters of tech, doing so piecemeal and sometimes reluctantly. Tech played a dominant role in their lives; it facilitated most aspects of their social, economic and family activities.

Some older participants were thoroughly pleased with the role technology played in their lives, enabling them to do things that would have been unthinkable in their earlier years. They are **proud** of their adoption of technology, although they relied on family or friends to get them set up. This, in turn, meant that they were not completely clear on what data they were sharing, or when or how to change their privacy settings.

> “As soon as I walk through the door my phone links to my iPad, and the pictures I took will go inside. **I don't have to do anything**… I can be completely lazy!
>
> - Paul, 67, Bristol



*these devices were not consciously used – it may well be the case that some devices or systems had cloud or “smart” capacity that the participant was not aware of

While ChatGPT made mainstream news headlines in March 2023, few if any participants were aware of it, or of generative AI more broadly

What we did:

Participants were shown two hypothetical situations in which…

1. *You use the tool to research house prices. The generative AI learns about how you and others feel about the issue of housing as a result of your data. A political party uses this information to run a campaign on help-to-buy schemes, which is a big success.*

2. *A UK charity that helps people with a rare disease has developed their own version of this AI tool. There are only 100 sufferers of this disease in the UK, and they have been using this AI tool to seek help. The AI chat tool uses their prompts to provide a better service to users, as well as provide anonymised data to academic institutions.*

It should be noted that this research was not aiming to test knowledge or interest in AI per se, but rather to establish general principles and cautions on which future innovations can be based.

The overriding response to both scenarios was confusion: generative AI has not made it into the mainstream of public thinking and the threats and opportunities behind this innovation felt difficult to grasp

> "I think people wouldn't have a problem with [generative AI], with certain conditions. Is it governed properly? Is it anonymous? Is it being used to make a profit?"
>
> -Sheila, 51, West Lothians

The public's responses to these hypothetical scenarios revealed some underlying assumptions about the right way to treat customer data

Good faith

The public wants to see organisations operating according to common sense principles. The challenge for generative AI and other innovations is that moral precedents and axioms have not yet been established. There is no hard and fast rule for how AI "ought" to behave.

Public good

Participants responded more positively to the example involving a charity. People were more willing to accept novel forms of data collection for the public good than for a profit motive. These needn't be mutually exclusive, but people find it hard to trust a new form of data sharing that feels exclusively for someone else's benefit.

Clarity of purpose

What is the goal of the data collection exercise? For the public, this is a deeper question than simply "legitimate interest". What is the interest, and what makes it legitimate?

Reflecting on generative AI revealed how the public expect organisations and companies to explain their "end game" for the data being shared.

> "I wouldn't be happy with it because it's not for good intentions. I would support anything if it's for a good intention, otherwise it's just a business ploy."
>
> -Raleigh. 34, Birmingham

Paul is a 42-year-old man living in Belfast. He has just moved into his first home and, due to his job, is very aware of data protection legislation. He holds technology to a high moral standard and worries that Twitter is being "handed over to AI" to the point where it won't be able to effectively censor homophobia, racism or sectarianism. When it came to ChatGPT, he worried that the profit motive underlying some of its most recent applications made it difficult to trust. He does *not* feel this concern as sharply for more established forms of data collection: he is comfortable with the trade-offs he makes with retailers, for instance. When faced with an unfamiliar data collection method, Paul defaults to first principles: it should be for the public good, and it should be transparent.

Responses to seeing the ICO website were positive, although questions around how to exercise their rights remained

Data rights with strings attached

The public assume that the exercise of data rights feels like it would be a battle. There is a strong belief that that in order to successfully exercise their rights, they would need to win an argument, or to *convince* the company that they must delete or rectify their data. People expected to need to hire a lawyer, or up-skill themselves to successfully argue a case against a data processor.

Good to know

That said, people liked the fact that they could put a face to a name; they knew something like the ICO must exist and were reassured to see that it was an organisation with enforcement powers. The overwhelming sentiment was that more people should know about the ICO. Even if they don't understand what these harms are.

There is an implicit belief that someone is out there looking out for them and it's important for the ICO to continue fulfilling this role. The challenge for the ICO is to foresee harm, and to understand what the public *would think* about a particular data protection concept if they had the time and space to think about it properly. The public expect the ICO to be forward-thinking and to do their horizon-scanning for them.

> "You'd think, with the organisations, they have to go through protocol. In my head, they have to go through a certain kind of protocol."
>
> -Sheila, 51, West Lothians

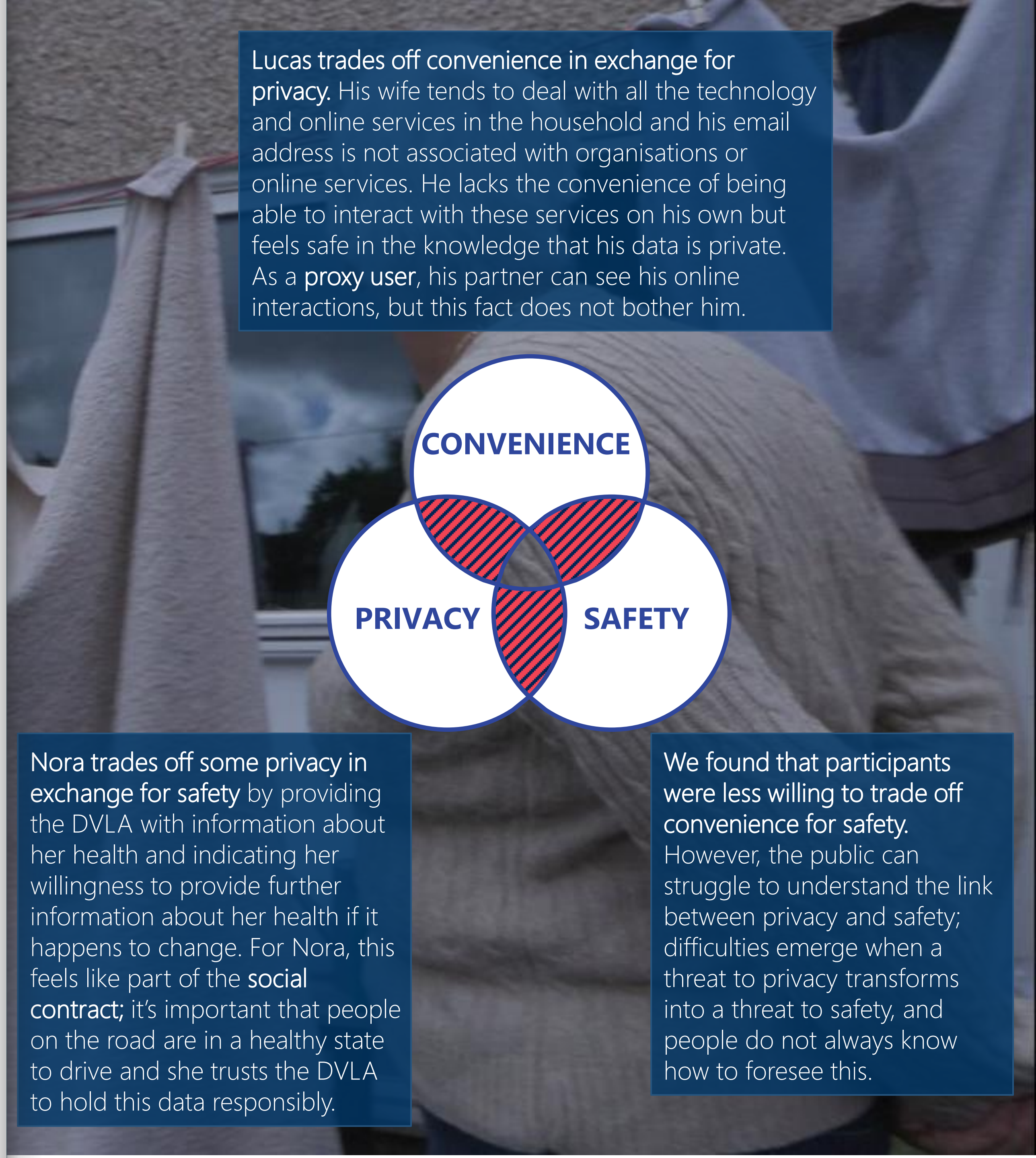
In an uncertain future, people assume that there is a regulator out there protecting them from the worst forms of data harm

Participants struggled to evaluate trade-offs in data protection

What we did:

Participants were shown a range of trade-offs to help establish general principles for future data protection requirements

1. *A public body gathers more data around earnings and energy so they can provide targeted benefits to those particularly in need of them*
2. *An app you have downloaded is tracking your profile information (photos and videos), location, browser, search history and biometric information. You may upgrade to a premium version that won't collect this information, which is £9.99 per month*
3. *An employer is monitoring employees' posts on their shared online workspace to better understand employee motivation and wellbeing*
4. *A healthcare provider combines data from personal smart devices with health information held by GPs and the NHS so they can make personalised health recommendations. The data is used by default unless you opt out.*



Lucas trades off convenience in exchange for privacy. His wife tends to deal with all the technology and online services in the household and his email address is not associated with organisations or online services. He lacks the convenience of being able to interact with these services on his own but feels safe in the knowledge that his data is private. As a **proxy user**, his partner can see his online interactions, but this fact does not bother him.

Nora trades off some privacy in exchange for safety by providing the DVLA with information about her health and indicating her willingness to provide further information about her health if it happens to change. For Nora, this feels like part of the **social contract;** it's important that people on the road are in a healthy state to drive and she trusts the DVLA to hold this data responsibly.

We found that participants were less willing to trade off convenience for safety. However, the public can struggle to understand the link between privacy and safety; difficulties emerge when a threat to privacy transforms into a threat to safety, and people do not always know how to foresee this.

Participants were worried by the prospect of having to make trade-offs around personal data

Paying for privacy

Being asked to pay *not* to have their data collected felt sinister for our participants. While they were conscious that their data likely held monetary value for organisations, this trade-off implied to people that the service could function perfectly well without their data, and if that were the case, they shouldn't be asking for it in the first place. The trade-off lacked transparency, suggesting to people that there was a hidden agenda behind the data collection that was of such (unknown) significance that they would have to pay to disable it.

Public sector data collection

Participants told us that they were more willing to see data collected for what feels like the public good. The specific data collected (earnings and energy usage) felt reasonable and proportionate to the intended aim of providing means-tested benefits to the people who needed them most. As previous research has shown, public sector organisations and those claiming to operate in the public interest tended to be trusted to act ethically. Here, we saw that public sector organisations were given the benefit of the doubt: the trade-off contained no inherent causes for concern and was therefore accepted.

Employee monitoring

A persistent theme in this research was the idea of data being "used against" the user. The employment relationship is recognised as a power dynamic and the risk of data being weaponised in this way felt palpable. This trade-off was complex for participants.

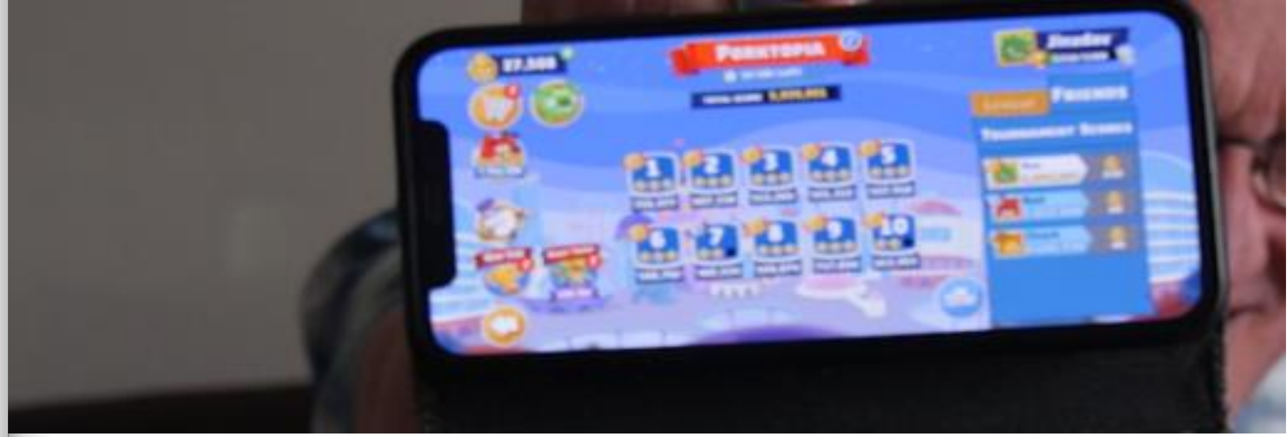
On the one hand, workplace channels like Slack or Teams are recognised as public: it is incumbent on the user to exercise care and discretion in what they say and what they share. On the other, the data processing methods in this trade-off were unknown: there was the possibility of an employee being punished as a result of data aggregation or analysis beyond their understanding. The concern here was that they would be held accountable for data that no longer felt like a true reflection of themselves.

GPs and smart devices

The concept of having to opt out of data collection did not appear as a significant frustration in the context of this trade-off.

In speaking to the public, there was a strong sense that "opt-in" consent does not feel particularly active or deliberate either – there was a persistent assumption that virtually all forms of data collection are, to some degree, taken automatically and without permission. As a result, participants found it difficult to respond to this trade-off.

Wherever technology moves in the future, a more balanced relationship between data holders and organisations will be critical



Blind spots persist between organisations and their users; ICO can facilitate a better relationship between them.

Data users: *The data user cannot always predict the consequences of their data sharing. They may not always trust the organisation but proceed with consent regardless.*

Organisations: *Organisations cannot always predict data harms on the user's behalf. They must sometimes assume that consent is made in possession of the facts.*

Blind spots:

- **What is the worst that could happen** if I click "accept"?
- Does the organisation's approach to data reflect their stated **values?**
- What will this data sharing mean for my family or **loved ones?**
- Will I **regret** consenting in the future, and what can I do about it?

Blind spots:

- What are the data user's **underlying goals** for data privacy?
- Did the user **think carefully** before clicking "accept"? Are they able to do so?
- What are the user's **"red lines"?** What outcomes do they want to avoid?
- Who else is using the service? Is there a **proxy user** behind the account?

Conclusions

When it comes to data, the public is behaving rationally given the contexts in which they live

The limits of "behaviour change"

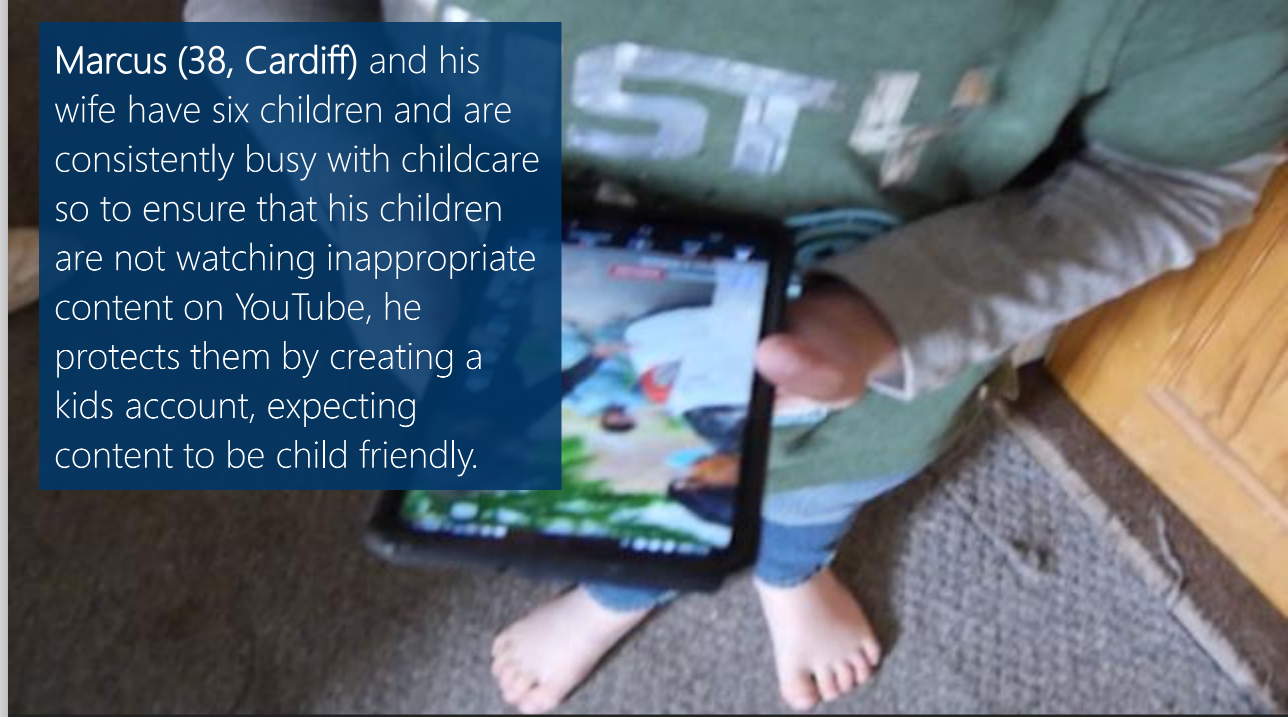
Having spoken to a diverse cross-section of the UK public, it is difficult to conclude that any one of them is behaving "irrationally" towards their data. When viewed in context, their actions, preferences and beliefs make sense. We observed that people do worry about the salient harms that could happen from sharing personal information, and they act in ways, when they can, that they sincerely believe are protecting them.

Keeping data private looks different for each person. We observed people relying on their inner circle to handle technology usage. By trusting others, they feel more protected. We may question what would happen if that trust were broken, but for these participants at this moment in time, the system worked well.

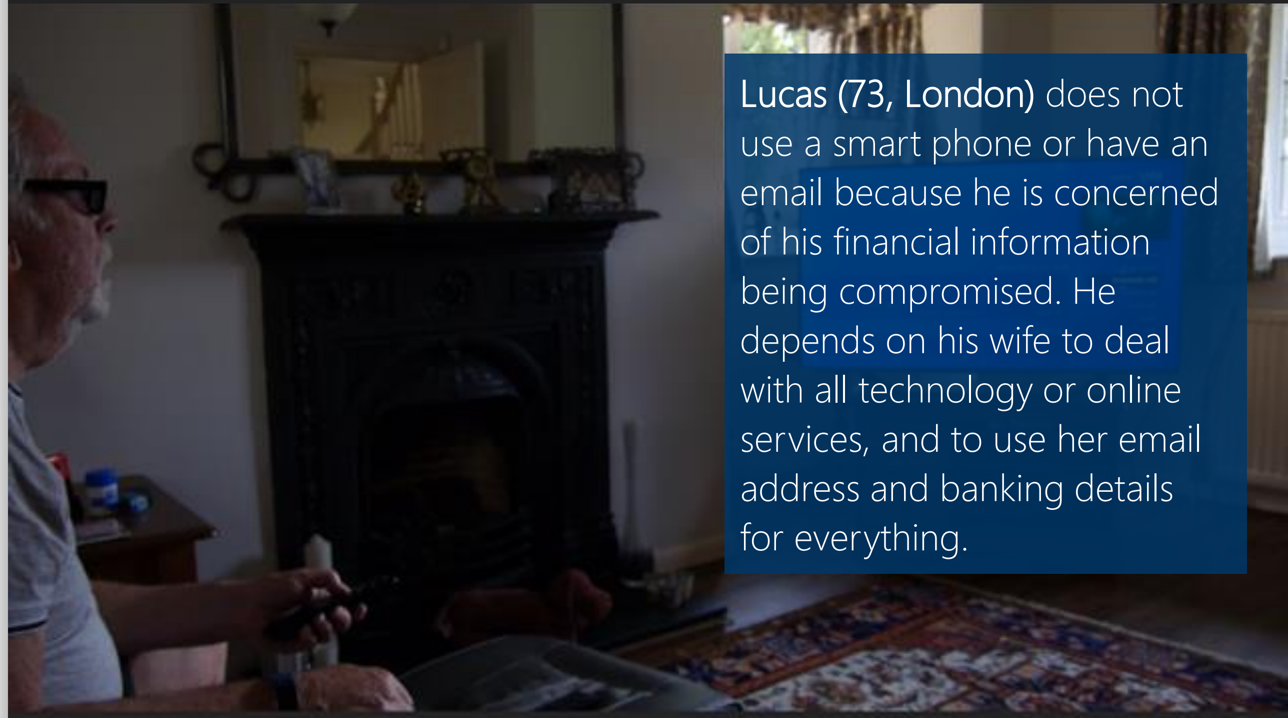
A repeated theme for some was the idea that people had "nothing to hide". This belief is valid; they may see value in being an "open book".

Participants built their own workarounds to achieve their data goals. People may generate fake emails with pseudonyms to use for online subscriptions such as Netflix or Amazon. While a person might balk at sharing their name, that same person may be comfortable sharing their payment details. To the data user, these apparent contradictions are valued parts of their data lives, and they hope to engage with organisations with these behaviours intact.

Future research is needed to understand how to make this happen: How can organisations work with, not against, the public's data behaviour, and how can it be demonstrated that it is in their interest to do so?



Marcus (38, Cardiff) and his wife have six children and are consistently busy with childcare so to ensure that his children are not watching inappropriate content on YouTube, he protects them by creating a kids account, expecting content to be child friendly.



Lucas (73, London) does not use a smart phone or have an email because he is concerned of his financial information being compromised. He depends on his wife to deal with all technology or online services, and to use her email address and banking details for everything.

Conclusions

Understanding the data user

Data users behave rationally within their contexts. We observed people living with real, overlapping stresses and challenges, and while data privacy is sometimes deprioritised, it is not devalued.

We saw that data privacy matters, both in the online and physical worlds. Physical privacy tended to take up the public's attention: it is more readily apparent, and threats to physical privacy have remained static in comparison to the pace of technological change.

Our participants were not cutting-edge users of tech: no sooner had they come to terms with one data innovation than another came along.

Personal rights, data rights, and privacy

Data rights can feel conditional. We saw a lapse in trust between data users and data processors, and greater transparency through DPIAs, privacy notices or consent requests does not always impart greater trust. There is a pessimism challenge here: if the public do not believe their rights are absolute or enforceable, they will not be asserted. And, if they are not asserted, the data user may struggle to come to a full understanding of what their rights are.

For our participants, trust does not come from the fine print, but from an overarching and implicit belief that an organisation will act reasonably with data, even when it does not have to, and even when it has not explicitly said that it will.

Understanding the future

When confronted with hypothetical situations about the future of privacy, people can struggle to make sense of the threats, opportunities or obligations at play. Generative AI and its potential benefits or harms are elusive, and it is hard enough to understand the data privacy implications of social media in the present. Faced with this difficulty, the public default to first principles.

We rely on the social contract, and "common sense", to deal with uncertainty and ambiguity in how we relate to individuals and organisations alike. In evaluating what the future of data could look like, our participants defaulted to ideas of public good, clarity of purpose, and good faith. In our participants' view, an innovation in data should, in the broadest possible sense, do no harm.