ico.
Information Commissioner's Office

ICO Data Lives Year 2 Ethnographic Research Final Report December 2024

Contents

Executive Summary: Background

The objective

Data Lives provides the ICO with a foundational, empathy-led picture of what the UK public are thinking, feeling and doing regarding their personal information.

Year 2 is the research programme's first opportunity to understand if and how social norms have **changed** around data. This research addresses the ICO's purpose: to empower the public through data, recognising that this was not consciously on participants' radars last year. The research also considers the barriers to engaging meaningfully with personal data, adding behavioural analysis to last year's interpretation. Finally, the research is intended to offer an up- to-date understanding of how the public are perceiving and using the cutting-edge of technology, such as large language models.

The method

Eight ethnographies and eighteen interviews.

- **Ethnography** is the study of people and cultures in their natural settings. Researchers spent 5-7 hours with each participant, and their social networks, to understand what people **see** in their culture, **say** about their beliefs, and **do** in their behaviours.

- **In-depth** interviews provided **breadth** to the research, to complement the depth offered by the ethnography. The shorter timeframe allowed for a greater number of interviews to be conducted, and for **hypotheses** to develop around how different demographic characteristics influence beliefs and behaviours around data. It should be noted that neither ethnography nor in-depth interviews are statistically representative.

Executive Summary: Key Insights

1. Data protection is a form of labour

This research saw people dedicating time, effort and skill towards looking after their information, but there are few opportunities for the public to **learn how to do it well.**

2. The public are DPOs of their own households

However, the public are not always aware of the responsibility they have for other people's information, or the **value and importance** of their work.

3. "Data empowerment" is a poorly understood term

People interpret data empowerment through the lens of **consumer rights**, which are seen as more tangible and comprehensible than data.

4. New technology stresses the social contract

The public establish "right and wrong" in data sharing through **social norms**, but new technology can leave users unsure about appropriate or inappropriate use.

5. Data sharing technologies are easily misinterpreted

Users draw inferences from the format, branding and "tone" of data sharing technologies to understand what data is being shared. **These inferences are not always accurate.**

6. Special category information is poorly-differentiated

There is little evidence in this research that users treat special category information differently to other data, unless the user already fears that they will be **discriminated against** based on it.

7. The cost of living can make data sharing feel compulsory

The requirement to transact data to secure healthcare, housing or other necessities can leave vulnerable people feeling as though they are sharing data **under duress**.

8. The public expect to know the motive for data collection

A distinction emerged this year between the "purpose" of data collection and the **underlying motive**. The public are considerably more interested in the latter.

9. Pay-for-privacy risks fostering ill-will and mistrust

The public felt **unable to evaluate the value-for-money** of this concept because they did not feel they knew enough about how organisations are currently using their data.

10. Data can be shared playfully, and carelessly

This research saw data being shared in gamified environments, leading people to **deprioritise their privacy** in pursuit of escapism and play.

Content warning

This report describes what day-to-day life looks like for a cross-section of the UK public, and some of these case studies involve situations that are upsetting, concerning and unexpected.

Ethnographic research involves spending a great deal of time with participants, being led by them and following their agenda for the day. Where people chose to be open with us about difficult times in their lives, we have chosen to share these stories with the participant's **explicit permission**. Where doing so could place a respondent at risk, they have been **anonymised**.

We have shared these stories because we feel that they reveal something important about the UK public and about data sharing at large – our aim is not to share these gratuitously, or to cause distress for its own sake. Readers can avoid encountering these stories by following the content guidance on the opposite page. The **executive summaries** and conclusions do not discuss these topics.

We take this opportunity to thank all participants for their openness and insight throughout the research.

This research includes discussion of the following topics, on
the following pages:

- **Bereavement** – Page 30
- **Blackmail** – Pages 10, 23, 50
- **Discrimination and racism** – Pages 19, 26, 29, 47, 50
- Physical **assault and theft** – Pages 10 and 17

Our Sample

The pie charts represent the sample of 29 people who took part in Data Lives Year 2.

Pie Chart 1 : Gender Distribution

- Male: 18 participants
- Female: 10 participants
- Prefer not to say: 1 participant

Pie Chart 2: Age

- 18-34 years: 14 participants
- 35-54 years: 11 participants
- 55-65 years: 3 participants
- 66+ years: 1 participant

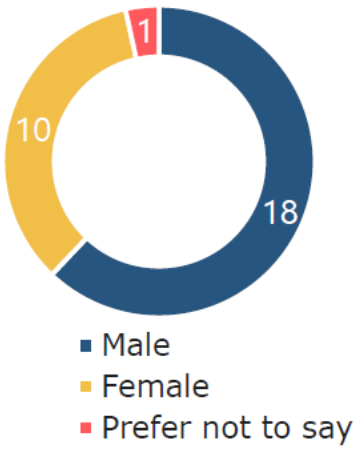
Pie Chart 3: Socioeconomic Status

- AB: 3 participants
- C1C2: 16 participants
- DE: 7 participants
- Students: 3 participants

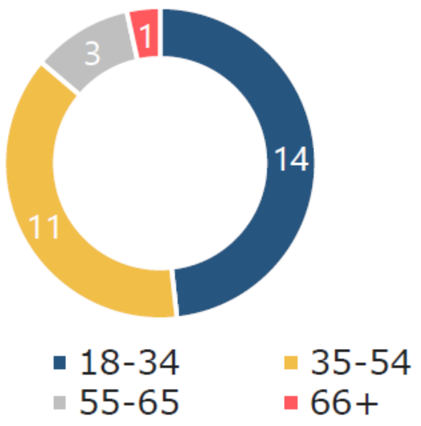
Pie Chart 4: Ethnicity

- White British: 20 participants
- Black British 5 participants
- Mixed Ethnicity: 2 participants
- Bangladeshi: 1 participant
- White Irish: 1 participant

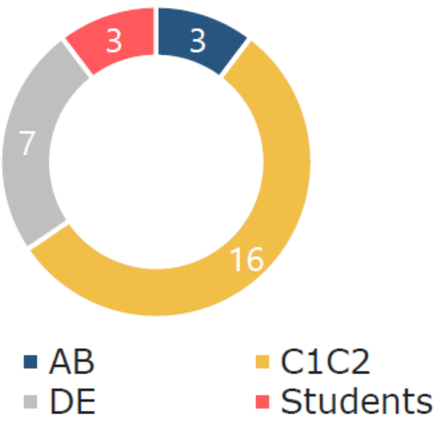
Gender



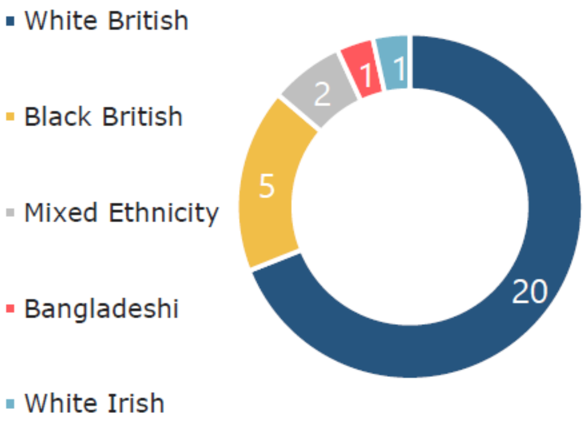
Age



Socioeconomic Status



Ethnicity



The sampling approach

26 Research sessions with households or peer groups

29 Core Participants

50 People met during the research

In recruiting participants for this study, researchers aimed to **recontact** participants from Year 1 and invite them to take part again.
This objective was balanced against the need to recruit younger participants from **higher socioeconomic contexts**, given that last year's research skewed towards older and less well-off participants.
Ultimately, **13 participants** from Year 1 chose to participate again. This provided an invaluable opportunity to see how their beliefs, behaviours and contexts have changed.

Two foundational notes on the UK public

People focus on their relationships with each other, rather than their relationships to organisations.

This research is **longitudinal**, aiming to capture change in how participants behave and think about their personal data. This year, researchers observed a stronger focus on keeping data safe from neighbours, employers and other people in their immediate social and economic lives. Cost of living pressures were perceived to have worsened since 2023, leading participants to feel less autonomy over when and if to share their data. However, attitudes towards organisations at large, for instance social media companies, banks or retailers, remain **static**, even among those spoken to in Year 1.

While the public do not always think about their "data", they do think about their secrets.

This year, researchers noticed a striking change in attitude when participants talked about their "secrets." This word was used unprompted and seemed to attract more emotive discussion than simply talking about "data." However, people do not always realise that their personal data can link back to or compromise things they hold as secret. Secrets are **treasured, intimate or sensitive information** about a person, and participants felt at their most empowered, or their most vulnerable, when secrets, not data, were at stake. When this report references secrets, it is referring to information that participants desperately want to protect or share on their own terms.

What is a secret?

"Treasured, sensitive information about a person. Secrets are more private, more emotive, and more commonly thought about than "personal information".

When the public want to share their secrets, they want to do so actively and purposefully. However, data sharing feels passive and automatic, and people worry about whether their secrets are at risk in the process.

Chapter 1
Social Norms and the Social Contract

Introduction

Year 1 of Data Lives emphasised that the UK public expect organisations that collect data to operate under a **moral and ethical framework**, not just a legal one.

This chapter aims to articulate what those moral and ethical frameworks are: what contracts or pacts the UK public implicitly make with each other, and what **unwritten rules** they expect organisations to abide by.

This chapter argues that to understand how the UK public want organisations to behave, we simply need to observe and understand how the UK public behaves with each other. Standards of "good behaviour", "fairness" and "transparency" are drawn from the culture and applied to organisation: from the ground up, not the top down.

We call these standards the **social contract**, and this research saw it play out in families, flat-shares, coffee shops, supermarkets and the workplace.

This chapter will make these unwritten rules explicit, offering a social and cultural perspective from which to understand the UK public's data needs under the GDPR.

Social Norms and the Social Contract

Key Insights

1. The public draw their expectations for data sharing from the implicit, unwritten codes of behaviour that govern day-to-day life, which we call the **social contract.**

2. The public continue to centre their lives on **physical, local communities**. Data protection is as much about the local cul-de-sac as the wider online world.

3. **Peer-to-peer data harms** emerged this year. Whether through outright crime or misunderstandings about smart doorbells, the public can cause harm to one another.

4. "**Domestic DPOs**" have emerged as data sharing technology proliferates – people who knowingly or unknowingly, and for better or worse, are responsible for other people's data.

As with Year 1, the public's privacy interests sit primarily at the local level

Local versus Global

Year 1 drew a distinction between tangible, local privacy and more abstract, online privacy. This year, the distinction has become even sharper.

Participants expressed a greater sense of tension, worry and unrest this year: several returning participants were facing redundancy and job hunting loomed larger on people's agendas.

Whether centred on housing costs, job instability, crime, or racial and social prejudice, our sample's focus is even more centred on tangible risks and harms, rather than the abstract and global harms presented by online data sharing.

Concerningly, one participant has been repeatedly physically assaulted on the doorstep for the way they look. This bullying has led them to fear for their physical safety more than their digital privacy. Another participant was recently subjected to **blackmail**. For these people, and many like them, privacy is not an abstract or intellectual concept: it is an **urgent safety risk** grounded in physical space and the real world.

"I've been threatened on several occasions and of course, being assaulted on your own doorstep you can't retaliate because they know where you live!" Anonymous.

James and his flatmates had their bikes stolen from the front hallway, and most of their collective effort as a household has understandably gone towards keeping their possessions, not their data, safe.

Weaponised data

In this local context, the greatest perceived data threat can be having one's information "used against them."

For some participants, this fear was the guiding principle that informed almost all their data behaviours, whether in the physical world or the online one.

For Philip, hearing that his grandfather had his mailbox broken into led him to worry about how the information could be misused.

This is an adversarial relationship. Users described an enemy, usually a criminal, who could weaponise their data and use it against them, even if they don’t know how.

Since Year 1, there is more concern for privacy breaches caused by other people

Concerned Neighbours

Participants continue to bristle at the idea of being monitored or "**spied on**" by their neighbours.

One participant's landlord regularly conducts work on their terrace without consulting them first, using a ladder to help workpeople onto their balcony at short or no notice.

Another participant reads their neighbour's mail out loud to them because they cannot read or write and has had to make complex judgments about what personal information to disclose or not disclose to their neighbour's loved ones.

Since last year's research, these **peer-to-peer** data harms have become more important, more complex, and more urgent: the UK public's data lives are about more than just the relationship they have with data processing organisations.

"People come down at like three in the morning and break into cars. You'll get a lot of people in the [neighbourhood] group chat sharing footage of them to be reported to the police." **(Carson, Cardiff)**

"I'm quite out there with people socially. Perhaps I don't disclose everything – we all have a little control. You might be chatting away at some point and think 'right I'm saying too much to you now!" Anonymous

In response to these local threats, the public act as DPOs in their own right

Domestic DPOs

Last year, this research identified '**proxy users'** of technology: people who access data services through the assistance of another. This is a subset, though an important one, of a much broader phenomenon seen in this year's research.

This year, participants showed us that in fact, **most people are responsible for other people's data in some form**.

As technology plays a greater role in the UK public's lives, the amount of data being entrusted to flatmates, parents, children, colleagues, friends and even strangers is increasing.

This report refers to such people as "Domestic DPOs" – these may be parents in charge of the (largely invisible) labour of managing the household's data, or a head tenant in a house-share. They may not be aware of their role, but their potential to empower or disempower people is significant.

The role of Domestic DPO appears to be gendered. Women did the majority of "data work" in our sample: storing and organising passwords, supervising children's online activity, educating the family about online privacy, and the emotional labour of worrying about all the above.

One anonymous respondent monitors her little brother's internet activity to ensure that he does not access inappropriate content. She worries that he doesn't get enough discipline and uses his phone too much, viewing "weird" content that isn't healthy or suitable.

Gaby acts as the data protection officer for her household of seven. She tries to get her husband to be more cautious around accepting cookies but can't monitor the whole household all the time.

Jay (unknowingly) became a domestic data protection officer when he bought a Ring doorbell for security. He stores information on his neighbours, family and friends and has not yet reflected on what obligations or responsibilities this may place on him.

Domestic DPOs can be highly proactive when consciously aware of their role

"She's in charge"

These data monitors can become influential members of the household. **Their concerns become the household's concerns**, and their beliefs about right and wrong forms of data collection tended to permeate through the social unit.

There was a tendency to defer **uncritically** towards the higher-knowledge member of the household or peer group. Conversations that might otherwise have been communal and democratic became **received wisdom**, cloaked in technical language.

Year 1's discussion of proxy users assumed a stark binary between a caregiver and a care recipient. This year, the research has found a more subtle power dynamic between high- knowledge users and low-knowledge users.

"Lower-knowledge" users, whether vulnerable or not, risk being disempowered and **excluded** from important conversations about their data. They may not know the technical nuances at play, but still have a view on the social, personal and ethical implications of data being shared.

"If [my wife] were here, she'd give me a right old row, but she's not, so "bang, accept cookies" and get on with making tea!" **(Marcus, Cardiff)**

"I'm not the mean sister, but I am because I am the one that disciplines him. I give him screen time on his tablet, but I don't like it when he is on it for too long. I put it for like 2-3 hours a day and he decides how to use this time.

On Family Link, on my email, through my phone – I can change screen time, lock the tablet, choose what apps he goes on. I banned him from using YouTube because he used to watch these evil characters that kill each other. I just didn't think that was right and
Mum doesn't really know about this stuff." **(Anonymous)**

There is a sharp, and gendered, divide between setting up and maintaining the “data life” of a household

Setting up: Technical, masculine, visible

The technical side of household privacy management could easily be viewed by our participants as a man’s work – technical skills found in the workplace, or general “know-how” was deferred to and followed. We met participants who recommended products like VPNs, browsers or devices to the family based on perceptions of their security, but did not extend this role into the actual upkeep and maintenance of those systems.

Maintaining: Domestic, feminine, invisible

Once the equipment has been bought, or the principles have been established, there is an ongoing and largely invisible labour to keeping the household’s data life in a stable state. Someone needs to monitor the children’s web activity or remind members of the household to keep their personal details private, and this labour can often fall to women. It is rarely thought of as “privacy management”, but rather part and parcel of being a parent: it becomes a routine part of domestic work, rather than a discrete activity worth discussing communally and executing together.

Faced with these new responsibilities, the public default to the social contract

The Golden Rule

“That’s my flatmate’s room. I don’t know if he’d be happy with you going in there, so I’ll just check with him that it’s okay.” **(James, London)**

The participants in this research were, with some exceptions, adept at respecting the privacy of others. They had an inherent ability to **identify boundaries** and stay on the right side of them.

One of the core principles that people use in handling one another’s data is the golden rule: do not do anything to someone else’s data that you would not have done to yours.

However, while people may hold to a golden rule of data privacy, they may assume that just because they are an “open book”, their peers and families are as well.

The concept of privacy is not universal, which led to a difficult exchange between one participant and her grandson, when she discovered that he had used her credit card information to buy online video game currency. The anger was genuine – not because of the money, but the **breach of trust** and the apparent mismatch of values that had just been laid bare.

“We’re five different households in this flat but obviously there are times where we need to come together as one household to get things done.” **(Riordan, London)**

The research saw the social contract play out in different settings

Family homes

Mutual supervision was a core value of the families we spoke to. There was a general acceptance of parental monitoring tools by children. Rules were set, and broadly followed, but children kept an open dialogue about what rules could be relaxed and under what circumstances. For some families, all spaces are communal: participants were not always able to point to spaces in the home that belonged to them alone.

Social media

A common theme among parents was the social etiquette of sharing photographs of their children, or other people's children, online. Again, the idea that privacy should be respected without question was common: if a parent requested that a child's face be blurred or taken off social media by another parent, this request was granted, without asking why, even if it meant not being able to share photographs of their own child. The lesson here is that the public expect to be able to keep data private, without the need to defend or explain their reasons.

Flat-shares

In flat shares with shared bills, there was an unspoken trust that the tenant in charge of paying rent or utility bills would not share their flatmates' financial information or personal details. Personal and communal space was divided up in minute detail, from individual drawers in kitchens to bedrooms themselves. Tenants were always considerate about where Ipsos researchers could or could not film, and communal obligations like chores were evenly distributed.

Neighbourhoods

Neighbourhoods in our sample could be tightly-packed and intimate. They were often altruistic, with busy group chats offering free giveaways of unneeded items.

Throughout, there was a mutual sense of discretion: an understanding that a neighbour would never call attention to something they noticed about another neighbour or reveal how much of their private lives they had seen in passing.

But that contract can be strained and tested when new technology emerges

Smart Doorbells

Since Year 1, smart video recording doorbells have entered the mainstream for the participants involved. They feel that they have become more common and widespread.

Reactions to this technology have been mixed. For some, this feels like a valuable and necessary tool to keep their homes and families safe.

But for others, this is a bridge too far. They worry about images of their children being recorded by neighbours or strangers, and those who live in close-quarters accommodation like apartment buildings or dense terraced housing worry about their private or unguarded moments being recorded, saved, and shared.

The UK’s social contract has not yet caught up with this technology. There is no etiquette or set of rules for how to manage the data stored on smart doorbells, or how to inform neighbours of its use in the first place, but this gap is causing genuine distress to a significant number of people who do not know how, or if, to object.

“Our neighbours have a Ring Doorbell. They’re lovely people, but they can see us coming in and out with the kids. It just doesn’t sit well with me.” **(Anonymous)**

This participant is considering **moving house** because of this perceived breach of their privacy, as well as a recent spate of break-ins in the neighbourhood.

There continues to be a disconnect between privacy rights under GDPR and the UK's lived experience of data

The public is beginning to sense that organisations are behaving online in ways they would not in person when it comes to personal data collection.

They recognise that it would be unsettling, and **strange**, for a neighbour or a friend to ask for data at the volume or scale that organisations frequently do online.

This is not (currently) a source of worry, but participants do feel that the purpose and manner of data collection is out of step with their own experiences of sharing and receiving data about their fellow members of the public. This continues to make it difficult to evaluate the benefits, or perils, of sharing information.

People are a great deal more discerning about sharing or withholding information with their peers, because they operate under a **mutual understanding** that organisations are not yet seen to be aligned with.

Cultural versus legal understandings of data sharing:

Data in law	Data in culture
Consent	Mutual understanding
Want-to-know basis	Need-to-know basis
Legal and illegal	Right and wrong

"I don't really trust big companies. I get these calls from Volkswagen trying to sell me stuff, and if I did that with my small business, I'd get called a ruthless [*****]!" **(Alanna, Manchester)**

"If you shop at Primark, the guy at Primark doesn't run over to Boots and say, "He's buying this!" But that's what happens online." **(Desmond, Manchester)**

Case Study Examples of Social Expectations

1 Making intentions clear

Under other circumstances, **Carson’s** landlord’s request for his financial information may have felt intrusive. However, Carson understands the need for his landlord to trust him, and **because these intentions are clear**, his sense of privacy is left intact.

“I mean it makes sense, doesn’t it - he can’t just rent to anybody.”

2 Avoiding being unsettling

James was concerned by recent news about Scarlett Johannsen’s voice being used by an LLM without her consent. It felt bizarre, and made organisations feel harder to understand, and **harder to trust**.

“…What, and they just did it anyway?!”

3 Safeguarding and protecting

In line with last year, the public tend to behave much more carefully around their children’s data than they do with their own. **Kristy** takes particular care to organise and safely store her children’s medical records in a way that doesn’t line up with her own data.

“These are the kids’ red books, which we need quite often these days.“

4 Avoiding discrimination

Sayeda will withhold her ethnicity from job applications, in case her prospective employer discriminates against her. She reflects that her ethnicity is clear to anyone who sees her but withholds it in this specific case due to the potential for **harm**.

“I’d never get a job if I put my actual ethnicity. So, I say “prefer not to say.””

5 Offering reciprocity

Walter continues to share information with the NHS about his health condition this year. Both in his data life and his daily life, he respects reciprocal and egalitarian relationships. He gives the NHS data; they give him treatment and an **insight into his condition**.

“I don’t get any money for it but what I input could save somebody’s life.”

6 Respecting the home

Kaylee’s biggest data worry is the privacy of her home – she has seen a rise in antisocial behaviour and most of her security behaviours have revolved around locks on doors. She is nervous about technology that can “see into” her home, including through in-built cameras.

“Even a picture of your face can be tracked now – that’s an issue.”

7 Taking no for an answer

Pascal has sensed a tendency for data sharing to feel compulsory. He tries to teach his daughter to resist this pressure. In line with Year 1, it can feel as though companies are **demanding data**, not asking for it.

“Whether it’s your friends or the wider web, do not feel pressured to divulge anything about you or your family.”

8 Doing no harm

Philip is job-hunting this year. While he is sanguine about automated decision-making, he is frustrated by the automated processing of his job applications. The golden rule is put into jeopardy here: his data sharing is potentially causing him to lose a job **unfairly**.

“All you’d have to do is tick the wrong box and suddenly you’ve lost the opportunity.”

9 Showing respect for privacy

Participants in this research did not always have a particular reason for withholding their information. They may not (always) fear the consequences of sharing details such their sexuality, but they found it inherently empowering to **choose** whether to disclose it.

“I used to do check-ups at a clinic. I gave a fake name, [even though] I had every confidence that they would treat it with utmost confidentiality.”

10 Avoiding being nosy

During our time with **James**, we went into his local coffee shop. He went in ahead to ask the owner if it was okay to film inside, fearing that we were being nosy. Data collection may not always be harmful, but it can be **rude**, and organisations are not exempt from this rule.

“Can they film in here? Sorry, it’s for some weird research they’re doing.”

Chapter 2
Empowerment

The UK public are skilled advocates for their own needs

Introduction

People in this research had an innate sense for when the social contract had been **breached**, and they needed to assert themselves.

Since Year 1, the research has amplified the fact that the public are **astute**: they understand that there are systems in place, bureaucracies to navigate, or workarounds to deploy, which they feel they can access if they choose to assert themselves.

These skills can be passed down from parents to children: researchers met Orla, Philip's mother, who stood up to a water company who threatened to cut off her father's supply, and who successfully lobbied her local council against a new traffic throughway being built on her street. The motivation, tools and skills required are all present and **inherent** in the public conscience, even if individual members of the public do not always test these skills regularly.

This chapter will show that the public do not need lessons in how to be empowered. It will establish that the data sharing process itself – perplexing, opaque and mysterious as it can be – can make empowerment feel **unworkable**.

An anonymous participant was blackmailed by competitors when setting up a new business. They spoke directly to one of the perpetrators and consulted the Citizens Advice Bureau about what to do next.

Sayeda conceals her ethnicity when applying for part-time student jobs to ensure that they cannot discriminate against her. She is pragmatic about this, taking the world as she sees it, rather than how she would like it to be.

Nora discovered during her daughter's ballet recital, that despite strict rules against parents filming for child protection reasons, event photos were being sold publicly. Although she had signed a consent form, Nora felt misled by the school's actions and has since become more cautious about such agreements.

Empowerment

Key Insights

1. Powerful lessons can be drawn from how the public empower themselves in contexts beyond data sharing: the **tools and motivation** are there, but not always applied to data.

2. **"Data rights" do not resonate easily with the public:** clarity is needed around what specific behaviours, outcomes and processes can fall under this label.

3. **Secrets** can be one of the more empowering aspects of a person's data life: having the ability to withhold, share and protect a secret can make people feel strong.

4. A distinction exists between **the purpose and the motive** of data collection. Making decisions based on the organisation's motive was seen as more empowering than the purpose alone.

5. The day-to-day labour of managing personal data can make empowerment feel less salient and achievable: data rights can be suppressed by **data responsibilities**.

People feel empowered through consumer rights frameworks

Getting your money’s worth

Consumer rights are more familiar to the public than data rights. There is a strong discourse around “getting your money’s worth” that people feel comfortable asserting.

One participant faced a situation where a cosmetic surgery service failed to meet the promised quality standards, leading to his request for a refund. After initially being denied, he resorted to **X** (formerly Twitter) to publicly call out the company and complain. His confidence asserting his rights ultimately led to him receiving his refund.

Consumer empowerment feels considerably more accessible to these participants. The ability to **“vote with your wallet”** feels close at hand, and the “culprit” is typically clear and easy to identify.

However, when it comes to data rights, this feeling of empowerment seems to fade; there was a sense from the public that data rights are not as clear.

The abstract nature of data, along with the intricacy of how data is collected, stored and used, adds another layer of complexity. This makes it more challenging for individuals to grasp how to assert their data rights effectively.

“If a company does me wrong, I know they don’t care about me; but they care about their reputations and I’m going to make sure people know about it.” **(Jay, London)**

“I don't think I've ever been in a scenario where I've had to assert my [data] rights. I don't know what rights I have, or what evidence I need to have that something's been jeopardised. People are only interested when they're in a negative situation, and then is it too little too late?“ **(Caroline, Manchester)**

By contrast, people struggled to identify what data rights mean in practice

“Too little, too late”

Participants were asked to consider what “being empowered through data” might mean to them. Responses were mixed and nonspecific. On first read, people tended to think of data rights as **transactional or adversarial**: monetising their data, or “getting away with” using a service without transacting data or paying an additional fee.

However, participants tended not to have a concrete view of what ”monetising” data could look like. Some suggested, with a hint of irony, that it could involve getting a ‘cut’ of the value that their data is providing companies.

When thinking more broadly, data rights tended to become subsumed under other, more familiar rights: non- discrimination, equity and equality.

The public interprets data rights in terms of…

Personal Rights	**Communal Rights**
Monetising personal data	Non-discrimination and fairness
Access to health data, preventative health	Rights for people with disabilities
Avoiding advertising altogether	

Lyn is a homemaker and caregiver to her 11-year-old granddaughter, as well as a recent adopter of a Ring doorbell. Lyn did not know what “data rights” could mean for her, but she has a clear sense of what “consumer rights” means. When Lyn tried to cancel a charity direct debit, she felt that the fund-raising caller tried to make her feel guilty, which intuitively made her feel that her consumer rights were being undermined.

This was a common theme among participants: people have a strong sense of when they are being **wronged**, but not with regards to data.

Data empowerment is made difficult when technology changes

Moving targets

The public are well-equipped to assert their rights when the context is familiar and the threat to their rights is clear.

However, participants in this research tended to view data protection as a moving target. No sooner had they understood the data implications of social media on their children or their own lives than LLMs emerged and caused them to reevaluate.

In both waves of the study, researchers asked participants to "map" their data, describing where it sits and where connections are made. As in Year 1, there was very little clarity or detail in these responses.

People relied on common sense to safeguard their information, but technological change risks stressing their capacity to rely on intuition alone.

As with last year, data protection behaviours centred on avoiding fraud, hacking or other crime. The cognitive load underpinning this effort was considerable, sometimes leading to **behavioural fatigue**: with so much focus on data responsibilities (to family, to peers, to employees), data rights can easily be sidelined.

"I've had to add this new app for parking. Which then asks you to add your bank details on your phone, which I'd avoided up until the other week. I couldn't pay any other way." **(Robin, Birmingham)**

Data Rights and Data Responsibilities

Households in this research had a strong focus on data responsibilities: the daily labour of keeping data safe. But data rights risk being sidelined and deemphasised.

Data Responsibilities
Laborious: a chore, but a known quantity

- Strong passwords
- Two-factor authentication
- Multiple email accounts
- Supervising children

Data Rights

Unknown: complex, inaccessible

- Writing complaints to companies?
- Litigating?
- Making FOI requests?
- Getting paid for my data?

"Writing an email to a company [about data] isn't exactly straightforward when you aren't sure what you're asking for." **(Sheila, West Lothians)**

Having secrets can be the most empowering, and high-stakes, aspect of the public's data life

The worst that could happen

Participants tended not to react with much emotion when asked about their "data". However, whenever "secrets" were mentioned, people spoke with more **urgency**, more emotion and more interest.

In some cases, the value of a secret is **pragmatic**: a secret can be damaging or humiliating; it can be a sign of trust when shared, or a sign of betrayal if given out without permission. But importantly, people valued secrets for the quiet satisfaction of knowing something that other people aren't allowed to know, whether about someone else, or about themselves.

Having secrets meant having autonomy, choice, even **mastery** over their information: holding it like a treasure and keeping it safe. This is potentially fertile ground for engaging the public in data empowerment: to think of their personal data like a secret and to exercise power over when, if and how to share it.

However, the public can struggle to identify when their secrets are at risk: it rarely occurred to participants that sharing the wrong combination of data could inadvertently lead to a secret being revealed. This links to last year's distinction between abstract and tangible data harms – while organisations can be clear about what data is being asked for, the **latent impact on a user's secrets is left up to the imagination.**

"As humans, we have secrets. We sometimes even need to tell lies to get through things. The fact is, we are becoming so inhumane and unnatural that your whole life and personality can be summarised and get in the way of things like a mortgage or something. That's messed up. We're not perfect people." **(Riordan, London)**

People are rarely reassured by learning the “purpose” of data collection: they want to know the motive

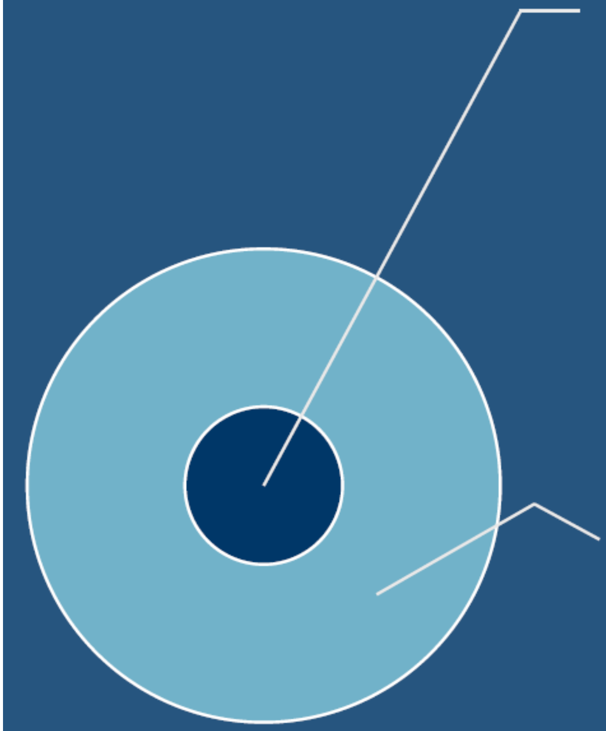
The public often feels like organisations are asking questions that could feel like “want-to-know” rather than “need-to-know.” This makes it difficult for the public to feel empowered as they do not understand the motive behind data collection.

Data users are often presented with lengthy, complicated T&C agreements – these important documents explaining how an organisation will collect, use and share user data are seen to be very difficult to understand. This perceived bureaucratic approach leaves users feeling disempowered and lacking true choice or control.

When individuals share their data with organisations, they may not fully understand how that data will be used, who will have access to it, or what the long-term implications of sharing might be. The lines between consensual data sharing and invasive data collection can become blurred, leaving the public feeling disempowered and uncertain about the fate of their personal information.

“They’ll say it’s for research purposes or whatever and then…” **(Alex, Riordan's housemate)**

“…and then they use it to make millions of quid! And you’ll say ‘allow essential only’ but you have no idea what those essentials are.” **(Riordan, London)**



The Motive:

Implicit, outcome-driven

- Sending marketing emails?
- Discrimination?
- Algorithmic targeting?
- Training an AI?
- Dynamic price changes?
- Fraud?
- **Are my secrets at risk?**

The Purpose:

Explicit, process-driven

- Research
- Marketing
- Legal obligation
- Legitimate interests
- Contract
- Consent

Sometimes empowerment means sharing the minimum amount of data possible to achieve a human need

An anonymous case study

One of the couples in this research is supporting their five-year-old son with the sudden loss of his baby brother.

The bereavement has rocked this family: it has led to some behavioural challenges for their son, who occasionally acts out at school or has sudden outpourings of grief. They are in the process of learning how and when to share their story.

Their son is often surprisingly upfront about their loss, sometimes telling strangers, or restaurant staff. His parents try to be more discreet, but when they need to access mental health services, bereavement leave from work, or general understanding and compassion from other people, they try to share the basic facts, without going into the details.

These participants show us that "data vulnerability" is often a by-product of much deeper, more painful vulnerabilities. Whether a bereavement, unemployment or illness, **when we need more from other people, we share more with them**, whether we are comfortable doing so or not.

"We never told his Taekwondo instructor, and we didn't want to bring it up but then one day he was just in floods of tears, and we had to tell him." **(Anonymous)**

Chapter 3
Data and Emotion

Introduction

"Behaviour change"

As in Year 1, it remains difficult to conclude that any member of the public is behaving "irrationally" around their data when viewed in context.

The purpose of this chapter is not to create a playbook for behaviour change, or "educating" the public, but rather to describe the emotional, psychological and contextual forces that influence their behaviours.

People were observed to operate based on misconceptions or **heuristics** about how data sharing works. This chapter will articulate those misconceptions, not to call on the public to change their behaviour or "correct" their assumptions, but to flag the pitfalls and challenges that they may face as they navigate the data sharing landscape, and to offer organisations and the ICO alike the opportunity to **help**.

Participants' beliefs and actions are analysed throughout the chapter through the **MAPPS** framework, a behavioural science tool used by Ipsos for understanding and explaining people's actions.

"It's different. I'm not worried doing this research because this is a conversation: I'm choosing to disclose things. It's not like on your phone where… well I suppose it's like that on your phone too, but it doesn't feel like it." **(James, London)**

What influences a person's behaviour around their personal data?

Motivation: What do I want to do?

Ability: What am I able to do?

Perception: How do I think about my choices?

Physical: What resources do I have access to?

Social: What are the people around me doing?

MAPPS Framework, Ipsos

Data and Emotion

Key Insights

1. Since last year, researchers sensed more **tension** and concern among participants. Cost-of-living pressures can make data sharing feel more necessary than optional, but also fuels a desire to share data for enjoyment and escapism.

2. A person's willingness to share data is mediated by their emotions, **social context**, and even the user interface and tone-of-voice of the data sharing service.

3. Data sharing can become **normalised** and expected within peer groups. These pressures can make it difficult to simply "opt out" of sharing information.

4. As with Year 1, the perceived **permanence** of data sharing does not always align well with the changeable nature of people's emotions and contexts.

5. Playful data sharing is given less careful consideration than more "serious" applications. The tone of voice or general feel of a data service influences willingness to share data.

Economic pressures can heavily restrict a user's ability to assert their data rights

Opportunity cost

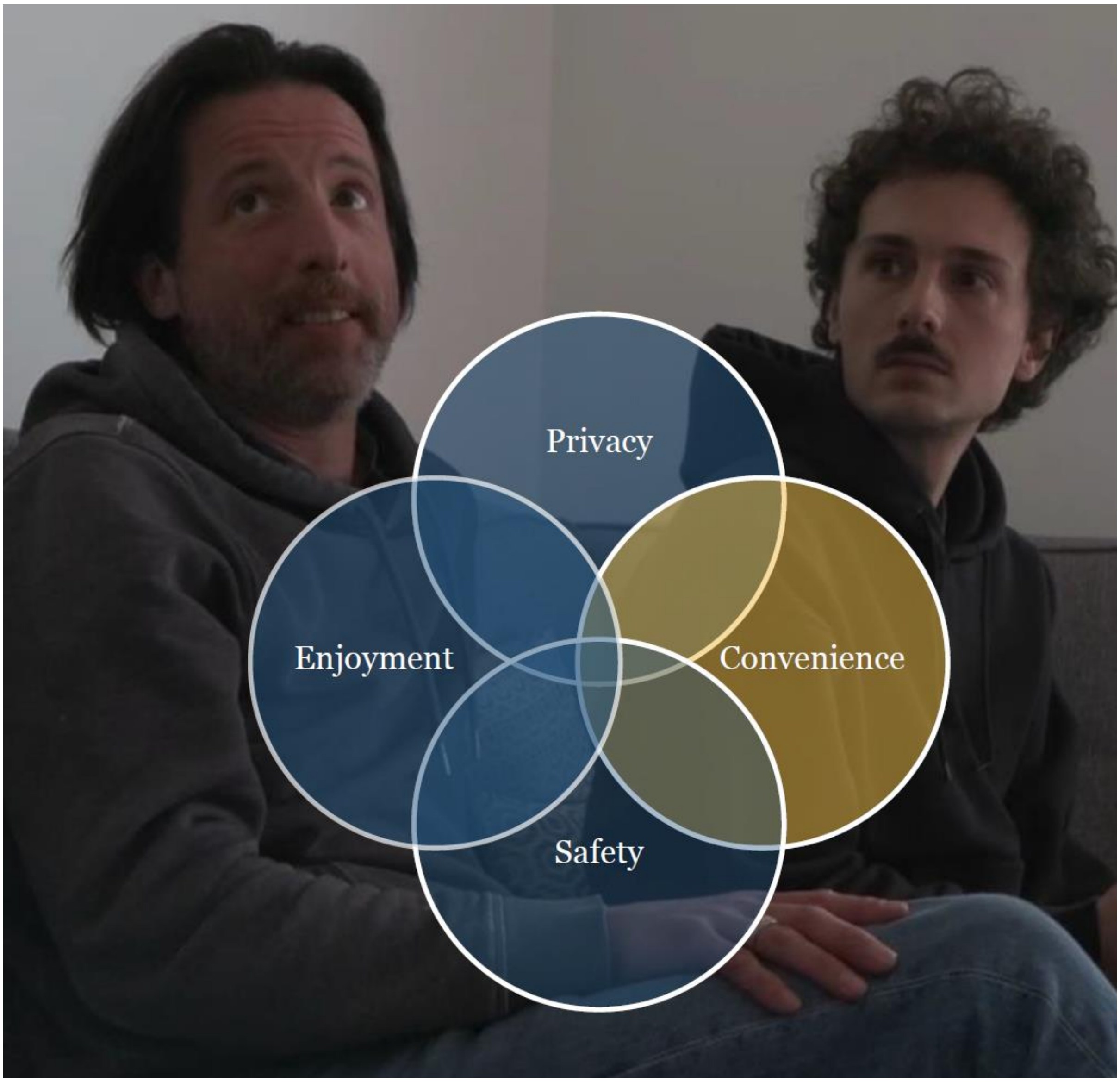
Sharing personal information in pursuit of economic security is not new. In Year 1, the research encountered people sharing information about their disabilities to secure Universal Credit, or information about their backgrounds to secure employment.

This year, however, the need to share personal information to stay afloat feels **more urgent** and more diverse.

Whether using ChatGPT to submit a job application or consenting to (or tolerating) the use of LLMs in the processing of that job application, users are recognising a considerable and increasing opportunity cost to opting out of data sharing or asserting privacy rights.

Users have not yet encountered "pay-for-privacy" in their day- to-day lives, but they are beginning to suspect that privacy is a luxury they cannot always afford in the face of redundancy or economic distress.

"I started using it last year for answering interview questions. It would literally give you fabulous examples of how to answer. You don't need to put in personal information." **(Anonymous)**



Ability: What am I able to do?

These pressures are a strong contributor to people seeking escapism and play

Data playgrounds

Users are implicitly (though sometimes explicitly) trading off privacy for the sheer enjoyment of sharing, whether with their close friends or with the broader online public.

The gamified and trend-led nature of online services can lead to a fear of missing out.

Deciding not to use a service is rarely as simple as "opting out": the user must also opt out of the social dynamics and trends that form around that service. For younger participants like Abi, tools like Snapchat let her be part of the fun, with little thought given to what data is being provided to whom in the process.

This tendency was particularly marked around children. Anna's son enjoys making skits on TikTok. This is stressful for Anna, who worries that he will inadvertently say something that will harm his reputation. She has asked that he not show his face in these videos, but this rule has not always been followed.

Similarly, Anna's son enjoys playing video games like Valorant which "need" voice chat to coordinate between players. Considerable amounts of data are transacted in the process of being part of the in-group.

"You hear more people having issues with privacy on social media. But that's not going to stop me from using them because I just want to chat with my friends and stuff." **(Abi, Bristol)**

As illustrated in the Venn diagram this year, "enjoyment" emerged as a factor in the privacy trade-off that was not observed last year.

Motivation: What do I want to do?

Sayeda creates a BeReal post with her ethnographic researcher, enjoying the opportunity to share the research process with her close friends.

The format and user experience of data sharing technology directly impacts how users transact their information

"Don't call unless it's serious"

The diverse settings and contexts in which a person shares, or does not share, influences their **motivation** to protect their data, as well as their framing and **perception** of the behaviour itself.

Sayeda showed us that even the format of a phone call can influence how "serious" the context is. Her friend phoned her using audio only – this worried her, and made her think something was wrong, because in her circle, Facetime is the default unless something deeply private or personal needs to be discussed. Data behaviours are therefore influenced at the subcultural level.

Similarly, for Kaylee, a targeted advert about something that interests her will make her feel warmer towards the process of data sharing that led to that advert than an irrelevant or uninteresting one.

It is difficult in such a diverse online landscape to form a coherent view about what the user really feels about the data sharing process.

Frustrations with data sharing can therefore be fleeting and inconsistent. While the research did uncover pockets of frustration, even outrage, around data processing, **users did not stay outraged for long.**

"When my home got broken into… it felt so invasive. But that's how you should feel about your data. It's only in the past year that I've thought 'I'm annoyed at how much information people know about me.' "
(Alanna, Manchester)

Perception: How do I think about my choices?

The format of data sharing technologies can also lead to outright misconceptions about how information is used

Friends only

A common assumption among participants in this research, particularly younger ones, was that if social media posts are **"made private",** they must also be private to the organisation behind the social media, or to their advertising partners.

The format of social media makes this an easy heuristic to fall into: users struggled to articulate exactly how their data might be used and instead focused on whether their friends, mutual friends, or the public at large, could see their content.

Across the sample, researchers observed that people tended to **overestimate the degree of control** they had over ad-tech and social media privacy more generally.

People frequently assumed that if they had expressed a preference on an advert, they had also expressed a preference over the data collected to serve them that advert.

Users were proud of the fact that they had "tamed" their algorithm to only serve content they enjoyed, but beneath this apparent mastery, their data transactions and privacy decisions remained unexamined and **uninterrogated**.

"My posts are private. AI doesn't have access to them. None of my friends have public accounts… If you had a private account they'd ask for your consent before doing anything with it. It's just an unspoken rule."
(Janet's daughter, London)

Perception: How do I think about my choices?

Users make a distinction between serious and unserious data use

"Important" data

The tone, language and user interface of a data sharing service can impact the user's attitude towards their personal information. In other words, a person may behave cautiously around their address or date of birth in "serious" environments, but less carefully in "playful" ones.

In line with last year, parents behaved a great deal more carefully with their children's personal information than they did with their own.

Likewise, they may use passwords and two-factor authentication in the workplace, but not in the home. Professional knowledge of GDPR does not always translate to implementing its principles in the home. Users were observed taking great care over forms of data that are well-established as "serious", such as financial or health information, but far less so around data that became associated with their leisure or personal lives. The tendency to see data protection as a form of "work" often left it excluded from times of play.

A five-year-old showed us the videos he watches (and is recommended) through the family YouTube account. For adults and children alike, privacy and personal data risk becoming collateral in the pursuit of play.

"Ah that's bad, they're meant to be back in their file. It's all the information about where they're born; you keep it 'til their five. It's their hospital number, their NHS number… It's quite a big thing really, isn't it?"
(Kristy, Manchester, On her children's medical Records)

Location tracking can blur the line between safety and enjoyment

Shifting norms

Users of location tracking software highlighted its value for keeping themselves, their families and their friends safe. As illustrated in the earlier Venn diagram, safety was highlighted in the privacy trade-off.

But this was not without its fun side: participants joked with each other about changes in their whereabouts, or odd locations they had seen each other at. This combination of the serious and the playful can make location tracking feel compulsory to take part in social life, primarily for children and young adults. As norms shift, new and innovative forms of data collection can be harder still to opt out of.

"It's just funny – in the morning I can check and see whether my friend's going to come into school because she would have been online. The first thing she does in the morning is go on Snapchat so if she's not on, she's not going to get to school for an hour." **(Sayeda, Manchester)**

"I don't have to ask my friends where they are; I just want to know why they left the house – was it to go to the shop or go to uni?" **(Lara, Reading)**

New forms of data sharing can become normalised, entering the mainstream

"A bit of a conspiracy theorist"

Since last year, the **social rules** appear to have shifted in favour of accepting data sharing on the part of large organisations; or accepting it as part-and-parcel of modern life.

There was a striking tendency to disregard, or even **mock**, people for taking a negative stance on forms of data collection that (currently) feel normal.

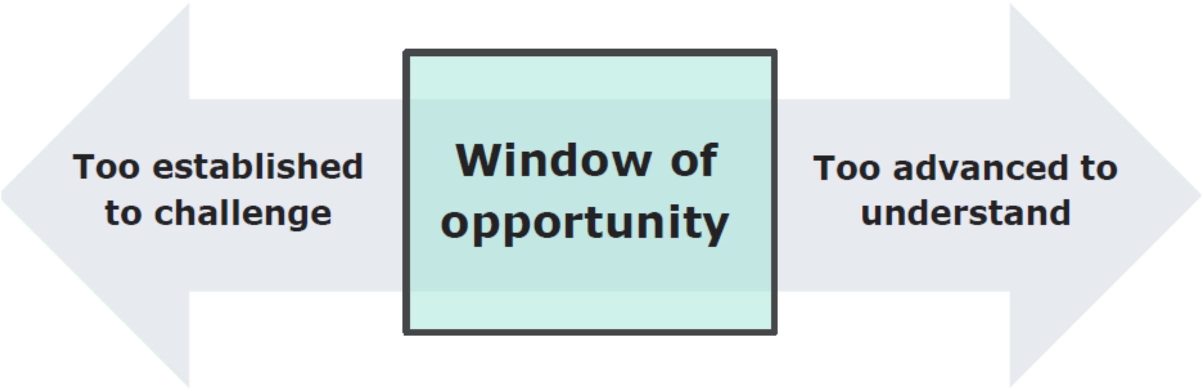
In one house-share, a tenant joked that researchers would never get to speak to one flatmate because he's "a bit of a conspiracy theorist;" a refrain that became common as the research progressed.

This year's research highlights the pace at which new forms of technology can become part of the social fabric of UK life. For those who object, their window of opportunity to do so can be narrow.

"I don't think much of it to be honest. I'm not a conspiracy theorist so I just get ChatGPT to do what I want it to do really." **(Abi, Bristol)**

"Well, biometrics… I mean we have biometric passports now and they've been around for ages." **(Philip, Belfast)**

New technology



Generative AI represents an opportunity to nuance and influence the conversation before usage trends become settled fact. The public know enough to be concerned about the technology, but not enough to know why.

Social: What are the people around me doing?

But sometimes, this normalisation comes from a belief that data sharing is simply beyond the public's control

"Alexa, are you listening?"

Chapter 1 argued that mainstream data sharing technologies can run counter to the social norms participants espoused. This being the case, the calmness, even **resignation**, towards these same forms of data processing among the public is striking.

Throughout the research, participants experienced brief, uncanny encounters with technology where it behaved differently to how they thought it would, or how they felt it ought to.

Janet's new Alexa inexplicably addressed her husband Pascal by name, without being linked to Pascal's account. This prompted a household review of how voice assistants collect and use their data, which did not lead to any answers they could act upon.

These unsettling episodes can make the public feel as though the curtain has briefly lifted, giving a taste of how much their privacy has been compromised but offering no ability to take back control.

A common response to these odd encounters was to simply take it in their stride: people may find it amusing, or **absurd**, but these responses did little to help the user assert their rights or tailor the technology to their needs.

"I do think your phone can hear you, which sometimes scares me. It's just weird." **(Lara, Reading)**

Physical: What resources do I have access to?

Chapter 4
Technology, Regulation and the Future

Introduction

2025 and beyond

This chapter focuses on specific, forward-looking questions of importance to the ICO and its 2025 Strategy. To do this, the research explored public perceptions of certain new technologies, regulatory challenges and the ICO itself. In particular:

- **Large-Language Models** (LLMs).
- "**Pay-for-privacy**" – allowing the user to opt out of data sharing for a fee.
- **Ad-tech** – tailoring advertising to the user's data profile.

Beyond this, researchers asked participants to reflect on what they personally would like to see from the ICO as an organisation: how might it help them be empowered through their data, and safeguarded against harm?

"I think the ICO should focus on AI; because I know that's absolutely going to take a lot of personal information. It's the new thing: a few years ago, you had crypto but now it's AI." **(Kaylee, Cardiff)**

Technology, Regulation and the Future

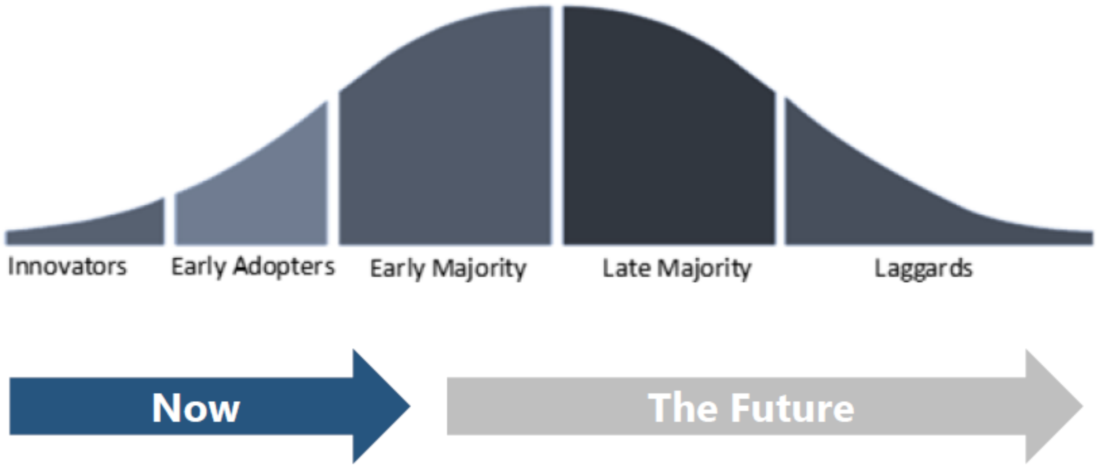
Key Insights

1. While users tended to feel comfortable with the information that they share with LLMs, the **inferences made** about them by LLMs was less clear, and, on explanation, unsettling.

2. The public take an **outcomes-focused approach** to advertising technology, and struggled to distinguish harms caused by data sharing from harms caused by advertising.

3. **Pay-for-privacy was worrying**. It tended to be read as insurance against what the organisation could do, or might do, rather than what it is currently doing.

4. Public engagement with the ICO will require **clarity** on the timing and expected outcomes of that engagement, but the prospect of speaking to an advisor was well-liked.



Rogers' Diffusion of Innovation model suggests that technological adoption is spearheaded by the most innovative and enthusiastic users before filtering into the early majority. While AI has entered the early majority, we can expect it to become still more mainstream and widespread in the future.

This year saw LLMs move from the cutting edge to the early mainstream

Artificial Intelligence

Year 2 saw people who had not even heard of **ChatGPT** 12 months ago using it in their daily lives, albeit irregularly.

The use cases for LLMs are still being established among the public, but in this research, users tended to use it for:

- Job applications
- "Googling" questions
- Writing work emails

While the public do not always have a clear sense of how LLMs "work," they have established workarounds to ensure that they are not disclosing more about themselves than they might wish to. Fake names, or "**dummy data**", as one participant put it, were common, to ensure that their personal information does not become attached to their query. Importantly, users of AI are discerning and careful about telling the model about **other people**. However, existing AI users tended to be knowledgeable, early adopters of tech: this considerate approach may change as adoption widens.

Respondents were told that because of how LLMs are trained, they may not be able to correct, amend or delete their information. This was not necessarily met with alarm: users generally trusted themselves not to input data into the LLM that they would not want shared, and the aggregated nature of LLM data simply felt too large and "anonymous" to create harm for the user.

Some misconceptions are developing around how data is transacted in LLMs

"Think what you like"

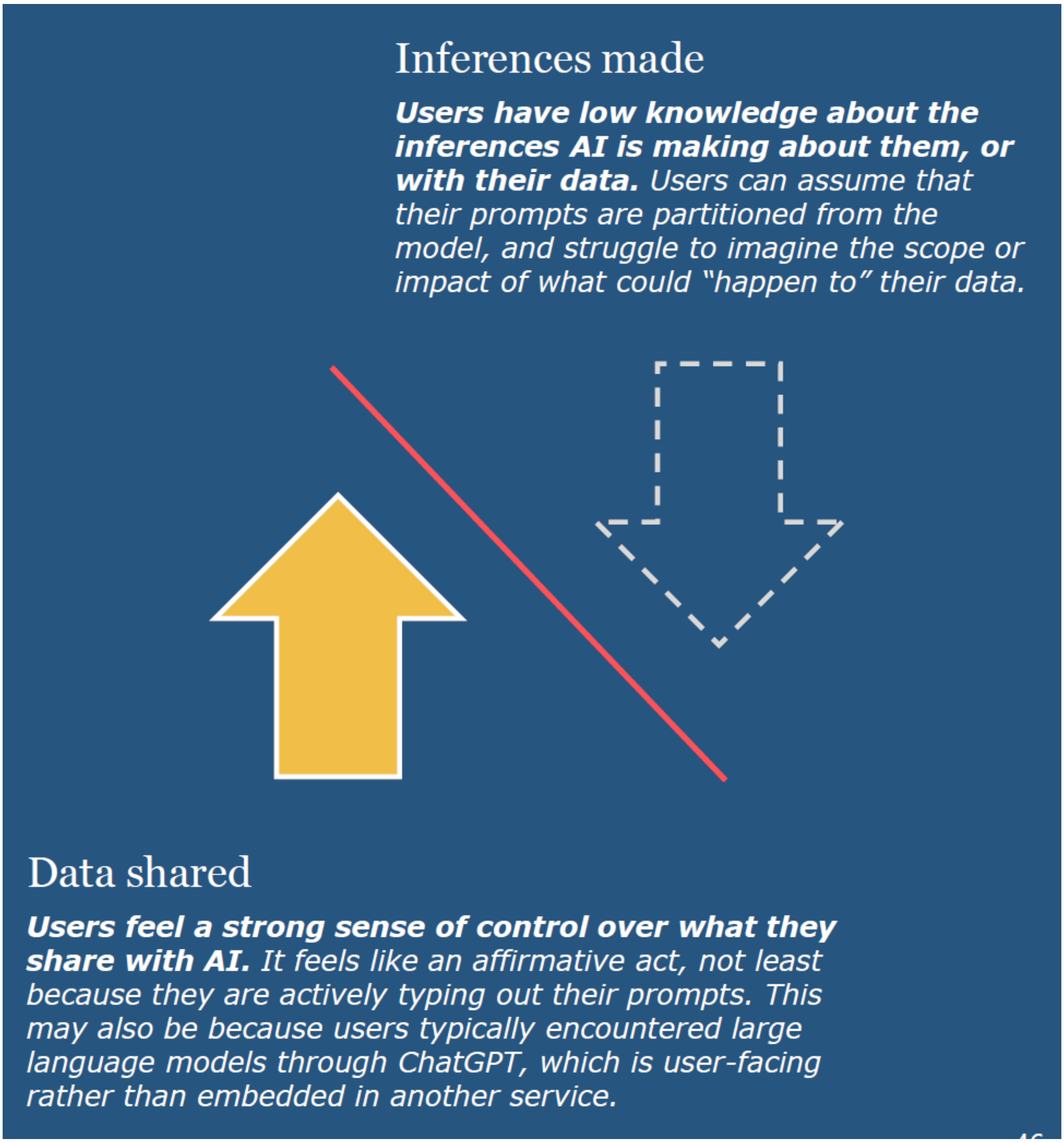
Last year, researchers asked whether respondents worried about how organisations **analysed, handled or inferred** from their data. Often, the response was muted: "You can think what you like about me", was a common reply.

In essence, the public are not used to thinking about the **"back-end"** of data sharing. Before the mainstreaming of LLMs, the data-sharing process felt one-way: data is shared, and the organisation holds onto it for some purpose or another.

Now, the public are contending with the prospect of their data being aggregated, disseminated and potentially **distorted** as LLMs respond to the prompts of other users. They have not yet come to a view on this: even when explained by a researcher, the implications still feel hypothetical, or as Janet's daughter put it, "just a bit step, step, step." Users felt it was unlikely, but not impossible, that their prompt history could be linked back to them.

To understand the full implications of AI, people felt that they would need to **become conspiracy theorists**: to imagine a worst-case scenario and work backwards from it. This is a difficult, perhaps even undesirable, mindset shift.

"It has the power to make banks more efficient, but not if you're on the receiving end and having decisions made about you." **(Mas, London)**



Inferences made

Users have low knowledge about the inferences AI is making about them, or with their data. *Users can assume that their prompts are partitioned from the model, and struggle to imagine the scope or impact of what could "happen to" their data.*

Data shared

Users feel a strong sense of control over what they share with AI. *It feels like an affirmative act, not least because they are actively typing out their prompts. This may also be because users typically encountered large language models through ChatGPT, which is user-facing rather than embedded in another service.*

Special Category data was a foreign concept to participants, but the identities it can represent matter greatly

Identity and Data

Respondents were asked about and shown the different kinds of special category data that exist under the GDPR.

Understandably, the public did not always feel that these categories reflected what mattered to them about their identities and ways of life.

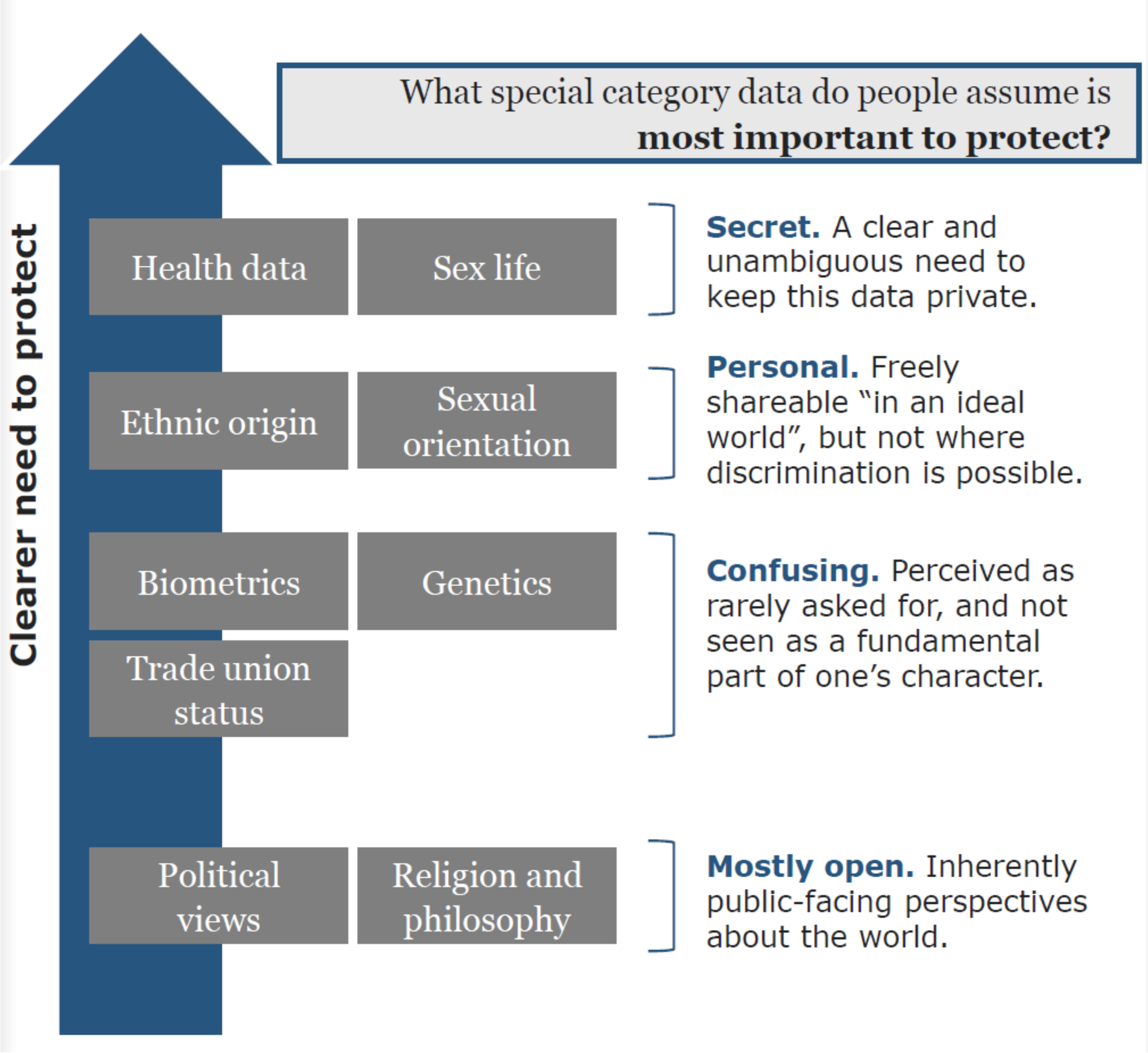
Data is an abstraction of a person, and people tended to argue that the Special Category data did not matter more than other forms of data, unless and until a bad actor decides to discriminate against them for those characteristics.

Accordingly, the public rarely paid additional attention to their special category data. They could not recall giving separate permission to organisations to use it and were surprised to learn that this is required under the GPDR.

This perception of special category data can lead people to feel that it only matters if they are from a marginalised or vulnerable group. White, male or able-bodied participants tended to self-exclude from the discussion, as if they didn't "have" special category data to begin with.

"I don't know about "ethnicity." Maybe "culture" makes more sense."
(Sheila, West Lothians)

What special category data do people assume is **most important to protect**?



What special category data do people assume is **most important to protect?**

Secret. A clear and unambiguous need to keep this data private.

Personal. Freely shareable "in an ideal world", but not where discrimination is possible.

Confusing. Perceived as rarely asked for, and not seen as a fundamental part of one's character.

Mostly open. Inherently public-facing perspectives about the world.

Ad-tech risks being misunderstood, and the public can struggle to unpick the data it deals in

Front-end and back-end

Ad-tech serves as an important **clue** to the user as to how much data they have shared with a particular organisation. It has been a spur for several participants to interrogate how much data they have shared, and ultimately what organisations know about them.

As with last year, it remains difficult to unpick where the **potential for harm** in ad-tech sits – with the advertising itself, which users can find irrelevant, offensive or boring; or with the data being collected to serve those adverts in the first place.

A consensus formed that data collection was harmful if it led to advertising being shown that was also harmful: a form of data being "**weaponised**." Whether this harm is mitigated through the regulation of advertising or of data collection felt somewhat academic to participants.

Likewise, people felt that advertising was the core motive for asking for data in the first place. As discussed in Chapter 3, this has become **normalised**, and gradually (if uncomfortably) assimilated into the social contract between users and organisations.

As Christians, **Mas and Simon** try to ensure that their children are not exposed to Hallowe'en-themed videos or advertising on YouTube. This is a dilemma: if YouTube knew about their religious beliefs, they could potentially avoid serving this kind of content, but the user would be giving up more data as a result.

As it stands, Mas has paid for YouTube Premium to avoid having his children targeted by advertising. But the data being collected is unchanged. He has not paid for privacy: he has paid to have the results of his data sharing hidden from him.

The concept of “pay-for-privacy” feels less distant and hypothetical than Year 1

Thin end of the wedge

Last year, the idea of “paying for privacy” felt unlikely, even absurd, to participants in the research. This year, while participants had not encountered the trade-off personally, it felt more real, more likely, and more **frustrating**.

Participants struggled to evaluate whether they personally would opt in to such an arrangement. This is understandable: people are generally comfortable with, or at least tolerant of, the status quo of data sharing.

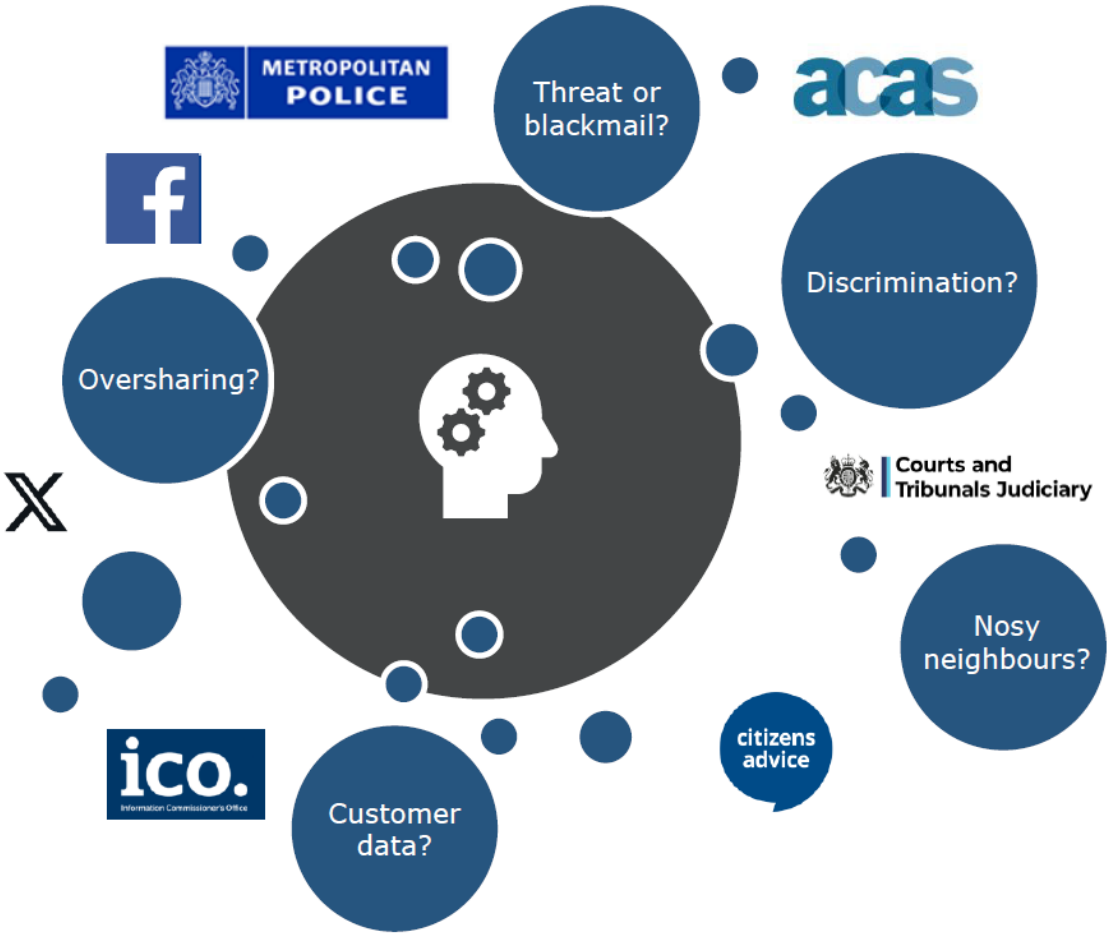
Pay-for-privacy was therefore read as insurance against what the organisation *might* do, rather than what it is currently doing. This is an asymmetrical power dynamic, and would, in participants’ eyes, reflect poorly on the organisation offering it. People did not feel that paying for privacy would leave them with a net gain, but rather a safeguard against the changeable nature of data sharing, to which they cannot assign a monetary value.

“Even if it’s £2 a month, that adds up per app, and it’s not the time to be paying that kind of money.” **(Kristy, Manchester)**

“A good site will say “tick this box if you don’t object to us passing your information to a third party.” I like it upfront. I like people to be upfront.” **(Walter, Bristol)**

“I didn’t tick that. That’s the default setting…!” **(James, London)**

Users struggle to identify the best port of call for a data concern



“I never knew about the ICO, but Citizens’ Advice should have directed us to them. It all just seems like a minefield.” **(Katie, Cardiff)**

Engagement with the ICO can feel unfeasible for the public, in part due to the diverse nature of "data harms"

Minefields

While people recognised that interacting with the ICO would probably be straightforward, they expressed real confusion about exactly what they would ask the ICO to do for them once contact had been made.

As discussed in Chapter 2, the UK public know how to advocate for themselves when the harms they feel are clear. With personal data, people tend not to know if they have been wronged, by whom, and **to what extent**.

Participants sought **clarity** over when in the process they might want to reach out to the ICO. Is this a preventative step, a reactive one, or both?

"Maybe there needs to be a QR code on everything you buy or every website you visit so you can go down that path if something happens. But I wouldn't unless something happened, or it happened to someone I knew." **(Caroline, Manchester)**

"Chat to an adviser" is music to my ears. I can just talk and get some guidance and say, 'Something's happened, can you advise me on what to do?'" **(Sheila, West Lothians)**

And fundamentally, the public still hope that the ICO will pre-empt data harms

Horizon scanning

The respondents in this research expected the ICO to take a **predictive approach** to data harms.

This year's exploration of the social contract suggests that taking a worst-case scenario or "conspiratorial" approach to data sharing is not always compatible with our participants' lives. Their peers will continue to encourage them to share data on social media; their prospective employers will continue to ask for personal details.

Participants wanted to engage with organisations in the spirit of **good faith**, but asserting data rights can feel like an expression of mistrust that is difficult to maintain when so much data sharing has been normalised.

The public make data decisions with **incomplete information** about the motives of the organisation, and in the absence of this knowledge, they expected the ICO to think "conspiratorially" on their behalf.

For this reason, the public sometimes felt that researchers were **asking the wrong question**: by the time they need to reach out to the ICO, the damage has been done.

There is, however, still genuine warmth to the idea of talking to an advisor. Respondents expected this to be a wide- ranging and informative conversation, offering concrete steps that the user can take to wind back some of the data sharing they regretted and helping the user establish who, ultimately, is to **blame**.

"I don't know how the ICO could help me because I don't know how this stats stuff works. I don't know what I'd need to be aware of. So, when I accept cookies, it's just collecting my preferences? That seems fine." **(Lara, Reading)**

Conclusions

Conclusions and Key Insights

These ten conclusions build on last year's insights, as well as incorporating entirely new ideas found in Year 2 of the research.

1. Data protection is a form of labour, with few opportunities to learn how to do it well.

   The public tended to read "data protection" as a set of responsibilities, rather than rights. Participants revisited from Year 1 had not significantly changed their behaviour, citing a **lack of knowledge** about where to even begin the process of "taking control" of their personal information.

2. Reminding the public about their role as Domestic DPOs can make data more engaging.

   Participants tended to minimise the importance of their data protection work, seeing it as just another part of managing a household. There is value in reminding the public that these activities are **meaningful**, both in terms of protecting their data and empowering them to use their data to achieve their goals.

3. Data empowerment risks being read by the public as a call to cynicism, even paranoia.

   This year's research highlighted a stigma against being perceived as a "conspiracy theorist" with regards to data. This is reasonable: participating meaningfully in social and civic life is difficult without some trust, however reluctant, towards institutions and organisations. However, participants tended to feel that the "ask" of data empowerment was to become conspiratorial and to **assume the worst**. Because data rights feel intangible, even people who want to engage feel forced to think in hypotheticals, and risk being thought of as awkward or unreasonable.

4. New technology can stress the social contract, alienating users from their underlying values.

   The public have intrinsic values and beliefs about where the boundaries of data sharing should sit. However, the social contract is not watertight, and new technologies can lead users to make exceptions, however subtle, to the rules they would otherwise abide by. What would once be mocked as "curtain twitching" can feel reasonable in the context of smart doorbells. Large step-changes in technology represent a **narrow window of opportunity** to engage the public and invite them to consider their values and where data might come to matter.

5. Users are reading promises and reassurances into digital services that are not always kept.

   Across the spectrum of digital competency, participants take the brand identities and tone-of-voice of digital services as an implicit promise that their data will be handled in line with the social contract. Whether these assumptions are "reasonable" or not, organisations risk **losing trust** by failing to live up to expectations they have not been able to manage.

6. Special category information is not well-differentiated or distinct among the public.

   There was little evidence in this research that special category data is treated "differently", unless the person has a suspicion that the data can be "used against them." This was a particular concern for religious or sexual preference, but only for those who saw themselves as **marginalised** within those categories.

7. Cost of living pressures can make personal data sharing feel compulsory

   Participants in this research existed on a spectrum of **vulnerability**, whether financial, health-based or otherwise. While participants consented to sharing data in pursuit of a job, a government benefit, health services or a place to live, it did not feel to them like a choice in the true sense of the word.

8. The public expect a greater degree of transparency than the "purpose" of data collection.

   We have known since Year 1 that the public can be pessimistic about organisations' motives for requesting personal data, and we have seen this persist into Year 2. This year, however, saw a more explicit and firm belief that organisations are **concealing** their motives behind the "purpose" as specified under the GDPR.

9. Pay-for-privacy can foster ill-will if organisations are unclear about why it is being offered.

   Offering not to transact the user’s data in exchange for payment raises unsettling questions in the user’s mind: what have they been doing up to this point, and what might they do in the future? The user may not know what they are paying for, but the insinuation of pay-for-privacy is that the user **ought to be worried.**

10. Data sharing alternates between a form of work and a form of play.

    People tended to see data sharing and its associated behaviours as a chore, or a form of entertainment. For encouraging data empowerment or data safety, **neither is optimal**. The public take cues from the organisation about how they “ought” to behave while using the service, meaning organisations have the potential to directly encourage caution or carelessness with data.