



# Public dialogue on location data ethics

Engagement report

**Geospatial Commission**

NOVEMBER 2021



# Version control

Document information	
<b>Client</b>	Geospatial Commission
<b>Title</b>	Public dialogue on location data ethics
<b>Subtitle</b>	Engagement report
<b>Dates</b>	24 November 2021
<b>Status</b>	Released
<b>Classification</b>	Open
<b>Project code</b>	11281
<b>Authors</b>	Maddy Maxwell, Skye McCool, Aidan Peppin, Katie Spittle, Tom Stocks
<b>Quality assurance by</b>	Anna McKeon
<b>Main point of contact</b>	Skye McCool
<b>Email</b>	<a href="mailto:skye.mccool@traverse.ltd">skye.mccool@traverse.ltd</a>

# Contents

Foreword	4
Executive summary	7
1. Introduction	10
2. Background and framing	18
3. Findings: Awareness and understanding of location data	23
4. Findings: Data insecurity	41
5. Findings: Accountability, agency, and governance	48
6. Findings: Reliance on and choices about data	57
7. Conclusion	65

# Foreword

Location data underpins our modern digital society, powering our everyday lives and driving innovation and better services. We have long been interested in capturing and accessing data about where we are and what we do. The widespread use of new technologies means that data about our lives, including location data, is available in increasing frequency, detail and accuracy. This necessary evolution of our geospatial ecosystem raises new and significant ethical considerations.

Last year, the Geospatial Commission published the UK's Geospatial Strategy, with an ambitious vision to unlock the power of location data. The Strategy recognises that society can only continue to benefit from the widespread use of location data and its future opportunities if location data is used in a way that retains public confidence.

The Geospatial Commission therefore committed to providing guidance about how to unlock location data's immense value, while mitigating ethical and privacy concerns. To inform this guidance, we embarked on a programme of work, starting with an independent public dialogue, which is one of the UK's first deliberative consultations on location data. The dialogue has been supported by an independent and diverse expert Oversight Group that we formed to guide this process. The findings of the dialogue are captured in this report.

The report provides evidence on public perceptions about location data use, offering valuable insights into what citizens believe are the key benefits and today's concerns. These findings can start to shape our priorities for future guidance. In this context, of particular note are the findings that relate to:

- **Personal location data:** Location data can be defined as both personal data that can be used to identify individuals, and non-personal data that can describe the location of objects, features or aggregated population data. Participants generally felt more comfortable when location data was not linked with data about individuals, and when location data linked with data about people was aggregated and anonymous.
- **Who benefits:** The report reveals how trust in the use of personal location data changes depending on whether participants felt the objective was to benefit wider society or to make profit. Participants were more content with businesses using their personal data when there was a clear and direct benefit to them or wider society.
- **Communicating clearly:** Participants felt that there was a general lack of clear information around location data use and that succinct, more accessible communication could help overcome feelings of data insecurity and empower more informed choices.

Translating the evidence we are gathering into guidance is bound to be complex. This includes understanding where the public's sentiments about data sharing differ from the decisions they make about their data every day, and why. Enabling innovation through improved access to location data will remain a priority. Innovations to date have given industry and governments the tools needed to take on the greatest global challenges, from protecting our planet from the impact of climate change, through to coordinating a public health response to the Covid-19 pandemic. We will continue our programme of work to explore the opportunities and how we operationalise the findings of the report, including what more transparency would look like in practice to move the public from feeling like data subjects to being empowered data citizens.

I am confident that, through engaging a diverse set of voices, we can continue to support the UK to reap the economic, social, and environmental benefits of location data in a way that mitigates ethical and privacy concerns and grows the trust of citizens. Today's report is an important step in achieving that aim.

I am grateful to all those who contributed to this project, including the UK Research and Innovation's Sciencewise programme, which provided funding and expertise; Traverse and the Ada Lovelace Institute, who designed and delivered the public dialogue; the members of our independent Oversight Group, in particular John Pullinger as chair, who ensured the expertise and independence of the project; and the members of the public, who so whole-heartedly participated and contributed to the debate.



**Thalia Baldwin**

**Director**

**Geospatial Commission**



The Geospatial Commission and the UKRI Sciencewise programme commissioned Traverse and the Ada Lovelace Institute to deliver a public dialogue on the ethics of location data use.

The Geospatial Commission wanted to understand participants' attitudes towards location data, in order to inform its policy development in this area.

85 participants from across the UK

5 significantly impacted groups involved

4 online workshops

7 specialist presentations

## What participants thought about location data



Participants saw location data as a subset of their personal data



Key **benefits** related to emergencies, planning, health, and convenience



Participants saw the ethics of location data use as complex, with no easy answers



Key **concerns** related to data breaches and misuse, privacy, and discrimination



Participants felt more concerned about data that could identify people



Opportunities often related to society, while risks focussed on individual impacts

### Data insecurity



Participants used the language of data security and safety to convey feelings of insecurity and powerlessness over how their data was being used and by whom. Risks of data misuse or 'breaches' deepened these feelings.

### Private and public sector use



Many discussions centred around private versus public sector use, as participants were concerned about location data use being primarily profit-driven. While participants prioritised use for public good, they did not equate that to mean 'not making profit'.

### Reliance and choice



For most participants consent with genuine choice was important for identifiable data. They felt that reliance on and ubiquity of digital services limits choice and the ability to opt out, ultimately leading to feeling disempowered.

### Governance and agency



Accountability, agency, and transparency were closely linked. Participants valued agency – they wanted accessible and transparent information to enable choice at the point of consent, and to more easily hold data controllers to account.

## A vision for ethical and trustworthy location data use



#### Intent

How data is used and who benefits are key in considering ethics and trustworthiness



#### Accountability

Data collectors should be accountable to regulators and data subjects



#### Transparency

Information on use, access, and storage should be succinct and accessible



#### Agency

Consent should offer genuine choice to people about how their data is used



# Executive summary

When location data is linked with other data about people and the world we live in, we can gain important insights and create new services that greatly improve how we live, work and travel. With these new opportunities, there are also emerging privacy and ethical considerations. To continue to benefit from location data, it is important that these considerations are addressed, so that location data is used in a way that mitigates concerns and retains public confidence. Understanding public perspectives is key to this, as recognised in the UK's Geospatial Strategy.

In March 2021, the Geospatial Commission and UK Research and Innovation's Sciencewise programme commissioned Traverse and the Ada Lovelace Institute to deliver a public dialogue on the ethics of location data use.

## About the dialogue

Between June and September 2021, the dialogue engaged 85 members of the UK public in a series of online workshops and activities, to gather their views on what trustworthy and ethical uses of location data look like.

The dialogue consisted of a series of online workshops, where participants shared their perspectives towards location data use and reflected on the benefits, concerns, opportunities, and challenges it raises.

Participants considered information about how and why location data can be used, and what governance exists around it. They also heard from subject matter specialists, including data scientists, academics, and industry experts.

The project included focus groups with communities who might be specifically impacted by location data use. These included women who have experienced abuse, refugees and asylum seekers, and Disabled people. We additionally increased the sample of digitally excluded people and Black British people in the main workshops.

## Public perceptions of location data

### Awareness and understanding of location data

**Participants brought a mixed range of awareness about location data to the dialogue.** Initially, most participants reported that they knew only a little or nothing at all about location data, and many were surprised about how much location data they might be sharing and saw location data as a subset of their personal data. By the end of the dialogue, almost all participants felt they knew a fair amount or a great deal about location data.

## Benefits and risks of location data

Participants thought the key benefits of location data related to safety and public services, like health and city planning; while the key concerns related to data breaches and misuse, privacy and discrimination. Overall, benefits were most often framed as being for the wider public, while risks were focussed on individual concerns.

## Data insecurity

Participants reflected feelings of insecurity and concern about how data about them was used and by whom. Many participants did not trust that data was being used in their best interests and felt powerless to change this. The risk that data might be misused or 'breached' deepened these feelings.

## Accountability and governance

Participants discussed how effective regulation, accountability and transparency are essential for ensuring trustworthy uses of location data. Some participants were concerned about the ability of regulators and the government to effectively hold data collectors accountable, especially powerful multi-national companies. Most participants also felt that current information about data use is inaccessible to them, as it is too complex or hidden within lengthy text.

## Reliance on and choices about data

Participants wanted more granular and less intrusive or complex ways to consent to, or have control over, how their location data is collected and used. They felt that the burden of solving challenges related to consent should not be on the data subject, and expressed feelings of resignation, disempowerment and/or ambivalence about location data collection and use.

## Dialogue conclusions: towards trustworthy and ethical location data use

**Throughout the dialogue, participants recognised that the potential uses of location data and their consequences are complex, and that there are no easy answers for ensuring ethical practice.** When reflecting on how the benefits and concerns of location data could be balanced, participants reflected on various conditions that suggest four components of ethical and trustworthy location data use:

### 1. Intent to benefit society



Participants think that why location data is used and who benefits from it are important when considering whether location data use is ethical and trustworthy, and that benefits to members of the public or wider society should be prioritised.



## 2. Effective accountability



Participants think data collectors should be accountable to regulators and data subjects, with consequences for breaches or misuse, and they questioned whether current governance is effective in achieving this.

## 3. Accessible transparency



Participants want data collectors to communicate in an accessible way what location data will be used for, who will have access, and how it will be stored, so people can make informed choices and ensure accountability.

## 4. Enable agency



Participants want more genuine ways to consent to and participate in ongoing data storage and use, and greater choice over how their data is used.

To our knowledge, this is among the first public dialogue projects on the specific topic of location data to ever be held in the UK. The findings from this dialogue should be at the core of any future policy and strategy work, to ensure that wider public interests are reflected.

# 1. Introduction

## Context

When location data is linked with other data about people and the world we live in, we can gain important insights and create new services that have the potential to improve how we live, work and travel. It is important that as this practice continues to expand, organisations consider privacy and ethical concerns around the use of location data in a way that retains public confidence and mitigates risks and concerns. Retaining the public's confidence in the use (and sharing) of location data means that we can make the most of opportunities and maximise benefits to individuals and society.

Whilst there is a growing body of research on the ethics of location data, and location data sharing, there is a significant gap in terms of understanding public attitudes, perceptions, and norms and expectations, as discussed in the next chapter. Location data can, in combination with other types of information, or by way of inference, reveal a range of personal characteristics about an individual. This raises particularly challenging questions relating to privacy, surveillance, discrimination, and equity. However, when used in a way that considers ethical and privacy concerns, location data can generate substantial public benefits and positive outcomes. Public dialogue can help understand these concerns and opportunities to address them.

[The Geospatial Commission](#) is responsible for setting the UK's geospatial strategy and coordinating public sector geospatial activity. The Geospatial Commission and UK Research and Innovation's [Sciencewise](#) programme commissioned this public dialogue in March 2021, as part of 'Mission 1: Promote and safeguard the use of location data' in [the UK's Geospatial Strategy](#) – a broad programme of work to develop guidance on how to unlock value from sensitive location data while mitigating ethical and privacy risks.<sup>1</sup>

The project has been delivered with support from public dialogue and data specialists [Traverse](#) and the [Ada Lovelace Institute](#), and aimed to open a conversation with members of the public to gather evidence on public attitudes and priorities around ethical location data use. An Oversight Group provided expert support and quality assurance.

---

<sup>1</sup>

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/894755/Geospatial\\_Strategy.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/894755/Geospatial_Strategy.pdf)

## Objectives and research questions

This project had three objectives:

- to engage a diverse section of the public, broadly reflective of the UK population;
- to understand participants' attitudes to location data and explore what risks, challenges and ethical considerations are brought about by its use; and
- to involve participants in the design of recommendations for the trustworthy and ethical use of location data, to help inform the Geospatial Commission's policy and guidance on the topic.

To achieve these aims, the design of the dialogue process and materials was guided by five **research questions**.

- What awareness do participants have of location data?
- What are participants' aspirations and concerns for location data?
- What do participants perceive the ethical issues to be, and how do they prioritise them?
- What are the conditions of trustworthiness for location data users<sup>2</sup> and processes?
- What experiences, values, and principles shape participants' views?

The findings from this public dialogue can be used to **inform research and practice** in the following ways:

- to inform more trustworthy and responsible uses of location data, to build public confidence and support;
- to inform wider work and research on location data ethics, in academia, private and public sector;
- to inform future research strategy & policy that supports unlocking the value of location data; and
- to inform guidance for the private and public sector on the appropriate use of location data, and government's future public engagement and communication approach on location data.

## Method

### Sciencewise approach

[Sciencewise](#) is an internationally recognised public engagement programme which helps to ensure research and policy is informed by the views and aspirations of the public. The programme is led and funded by UK Research and Innovation (UKRI).

---

<sup>2</sup> 'Data users' was the language used in the agreed research questions, however this is referred to as 'data controllers' throughout the rest of this report.

Sciencewise supports policymakers and research funders to carry out public dialogues on issues with a scientific or technological component.

This public dialogue was conducted in line with [Sciencewise Guiding Principles](#)<sup>3</sup>, including their latest quality framework and considerations for online dialogues, and supported by a Sciencewise dialogue and engagement specialist. As with all Sciencewise projects, an independent evaluation was commissioned at the beginning of the project in this instance from Sophie Reid.

## Project governance

Two groups were convened to manage and govern the project: the project management team, and the Oversight Group. Project delivery – in terms of project management, design, facilitation, analysis, and reporting – was led by Traverse with support from the Ada Lovelace Institute. For more detail on project governance, see Appendix A.

## Participants

For the main dialogue process, we recruited 85 people, organised into groups of no more than 7 people for the discursive and deliberative elements of the dialogue. These groups were consistent throughout the dialogue, other than the final workshop which included a sub-set of participants in new groups. We worked with a fieldwork agency to recruit a group of participants that was broadly reflective of the UK population, boosting for certain characteristics to ensure that each small group would be sufficiently diverse. See Appendix A for more details on participant demographics.

In parallel to recruiting for the main dialogue, we wanted to involve people who identify as being part of communities or groups who could be specifically impacted by location data and the surrounding opportunities and risks. We identified five groups likely to be specifically impacted by the collection and use of location data, based on findings from the topic review and discussions in the stakeholder workshop: digitally excluded people, Black British people, women who have experienced abuse, forced migrants (refugees and asylum seekers), and Disabled people<sup>4</sup>.

We took advice from civil society organisations in terms of how best to involve people from these different groups in the dialogue – either through recruiting them to take part in the main dialogue, or in more focused small group discussions. The approach we took is summarised in Table 1.

---

<sup>3</sup> <https://sciencewise.org.uk/about-sciencewise/our-guiding-principles/>

<sup>4</sup> We capitalise “Disabled” throughout this report in line with the social model of disability, described here: <https://www.disabilityrightsuk.org/social-model-disability-language>

**Table 1: Specifically impacted group involvement**

Specifically impacted group	How they were involved in the dialogue
<b>Digitally excluded people</b>	Recruited to take part in main dialogue
<b>Black British people</b>	Recruited to take part in main dialogue
<b>Women who have experienced abuse</b>	Took part in parallel track of engagement (consisting of a focus group before the first and final main dialogue workshops)
<b>Forced migrants</b>	Took part in parallel track of engagement (consisting of a focus group before the first and final main dialogue workshops)
<b>Disabled people</b>	Took part in parallel track of engagement (consisting of a focus group before the first and final main dialogue workshops)

## Dialogue structure

The process consisted of three workshops delivered on Zoom over 6 weeks, through June and July 2021, with a fourth workshop for a smaller number of participants in September 2021. To ensure we captured a wide range of views and provided participants with the opportunity to meaningfully contribute to the discussion, we also included a participant-led research component to the process. See Appendices B for process plans and C for the materials used throughout the dialogue.

**Figure 1: Dialogue process**



This programme design was informed by a topic review on location data ethics led by the Ada Lovelace Institute, as well as by a workshop with subject matter experts.

Due to the COVID-19 pandemic, the dialogue was designed to take place exclusively online rather than face-to-face, as has previously been the norm for public dialogues. The online nature of the dialogue informed the following design decisions:

- Limiting the time of workshops to two hours each, with a maximum of 4 hours in online workshops on any given day.
- A focus on a virtual, online community space outside of the workshops, to foster relationship-building and informal discussion, in addition to asynchronous activities.
- Incorporating a range of different formats, mediums, and messengers to provide information, to maintain momentum and energy through multi-hour online workshops.

## Analysis and reporting

The Traverse and Ada Lovelace Institute analysis and reporting team met regularly to reflect emerging themes and to develop our thematic analysis approach. After each participant session, facilitators reflected on emerging views from their group discussions. Emerging findings from participant discussions were explored and validated with participants in later workshops to test and refine our understanding.

All qualitative data was thematically coded in Traverse's bespoke analysis tool Magpie. Early findings were shared in the fourth workshop, and in dedicated sessions with specifically impacted groups, for participants to review and comment on.

For a full review of the analysis and reporting process please see Appendix A.

## How to read this report

Findings are reported thematically, following the key themes that emerged through the analysis process. Values such as 'privacy' and recurring themes such as 'trust' are reported on throughout the chapters, to reflect their cross-cutting nature.

Key findings and conclusions developed through the analysis and reporting process are articulated as a 'vision for ethical and trustworthy location data use' in chapter 7. Detailed data and explanations of the method and recruitment process can be found in Appendix A.

## Terminology and language

Through this report, we use the following key terms.

- **Data subject:** "The identified or identifiable living individual to whom personal data relates." <sup>5</sup>

---

<sup>5</sup> <https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/>

- **Data controller:** “A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.”<sup>6</sup>
- **Data about people:** We refer to data about people to distinguish this from data about objects and places. This is different from the ICO definition of personal data<sup>7</sup>, which can be used to identify a data subject.
- **Identifiable location data:** Data about people can (but does not always) include identifiable information – where we are referring to this kind of data, we describe it as identifiable location data.
- **Aggregate data:** When talking about aggregate data, participants were generally talking about aggregate data on the assumption it was anonymous data (location data where people cannot be identified). As such, when we refer to aggregate data in the report, we are referring to aggregate anonymous data.

## Quantifiers

We use quantifiers to give relative weighting to qualitative data, instead of reporting on numbers or percentages of participants, because numeric quantifiers would be misleading given the sample size.

- ‘Most’ or ‘majority’ when a clear majority of participants shared a similar view
- ‘Some’ when a minority of participants shared a similar view
- ‘A few’ when a small number of participants shared a similar view

Where multiple views on an issue are presented, more prominent views are generally reported first. We use terms such as ‘consistent’, ‘commonly held’, or ‘less common’, to show the relative frequency of occurrence of views.

## Interpreting and extrapolating findings

Public dialogues are a well-respected, robust approach for engaging the public with complex policy issues in a meaningful and informed way. As with any research method, it is important to consider what the approach means for interpreting or extrapolating findings.

- People interested in a topic are more likely to sign up and attend. While our recruitment process was designed to reduce potential bias, participants may have been more interested in questions around the ethical use of location data than the general public. See Appendix A for more detail on recruitment.
- This report is a snapshot in time, people’s views may change in the future.
- The dialogue was a qualitative exercise, which did not aim to be representative of the UK population. As such, findings (particularly graphs and quantitative data) are not intended to be statistically representative of the wider public in the sense that they are generalisable (for example, it is not possible to assert that because

---

<sup>6</sup> <https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/>

<sup>7</sup> <https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/>



50% of female participants in this dialogue held a certain view, that 50% of the female population of the UK holds that view).

- The purpose of deliberation is to work with a group of the public to explore their deeper views on a topic. The sample size is based on an appropriate number of people to ensure a diversity of views and theoretical saturation – even if more people were involved, no new findings would emerge.
- We took the criteria outlined by Whittemore, Chase, and Mandle<sup>8</sup> to ensure the reliability and validity of these findings, and ensured:
  - **credibility** – through involving participants in feeding back on our thematic analysis, and involving workshop facilitators and observers in the reporting, analysis, and review of the findings);
  - **authenticity** – through ensuring a diverse mix of participants, and running further groups with people who may hold different views due to their life experiences;
  - **criticality** – all stages of the project have been scrutinised by an independent Oversight Group (Appendix D); and
  - **integrity** – the delivery team was made up of a collaboration, ensuring challenge and breadth of ideas, they regularly reviewed and challenged their findings and processes in addition to overarching project governance.

As such we are confident in the robustness and reliability of these findings, and their appropriateness to inform future guidance and policy.

## Finding your way around



**Quotes** are used throughout the report to illustrate points, not replace narrative. When using participants' own text, these are provided verbatim, without changes to spelling or grammar.



**Take-away messages** are highlighted at the end of sections in pink blocks like these. These present the analysis team's interpretation of the key take-aways from the data of each theme.



<sup>8</sup> Whittemore, Chase, Mandle (2001) 'Validity in Qualitative Research' *Qualitative Health Research*, Vol 11, Issue 4 <https://journals.sagepub.com/doi/10.1177/104973201129119299>

## Summary

**Summaries** are presented at the start of each findings chapter, in purple-outlined blocks such as this.



## Spotlights

Spotlights are featured throughout the report in blocks such as this. These give more detailed insights on cross-cutting themes.

- Spotlight: Public good, page 28
- Spotlight: Specifically impacted groups, page 37
- Spotlight: Digital resignation, page 60

## 2. Background and framing



### Summary

This chapter explores key definitions and baseline participant awareness and understanding to contextualise the findings that follow.

The chapter explains the rationale behind the definition of location data that was used through the dialogue: Location data is any data or information that can describe the position of an object or person in relation to the Earth or some other object or person.

It also synthesises findings from existing dialogues and research on public attitudes towards data. It describes how a limited body of research suggests public comfort with sharing location data is low, but more research is needed.

This chapter goes on to summarise a much broader array of research about attitudes towards data more broadly. Existing research suggests that many people identify both benefits and concerns of data sharing and use, and consider fairness, trustworthiness, and responsible data use to be important factors, among others.

### Defining location data

Location data is a complex topic, with technical and practical nuances in its related concepts and language. To enable participants to engage with the topic, it was important to find an accessible and plain-English definition of location data that dialogue participants could understand and explore together.

As part of the background research prior to conducting the dialogue, we looked at a range of definitions of location (and geospatial) data, including those from the Geospatial Commission, the UK's Information Commissioner's Office, an academic publisher and commercial organisations.<sup>9,10</sup>

Drawing from these definitions, we developed the following definition of location data to present to the dialogue participants:

**Location data is any data or information that can describe the position of an object or person in relation to the Earth or some other object or person.**

<sup>9</sup> ICO definition: <https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/>; IGI definition: <https://www.igi-global.com/dictionary/location-data/42216>; Arm definition: <https://www.arm.com/glossary/location-data#:~:text=Location%20data%20is%20information%20about,such%20as%20a%20mapping%20application>

<sup>10</sup> Geospatial Commission definition of location data: <https://www.gov.uk/government/publications/unlocking-the-power-of-locationthe-uks-geospatial-strategy/unlocking-the-power-of-locationthe-uks-geospatial-strategy-2020-to-2025>

This definition is purposely concise and broad. It was used in the dialogue as a starting point for discussion, and was explored through examples, case studies and other resources.

Location data encompasses data about people and data about objects and places. These different types of data are accompanied by varying ethical considerations.

## Existing research on public attitudes towards location data

We synthesised findings from existing research on public attitudes towards location data, as well as towards data more broadly. We did this to ensure the dialogue design was informed, rigorous, and built upon existing knowledge.

Through this synthesis, we found that **there is limited research concerned with public attitudes to location data specifically**, in comparison to research on public attitudes towards data more generally. Of the research focused specifically on location data, we found that comfort around sharing personal location data is low, according to a [small survey of 700 UK adults in 2020](#).<sup>11</sup> This has been [similarly reported](#) in other countries, such as the US and Germany, where consumers do not fully trust organisations to handle location data responsibly.<sup>12</sup> This survey also reported that there is less comfort with utilities and private companies using location data, compared to the public sector or civil society. A [2020 study](#) by the Centre for Data Ethics and Innovation (CDEI) and Ipsos MORI found that few people see the value of location data being used for targeted advertising.<sup>13</sup>

**Levels of comfort in sharing location data have [remained low during the COVID-19 pandemic](#)** in the US, UK, Germany, Spain, Australia, and Singapore. This is despite people recognising the role location data plays in addressing the pandemic and being more comfortable sharing some other types of data about people to inform public health response.<sup>14</sup>

Despite this relatively small body of research in relation to public attitudes towards location data specifically, there is a much larger body of research on the topic of

---

<sup>11</sup> Grünewald, P. and Reisch, T. (2020) 'The trust gap: Social perceptions of privacy data for energy services in the United Kingdom', *Energy Research & Social Science*, 68, p. 101534. doi: [10.1016/j.erss.2020.101534](https://doi.org/10.1016/j.erss.2020.101534).

<sup>12</sup> HERE Technologies (2018) *Privacy and Location Data Global Consumer Study*. Available at: <https://www.here.com/sites/g/files/odxslz166/files/2019-02/HERE%20Technologies%20Privacy%20and%20Location%20Data%20Global%20Consumer%20Study%20March%202018%20-%20Reviewed.pdf> (Accessed: 17 March 2021).

<sup>13</sup> Centre for Data Ethics and Innovation and Ipsos MORI (2020) *Public Attitudes Towards Online Targeting*. Available at: <https://www.ipsos.com/sites/default/files/ct/publication/documents/2020-02/attitudes-to-online-targeting-full-report.pdf> (Accessed: 17 March 2021).

<sup>14</sup> Elliot, D. J. et al. (2020) *Data-Sharing in the Time of Coronavirus*, Oliver Wyman Forum. Available at: <https://www.oliverwymanforum.com/future-of-data/2020/apr/data-sharing-in-the-time-of-coronavirus.html> (Accessed: 17 March 2021).

public attitudes towards data more broadly, and on other types of data, such as health data.

This broader research shows that **many people support the use of data for public good, such as improving public services.**<sup>15,16,17</sup> [Multiple research studies](#) also highlight that most people support the use of data about people for health care and medical research.<sup>18,19</sup>

However, a [2021 public dialogue](#) found that **there is not one fixed definition for 'public benefit'**, and those using data must carefully reflect on how they define public benefit and continually assess whether their use of data achieves this.<sup>20, 21</sup> Studies also show that where data is collected in public settings and used for public good, **people place an emphasis on the value of fairness and trust.** This is partly because [many people](#) consider the public to be a key stakeholder in data collected by public institutions such as the NHS.<sup>22</sup> This is reflected in media and public controversy about the sharing and use of NHS data, for example through the [partnership between DeepMind and the Royal Free Hospital](#).<sup>23</sup>

**How trustworthy an organisation is perceived to affect how comfortable people feel sharing data with them.** A [2014 study by Ipsos MORI](#) for the Royal Statistical Society found a 'data trust deficit' in the UK, where the NHS and public institutions are the among the most trusted when it comes to data use, but social media companies, technology companies and retail companies are the least trusted. National and

---

<sup>15</sup> Open Data Institute (2018) 'ODI survey reveals British consumer attitudes to sharing personal data'. Available at: <https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/> (Accessed: 4 March 2021).

<sup>16</sup> Cameron, D., Pope, S. and Clemence, M. (2018) *Dialogue on data*. Ipsos MORI, Office for National Statistics and Economic and Social Research Council. Available at: <https://esrc.ukri.org/files/public-engagement/public-dialogues/dialogue-on-data-exploring-the-public-s-views-on-using-linked-administrative-data-for-research-purposes/> (Accessed: 4 March 2021).

<sup>17</sup> Waind, E. (2020) 'Trust, security and public interest: Striking the balance: A review of previous literature on public attitudes towards the sharing, linking and use of administrative data for research', *International Journal of Population Data Science*, 5(3). doi: [10.23889/ijpds.v5i3.1368](https://doi.org/10.23889/ijpds.v5i3.1368).

<sup>18</sup> Understanding Patient Data (2018) *Public attitudes to patient data use*. Available at: <https://understandingpatientdata.org.uk/sites/default/files/2020-10/Public%20attitudes%202010-2018.pdf> (Accessed: 4 March 2021).

<sup>19</sup> Ghafur, S. et al. (2020) 'Public perceptions on data sharing: key insights from the UK and the USA', *The Lancet Digital Health*, 2(9), pp. e444–e446. doi: [10.1016/S2589-7500\(20\)30161-8](https://doi.org/10.1016/S2589-7500(20)30161-8).

<sup>20</sup> Hopkins, H. et al. (2021) *Putting good into practice*. Hopkins Van Mil, Understanding Patient Data and the National Data Guardian. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/977737/PGiP\\_Report\\_FINAL\\_1304.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977737/PGiP_Report_FINAL_1304.pdf) (Accessed: 17 September 2021).

<sup>21</sup> Burall, S., Lansdell, S. and Prior, A. (2019) 'Greater London Authority/Royal Borough of Greenwich data trust pilot'. Involve and the Open Data Institute. Available at: <https://theodi.org/article/data-trusts-gla/> (Accessed: 4 March 2021).

<sup>22</sup> Ada Lovelace Institute and Understanding Patient Data (2020) *Foundations of Fairness*. Available at: <https://www.adalovelaceinstitute.org/news/accountability-transparency-participation-third-party-use-nhs-data/> (Accessed: 30 March 2021).

<sup>23</sup> BBC News (2021) DeepMind faces legal action over NHS data use <https://www.bbc.co.uk/news/technology-58761324> (accessed 7.10.21)

local government bodies fall somewhere in the middle.<sup>24</sup> Multiple studies have since reported similar findings.<sup>25, 26, 27</sup>

A 2020 [report by the Ada Lovelace Institute](#) drew on multiple public dialogues and concluded that public trust in data use is dependent on not just privacy and data protection, but on whether digital interventions are effective and whether the organisations involved were perceived to be trustworthy.<sup>28</sup> Similarly, a 2020 public dialogue on the use of data driven technology during the pandemic, led by Traverse and the Ada Lovelace Institute, found that **people desire greater transparency and accountability around data use**, and to be more empowered over how data affects the world around them.<sup>29</sup> These studies suggest greater awareness about and control over the collection and use of data is important for many people.

Over the past eighteen months, the COVID-19 pandemic and the role data has played in the response have influenced public attitudes. The Centre for Data Ethics and Innovation reports that **most people think that data-driven technologies can help tackle the pandemic, but that potential isn't always realised**.<sup>30</sup> Work by the Ada Lovelace Institute has shown that data-driven tools like contact-tracing and potential 'vaccine passports' have led to public concern around data use, privacy and the potential to unfairly discriminate against already marginalised groups in society.<sup>31, 32</sup> However, research on the impact of the COVID-19 pandemic on attitudes towards data requires further qualitative and quantitative research.

Overall, this **existing research shows that many people identify both benefits and concerns of data sharing and use, and consider fairness, trustworthiness, and responsible data use to be important factors**, among many others. We used these findings as starting points and topics around which the dialogue was structured, and drew on existing research as a foundation that enabled the dialogue to address gaps in understanding of public attitudes to location data.

---

<sup>24</sup> Ipsos MORI and the Royal Statistical Society (2014) *New research finds data trust deficit with lessons for policymakers*. <https://www.ipsos.com/ipsos-mori/en-uk/new-research-finds-data-trust-deficit-lessons-policymakers> (Accessed 7.10.21).

<sup>25</sup> Open Data Institute (2018) 'Who do we trust with personal data?'. Available at: <https://theodi.org/article/who-do-we-trust-with-personal-data-odi-commissioned-survey-reveals-most-and-least-trusted-sectors-across-europe/> (Accessed: 4 March 2021).

<sup>26</sup> Worledge, M. and Bamford, M. (2020) *ICO Trust and Confidence Report*. Harris Interactive and Information Commissioner's Office, p. 39.

<sup>27</sup> Miller, C., Kitcher, H., Perera, K., Abiola, A (2020) *People, Power and Technology: The 2020 Digital Attitudes Report*. London: doteveryone. Available at: [https://doteveryone.org.uk/wp-content/uploads/2020/05/PPT-2020\\_Soft-Copy.pdf](https://doteveryone.org.uk/wp-content/uploads/2020/05/PPT-2020_Soft-Copy.pdf) (Accessed: 4 March 2021).

<sup>28</sup> Ada Lovelace Institute (2020) *No green lights, no red lines*. Available at: <https://www.adalovelaceinstitute.org/report/COVID-19-no-green-lights-no-red-lines/> (Accessed: 4 March 2021).

<sup>29</sup> Ada Lovelace Institute and Traverse (2020) *Confidence in a crisis?* Available at: <https://www.adalovelaceinstitute.org/report/confidence-in-crisis-building-public-trust-contact-tracing-app/> (Accessed: 4 March 2021).

<sup>30</sup> Centre for Data Ethics and Innovation (2020) *Trust in technology: COVID-19*. Available at: <https://cdei.blog.gov.uk/wp-content/uploads/sites/236/2020/07/CDEI-Trust-in-Technology-Public-Attitudes-Survey-1.pdf> (Accessed: 4 March 2021).

<sup>31</sup> Ada Lovelace Institute (2020) *No green lights, no red lines*. (ibid)

<sup>32</sup> Ada Lovelace Institute (forthcoming) *The Data Divide*.



A limited body of research exists about public attitudes towards location data specifically. It suggests people's comfort with sharing location data is low.

There is a rich body of research on attitudes towards data more broadly.

This research suggests people identify both benefits and concerns around location data.

Many people are comfortable sharing data when benefits the public, but consider fairness and responsible data use important to feeling comfortable.

How trustworthy an organisation is affects how comfortable people feel about that organisation using data.



# 3. Findings: Awareness and understanding of location data



## Summary

This chapter explores participants' awareness and perceptions of location data use, and how they began to identify related benefits and risks. It outlines different ways that participants engaged with the topic, **such as using 'data' and 'location data' interchangeably and generally focussing discussion on data about people**. It also outlines differing attitudes to private and public sector data controllers, based on how participants reacted to location data use for commercial versus public benefit.

The majority of the chapter focuses on how participants considered the potential benefits and risks of location data use to them as individuals and to society.

**Overall benefits were most often framed as being for the wider public, while risks were focussed on individual concerns.** Learning more about more specific uses of location data from specialists helped to move participants' thinking beyond commonplace, everyday individual use to consider uses for society.

**Participants felt there were many benefits of location data to themselves and society, with the strongest consensus in relation to personal and public safety.** They felt that use of location data by emergency services in times of crisis, and in preventing and solving crime was of great benefit, and that barriers should be removed as much as possible for this to happen. However, they also identified risks, namely the potential for misuse or being wrongly accused of criminal behaviour.

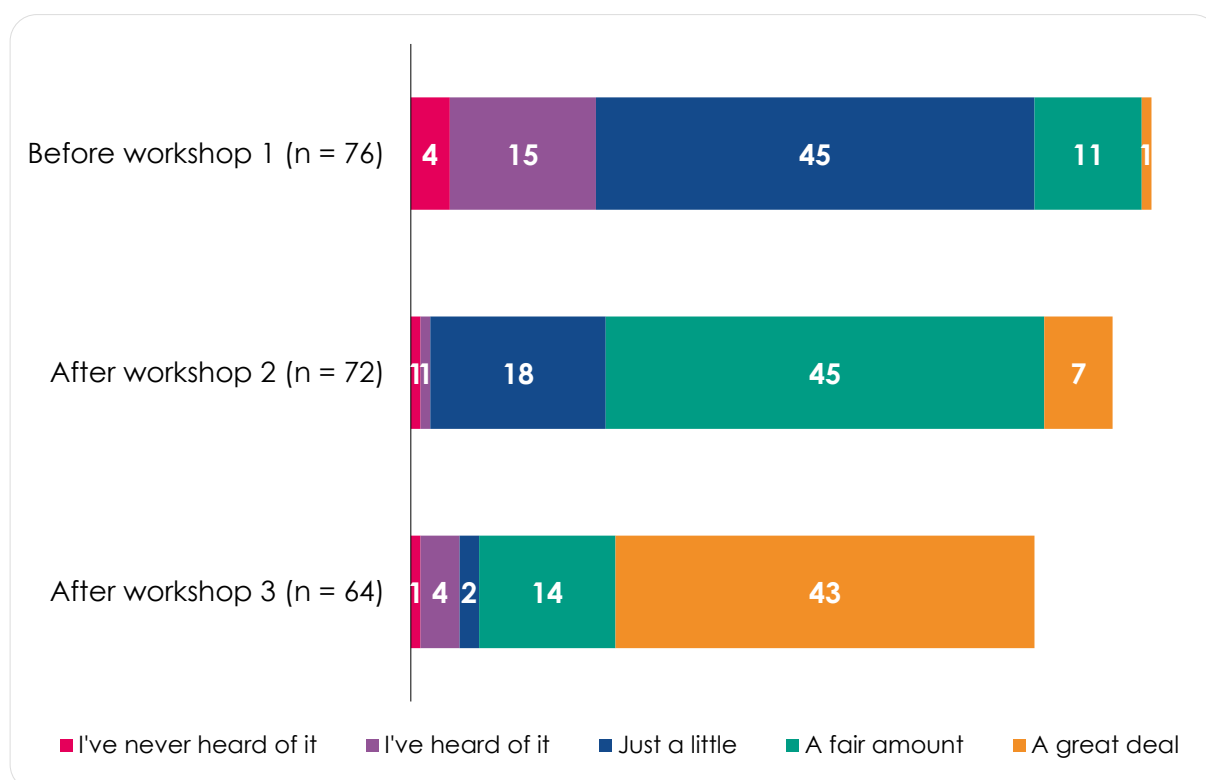
**Participants valued how location data could be used to improve public services, and also to make life more convenient.** They also considered health benefits and risks. The COVID-19 pandemic was a key discussion point, with the [NHS Test and Trace service](#) helping to frame arguments for, and against, the use of location data in managing health care. **Discussion of location data use to support improved environmental outcomes was less prevalent**, but where it was raised it was seen as an important opportunity to maximise.

In discussing benefits and risks, participants began to explore some of the ethical considerations and tensions around location data use, such as equity and privacy. **They discussed how the use of location data could redress or worsen existing inequities, and potential impacts on privacy as a result of personal or identifiable location data, such as risks to freedom or individual rights.** These considerations then formed the basis for wider ethical discussions which are explored in later chapters of the report.

## Awareness of location data

Before the first workshop, participants completed a baseline survey about their awareness of, and views on, location data and its uses. Similar questions were asked at different points throughout the dialogue journey, to understand any changes in views over time. Survey responses show that before the first workshop, most participants felt they knew nothing to just a little about location data (Figure 2). Following the third workshop, most participants felt they knew a fair amount to a great deal about location data.

**Figure 2: Participant responses to the survey question 'How much, if anything, do you feel you know about location data?' at different points in the dialogue.**



In the survey before workshop one, just over half of participants felt the use of location data was positive for society, growing to three quarters after workshop 3. Increasing levels of support for the technology in question through the course of an engagement programme is a common finding in deliberative processes. A third of respondents felt the use of location data was positive for them personally before workshop 1, growing to just over half after workshop 3 (Appendix F, Figures 11 and 12). This indicates that participants felt there were more benefits to society than there were to them as individuals.

## How participants connected with the topic

### Using 'data' and 'location data' interchangeably

Although the workshops focused on location data, participants often spoke about location data and other forms of data almost interchangeably. In the context of

activities designed to explore attitudes towards location data specifically, the tendency of participants to think about other forms of data suggests several things.

Firstly, it reflects how in their everyday life experience, the different types of data systems they may interact with do not prompt them to distinguish between data types. For example, a smartphone app may interact with a person's location, contact details, financial information and more to provide a service. As people interact with the service, and what it does for them, they tend not to consider the interlinked data the service uses, nor the role of each separate type of data.

The connection between data and location data in participants' views may have also reflected how participants engage with and hear about data in their everyday life. Public discourse, for example news articles about data breaches, does not always focus on specific types of data, and cookie notices and app data notices do not always refer to specific types of data, but to a user's data generally.

The manner in which participants used 'data' and 'location data' interchangeably indicates a key dialogue finding. When considering data about people, participants generally did not separate their views by data type – they saw location data as one part of a person's wider data set. This suggests that it is important to acknowledge people's wider experience of data when engaging with people about location data, or considering what constitutes ethical and trustworthy location data use.

### A focus on location data that is about people

Throughout the dialogue, participants were particularly interested in location data about people. While they sometimes referred to 'personal data', they were not using that term in the legal sense (as per GDPR), but rather through a lens of feeling that their location is something personal or private.

“I think location data is very personal. I think these could be valid for all types of data though. I want it all to be safe and with the right security and laws.”

Participants' focus on location data about people may have been influenced by the dialogue design. Early activities, such as the pre-task (see Appendix B for more information) or location data story (Appendix C, Figure 4), were designed to help participants connect with the topic of location data by focusing on examples of people sharing their location data.

However, reflecting on the entire dialogue journey, this focus appears to be due to participants being concerned about the risks to themselves (and others) as individuals – something that we see often in public dialogue processes. When workshop 4 participants were specifically prompted to consider the use of location data that is not about people (like physical maps, or the location of infrastructure), they were generally comfortable with its use. The key concern participants raised in relation to location data about objects and places was around data quality, including how systems sharing this kind of information are maintained and kept up to date. Some participants reflected on how inaccurate location data (for example, the location of a gas pipe, or the location of a pub) could affect businesses or house prices.

## Attitudes to public and private sector data controllers

Throughout the dialogue, participants discussed access to and uses of location data by different types of organisations. To support discussion, the dialogue broadly framed organisations as either **private or public entities**, however, it was clear that some organisations did not neatly fit into one of these groups.

When discussing private entities, participants cited examples such as large online retailers, technology companies, and high street retailers. They felt that uses of location data by these entities benefit individuals through providing a better experience of a product or service, and increased convenience. When discussing public entities, participants cited examples such as the NHS, police services, and local authorities. They felt that public sector uses of location data benefit society largely through improving public safety and public health. Participants often talked about central government separately to other public sector data controllers, and there was less consensus about whether their use of location data was for the public benefit – this was dependent on existing levels of trust in central government.

Participants by and large saw more individual and societal benefits from uses of location data by public sector organisations. This was often in relation to levels of trust in different organisations and institutions (See Appendix F, Figure 16), and their perception of how ethical their use of location data would be.

Table 2 shows what participants perceived the benefits of location data to be, and the level at which those benefits are realised (benefits for the individual, benefits for the data controller, and benefits for society at large) in relation to the type of data controller.

**Table 2: Overview of benefits of location data use by public and private sector organisations, as identified by participants**

		Who benefits and how		
		Individual	Data controller	Society
Data controllers	Private sector	<ul style="list-style-type: none"> <li>Location data use can improve user experience of a product or service</li> <li>Location data use in products and services can make people's lives more convenient</li> </ul>	<ul style="list-style-type: none"> <li>Location data use can improve services and increase efficiency, thereby increasing profits</li> </ul>	<ul style="list-style-type: none"> <li>Location data use can increase access to services for disadvantaged or vulnerable groups</li> </ul>
	Public sector	<ul style="list-style-type: none"> <li>Location data can be used in systems and services that keep individuals safe and healthy</li> </ul>	<ul style="list-style-type: none"> <li>Location data use to improve services and increase efficiency, potentially extending impact and saving money</li> </ul>	<ul style="list-style-type: none"> <li>Location data use in systems and services that keep the public safe and healthy</li> </ul>

There were two key distinctions that impacted participant views on private data controllers as opposed to public sector bodies. The first was in relation to profit, and the second in relation to transparency and accountability.

Most participants were concerned that, as private data controllers seek to maximise profit, they may prioritise their own interests over the interests of data subjects or society. They recognised the benefits of the services that for-profit data controllers provided, but voiced concerns about data markets and where their data could end up when it's being sold to third parties. A few participants felt frustrated that information about them was being commodified, and that businesses were making money in this way. This view was often driven by experiences of targeted advertising, which some participants found to be disconcerting and 'creepy', particularly when it wasn't obvious how they had consented to that company having their data. These concerns are discussed more fully in chapter 4.

These findings reflect those observed in other dialogues around data use, such as a 2020 citizen's jury on the use of NHS data which found that "public trust is undermined when a data access partner is seen to profit excessively from realising the potential from NHS data."<sup>33</sup> A 2018 public dialogue about the use of administrative data similarly found that people feel specific safeguards must exist to prevent businesses from unfairly extracting profit from the use of people's data.<sup>34</sup> These perspectives are also reflected in the trust deficit (described in chapter 2), whereby the organisations least trusted with data tend to be those with commercial interests.

Participants were also sensitive to a perceived power imbalance between data subjects and the power to use data. This was linked to feelings of disempowerment and a lack of control, which drove mistrust in data controllers, particularly private controllers. As a result, some participants did not trust that private data controllers would stick to the terms and conditions participants were agreeing to. Some participants were sceptical about the extent to which large private corporations could be held to account for the misuse of their data, which contributed to their sense of disempowerment.

Participants contrasted this with public sector data controllers. While they had some similar concerns about the lack of control over their data, they felt less strongly about this as they saw their data being used primarily to benefit data subjects or society. Furthermore, they felt there are more accountability structures for public sector data controllers (discussed more fully in chapter 6). In turn, participants felt more trust towards them, as shown in Appendix F, Figure 16.

---

<sup>33</sup> Hopkins Van Mil (2020) Foundations of fairness: views on uses of NHS patients' data and NHS operational data. Available at: <https://understandingpatientdata.org.uk/sites/default/files/2020-03/Foundations%20of%20Fairness%20-%20Full%20Research%20Report.pdf> (Accessed: 22 October 2021).

<sup>34</sup> Cameron, D., Pope, S. and Clemence, M. (2018) *Dialogue on data*. Ipsos MORI, Office for National Statistics, ESRC. Available at: <https://esrc.ukri.org/files/public-engagement/public-dialogues/dialogue-on-data-exploring-the-public-s-views-on-using-linked-administrative-data-for-research-purposes/> (Accessed: 4 March 2021).



Most participants felt that the use of location data by private and public sector organisations offered benefits to them as individuals as well as to society as a whole. On the whole, participants saw more societal benefits coming from public sector uses of location data as compared to private sector organisations.



## Spotlight: Public good

Throughout the dialogue, participants were asked to talk about the various uses of location data, and how these uses could result in benefits for themselves and wider society. This led to conversations about the different uses of location data that could be for the “public good”.

The dialogue did not propose a definition of public good, nor ask participants to explicitly define the concept, but facilitators encouraged participants to articulate and explore their understanding of it through suggesting examples. **They typically used the term “public good” to convey things that benefit society and communities.** Location data used within public services such as policing, health and care services, and public infrastructure (such as the design of roads and public transport services), were all seen as being for the public good.

Participants did not use the term “public good” exclusively, but drew on a range of language, including public benefit, wider good, for the benefit of society, and community benefit. Participants often used public good and public benefit interchangeably and spoke about location data **being used for the public good**, for example to help plan and improve infrastructure, rather than location data **as a public good** in and of itself.

**Participants articulated high levels of comfort around anonymous aggregate location data being used for public good.** Many discussions centred on the role of private companies in location data use, and participants expressed concern about the amount of profit a company may generate from using location data being disproportionate to the ‘amount’ of good or benefit to society from that use. However, they did not necessarily think that the existence of any profits negated societal benefits entirely. For example, profit making products and services that use location data like Google Maps and home deliveries were also described as providing benefits to the public.

The topic of public good – and associated concepts like societal benefit – commonly occur in public dialogues relating to uses of data. This has been explored widely in the context of health, including citizens’ juries on data use during the pandemic, and a recent public dialogue on what ‘public benefit’ looks

like when it comes to health data sharing and use.<sup>35, 36</sup> This growing body of work supports this dialogue's findings around proportionate use of data, and adds that this isn't just about profit, but about ensuring a balance between data subjects and data owners in terms of all kinds of benefits from data use. **Together, these findings suggest that data being used for the good of people and society is important for many people.** Further public engagement would be valuable to build a more nuanced understanding of how people understand location data in relation to public good.

## Exploring benefits and risks

The remainder of this chapter explores participants' perceptions of the benefits and risks of location data use under seven themes: **safety and security, public services, convenience, health, environment, equity, and privacy.** These seven themes elicited the most conversation and consensus throughout the dialogue. This was partly because of the information shared through the dialogue, but also reflects how participants connected with the topic, and what they returned to in their discussions. The first five themes are presented in order of prevalence across discussions, while the final two (equity and privacy) are not in any order. Instead, these two themes relate to ethical issues that were raised by participants in early discussions, and were then built on during the rest of the dialogue. Equity and privacy are discussed further throughout this report.

In workshop 1, participants gave initial examples of benefits and risks centred around their everyday lives, such as being called by the bank to verify transactions, targeted advertising, or using Google Maps or other apps to find the best routes to travel.

In the second workshop, participants attended break-out sessions to hear from specialists about different location data uses in more depth, spanning four topics (Appendix B, Figures 7-10).

- **Urban planning:** how location data facilitates sustainable urban development. This included how people can move through spaces more efficiently and safely, where best to build services, and how to make cities healthier places to live.
- **Health and wellbeing:** how location data is used to support patients to manage their health and enable health related research.
- **Retail:** types of location data used by shops (such as CCTV footage and census data), and how it is used to increase sales and inform business decisions.
- **Public safety:** how location data is used to help keep people safe in public spaces, such as geo-fencing (a virtual fence that monitors movement of mobile

---

<sup>35</sup> Ada Lovelace Institute (2020). *Confidence in a Crisis?*  
<https://www.adalovelaceinstitute.org/report/confidence-in-crisis-building-public-trust-contact-tracing-app/>

<sup>36</sup> Understanding Patient Data, the National Data Guardian and Hopkins Van Mil (2021). *Putting Good into Practice.*



devices in and out of a particular location for various reasons, as used by United States law enforcement).

Through learning about these topics, participants became increasingly aware of the potential benefits and risks to themselves as data subjects, and the benefits to society, which helped stimulate further discussion and reflection. A majority of participants expressed surprise at the breadth of location data uses and how it fed into so many aspects of their lives. A key takeaway for participants was how location data is used to make existing services more efficient and convenient, and to help with future planning.

During these discussions, participants grappled with the question, “what counts as a benefit?” when considering both public and private sector organisations. They highlighted that “benefits” for a large retailer may be at odds with, or be different from, what benefits society at large, but that there are also “win-win” situations, where these benefits are more aligned.

Overall, participants mostly articulated benefits through a lens of public services and society (such as emergency responses and equity) rather than benefits to data subjects, while concerns were often rooted in perceived risks to individual data subjects (such as privacy).

## Safety and security

Most participants felt the use of location data had obvious and important benefits for personal safety and security, identifying a wide variety of interconnected benefits for individuals and society. Participants generally focussed on community-level safety, with very few mentioning national safety and security. Participants also raised safety and security risks but most often referring to data breaches and misuse. This is explored in more detail in chapter 4.

Most participants felt that location data might help keep themselves or loved ones safe in an emergency, giving examples such as finding missing persons, medical emergencies, and crime prevention. The majority of participants were therefore supportive of organisations (like emergency services) using location data in such crisis moments, some welcoming the idea of having this access themselves, to monitor children, or vulnerable or older relatives.

“I quite like that one...a safe way for the children to go out and have a level of independence and go out. When my children were that age, we didn't have that and just wondered where they were.”

Participants often explored issues of privacy and consent in connection with the opportunities of location data use for safety and security. In terms of individually identifiable location data, the majority of participants were most comfortable with it being used for public and individual safety, with some willing to forgo consent in emergency situations. Consent is discussed in greater depth in chapter 6.

“Emergency services should be the only ones that don't need permission.”

However, participants in the focus group for women who have experienced abuse highlighted risks to their personal safety regarding the use of location data for emergencies and crime prevention. They shared how the perpetrator of abuse might be able to track their location, and that this real risk and associated fear was a key reason for privacy protecting behaviours, such as keeping location data switched off. These participants, and those in the focus group for forced migrants and refugees, raised further concerns about police having such open access to their data, highlighting that trust in the police is not universal, and that some groups would feel uncomfortable with the idea of their location being tracked by emergency services without their consent (see the Spotlight on page 34 for further detail on these views). These concerns were echoed by some participants in the main dialogue, who were concerned about data of children and vulnerable people being accessed by those without authority or with malicious intent, and also the privacy connotations of preventative surveillance.

“[Location data] can be used for the good but can be used for the bad too. [It leads to] more intrusion and more tracking by default.”

Overall, participants recognised that while there was a majority of support for the use of location data relating to security and safety issues, the risks and concerns raised posed significant ethical issues, especially in relation to equity. These issues were then explored more thoroughly by participants and are discussed more fully in the section on equity below, and in chapter 4.

## Public services and transport

Participants spoke about public services and transport regularly throughout the dialogue, with a particular focus on both public and private travel, infrastructure planning and improvement. This was mostly prompted by the location data story (Appendix C, Figure 4) and later by the specialist deep-dive on urban planning (Appendix C, Figure 7).

Most participants saw the use of location data in transport to plan routes, monitor traffic, and find places as an essential individual benefit rather than a public benefit. They used examples such as personal navigation apps (like Google Maps) when driving and being able to plan public transport journeys using services from Transport for London. A few participants felt that these services might be particularly valuable for those with mobility issues, allowing them to plan accessible routes.

“My life is so busy, being stuck in traffic is my worst nightmare. I rely on the Waze app when I get in the car. If that wasn't available to me, it would ruin my day.”

Some participants saw the benefit to the wider public of sharing their location data whilst using transport services. They noted how this data could feed into infrastructure planning, improving transport services through monitoring crowd movements to plan new roads, train stations and pedestrian crossings.

“...adding crossing lights in a different location as it is going to benefit you and other people. Transport provision is public good, buses and trains on each route and how many people are on train at each time.”

When discussing how location data might help public transport operators plan for busy periods and assess capacity, a few participants questioned this benefit due to their negative experiences of public transport. A few participants expressed concern about what happens to their data after sharing it with these services, referring to privacy risks of data selling. Others conversely saw a risk in **not** sharing location data to feed into services and plan infrastructure, given the valuable insights it offers to enable improvements. Building on this, a few participants were concerned that data gaps might result in exclusionary infrastructure and services, and suggested that organisations must not solely rely on location data for decision-making.

Overall, most participants felt the benefits of their location data being used for transport and infrastructure planning outweighed the risks. This was largely because they associated this use with non-identifiable, aggregate data, and therefore felt there were limited risks to themselves as an individual.

“I see a lot of the positives...I'm quite trusting with my data. I feel people are not interested in what I'm doing myself. More looking as a group.”

**Most participants supported the use of location data for public services and infrastructure, and particularly for both private and public transport planning. They liked how location data allowed them to plan travel and navigate, seeing this as a vital individual benefit. They felt that sharing location data with transport services benefits the wider public through enabling planning and improvements. However, they were concerned that data gaps might result in exclusionary infrastructure and felt that organisations must not rely on location data alone.**

## Convenience

Most participants appreciated how location data helped them do everyday tasks more efficiently, like finding the quickest route, tracking deliveries, and online shopping. They saw this as one of the key benefits to them as individuals in the sharing and use of their location data.

“Home deliveries are a must have, rather than running around different places. I don't get home deliveries for groceries but Amazon etc. Even for essentials it's important.”

However, participants did not necessarily consider convenience as relating to wider societal benefits (for example, through thinking of it as efficiency, or considering the

examples of 20-minute cities<sup>37</sup> and crowd control discussed in the urban planning deep dive). This might be in part because of the familiarity of individual services such as Google Maps compared with more theoretical ideas associated with urban planning. As such, they didn't feel this benefit of individual convenience to be essential, or as valuable as some of the other more pro-social benefits they identified.

The risks around increased convenience through the use of location data was often discussed through the subject of targeted advertising. Participants held polarised views on this. While most participants complained about it, finding it annoying, or intrusive, some identified advantages, such as how targeted advertising could help when looking for things in a new area.

“I think ads are cheaper and it saves you from searching the internet. Just a bonus – makes it easier and more convenient for you if they are doing the leg work.”

Most of the examples that participants shared relating to increased convenience due to the use of location data were based on profit-driven data services (such as Google Maps or Amazon collecting location data to improve their service delivery). As such, participants expressed a tension between wanting these benefits but feeling negative about sharing location data with the relevant organisations due to a perception of those organisations prioritising profit over risks to the data subjects. This led to feelings of insecurity and distrust explored more in [chapter 4](#).

Furthermore, participants also spoke about the risks of increased convenience in relation to technological ubiquity and data use in general. Typically, they spoke about this in a negative way, sharing concerns about being over-reliant on such services, and feeling resigned to having to use them, as not doing so would disadvantage or marginalise them. This is discussed in more detail in chapter 6.

**Convenience was one of the most easily identifiable benefits for participants. However, they identified a range of associated tensions, and felt negative about the potential impacts of increased use of location data in this way, particularly as a result of sharing location data with profit-driven data collectors.**

## Health

Participants spoke more about public health benefits of location data than individual benefits. This could reflect the focus on health in workshop activities such as the deep dives (Appendix C, Figure 8), but it could also reflect participants' recent experiences of location data collection during the COVID-19 pandemic. They most often referred to health benefits through the lens of emergency response (as discussed in safety and security) and in relation to the NHS Test and Trace service.

<sup>37</sup> <https://www.tcpa.org.uk/the-20-minute-neighbourhood>

“It is not bad as it is about improvements, help, support, more about the country and to push things going forward in the positive way. For example, if they want to collect data for the Covid cases they will use some people and will understand more from that.”

Participants used the NHS Test and Trace service as an example of location data use that involved clear societal benefits for the containment of COVID-19. This was partly due to specialist examples and partly due to the COVID-19 pandemic. It is possible that this was an example participants could easily relate to because of regularly interacting with it, such as using the app to monitor exposure to the virus or ‘check in’ to venues. With media attention surrounding the NHS Test and Trace service, a few participants mentioned stories of data selling, which left them wondering about who else might have their data and for what purpose.

In workshop 2, some examples of location data use, such as a fitness app connected to an insurance rewards programme in the location data story (Appendix C, Figure 4), prompted participants to think about individual health benefits. In a deep dive session (Appendix C, Figure 8), a specialist explained how health insurance companies could make inaccurate inferences based on where people live. These differing perspectives prompted a few participants to explore potential trade-offs of sharing location data with private sector health apps. Some participants felt the potential to lower insurance premiums through increased activity might be a good way to incentivise people to be healthy. Others were concerned that it could penalise people unfairly through inaccurate inferences based on their level of movement.

“...it does incentivise because some people do need to be incentivised. Paying in terms of your health in the future but it should be made clear that you’re opting in. It should be a question do you consent for this to be shared.”

This led participants to consider the equitable and fair use of location data and the potentially unfair treatment towards different individuals and groups as discussed further in the section on Equity on the following page. On the whole, in terms of the use of location data to realise health benefits, participants were supportive of the use of location data for public health services, but had more mixed views in relation to individual health services.

**Participants were keenly aware of how location data was being used for public benefit through the NHS Test and Trace service, and had limited concerns about health risks from location data use. They generally supported location data use for public health, but had mixed views in relation to individual health services.**

## Environment

A few participants discussed the use of location data for environmental outcomes, but this did not regularly come up in discussion. This may have been because there were fewer examples and prompts provided. Where it was discussed, participants only spoke about opportunities for using location data to tackle environmental issues and that it was important that these were realised. After the deep dive on urban planning, a few participants could see environmental benefits associated with 20-minute cities<sup>38</sup>, for example reducing car use thereby reducing carbon emissions. It is likely participants did not associate any risks with environmental outcomes as they understood uses to involve non-identifiable aggregate data or the location of objects or issues like pollution hotspots.

“20-minute cities are a great idea...We're in a climate emergency and we have to rethink our cities. We can't be reliant on cars...and if you do need to travel you need to have better transport options.”

Those participants that raised environmental benefits, saw them as public benefits rather than individual and articulated them through the lens of future planning and development, such as monitoring emissions to develop transport infrastructure.

“If they can gather info about specific postcodes...The positive is the environment, an area which was polluted, they can use that to get rid of buses, for emissions and put a train track.”

**Although not a common topic, participants felt that the use of location data for tackling environmental issues was very important and saw this as a public benefit. They did not feel that this use posed any risks to themselves. This is likely because they associated it with non-identifiable aggregate data or location of objects or issues.**

## Equity

Participants did not typically use the language of equity. Nevertheless, they often spoke about the potential for location data to address social issues in which they saw some people as being disadvantaged, focussing on how location data use might impact people in specific vulnerable situations. Some raised these opportunities and considerations without prompting, but most often participants' views on equity were in response to prompts or materials, such as the personas (Appendix C, Figure 6).

<sup>38</sup> <https://www.tcpa.org.uk/the-20-minute-neighbourhood>

Some participants were concerned that the risks around location data use may have a greater impact on people in vulnerable situations and were more cautious about how it might be used to support people in these circumstances. Others identified how it could improve some people's lives and were keen to maximise such opportunities for people in vulnerable situations. For example, they cited 20-minute cities<sup>39</sup> from a deep dive (Appendix C, Figure 7) as a great idea for older and vulnerable people to prevent isolation and ensure access to amenities.

“In terms of age and demographic you want more facilities nearer to elderly people for instance. 20-minute cities are a great idea.”

Some participants noted benefits for one of the personas (Vinny – a digitally excluded older man with health concerns; Appendix C, Figure 6), such as increased safety through people knowing where he is and being able to find accessible travel routes.

“With his health and being diabetic, if he was hypo[glycemic] and needed help, how would he get the help? I can see the benefits for someone like this with location data, I feel like he is quite restricted to moving about in his local community, so I feel he would really benefit. For example, with a journey planner, buses, and trains. Someone like him could really benefit from that.”

Most participants wanted location data to be used in a way that supports social equity, although some raised concerns as to whether this could be realised – and that the use of location data could create further inequity. For example, some participants were concerned small businesses could not afford to use location data, giving larger businesses an unfair advantage. A few felt that this was particularly negative for local economies. However, others felt that location data such as high street footfall could support recovery from the impacts of the pandemic. Others noted that data may be too sparse in rural areas, leading to disparity in benefits between rural and urban populations. A few participants worried that data collectors may not do enough to examine data gaps and that some groups, such as older people, might not be considered in decision-making.

Overall, most participants agreed that the use of location data could contribute to unfair treatment of individuals or different societal groups. They felt data controllers have a responsibility to ensure equity and fairness, and most were generally confident that this was happening in the public sector.

<sup>39</sup> <https://www.tcpa.org.uk/the-20-minute-neighbourhood>





Participants had mixed views about the potential impact of location data use on different people. They felt that location data offered opportunities to improve equity and support people in vulnerable situations, but remained concerned about risks to these people if location data was misused. Participants would like data collectors to ensure that their location data use does not worsen inequity, and consider potential data gaps when making decisions.



## Spotlight: Specifically impacted groups

We hosted three focus groups – one each with women who have experienced abuse, forced migrants, and Disabled people – at two points in the dialogue. Through the focus groups, we set out to understand participants' views on location data, and how aspects of their identity and experience influence these views. These focus groups were designed to enable participants to share their perspectives and experiences, and to feed into the development of personas to be used in the main dialogue.

By and large, focus group participants echoed the same sentiments, priorities, and concerns as in the main dialogue workshops. For the most part, focus group participants felt that the aspect of their identity and experience that we were interested in (i.e., being a forced migrant, having experienced gender-based violence, or being disabled) was not a key factor in shaping their views on location data. However, they did offer some specific considerations they felt were connected to their identity and experiences, which we have summarised below. These findings highlight the need to consider how concerns and conditions for trust vary between groups and communities.

### Key takeaways from focus group with Disabled people

#### ■ Concerns about the implications of disproportionate digital exclusion.

- Participants were concerned digital exclusion among Disabled people could mean that they would be excluded from potential benefits of data sharing (for example they would not be able to access services that require you to share location data or to have a smartphone), or that their experience would not be reflected in the systems that use location data (such as in planning and transport).

#### ■ Concerns that the government might be able to track their movements.

- This was due to being worried about systems making biased or incorrect inferences about their degree of disability, and therefore their eligibility for different kinds of benefits, based on where they go (such as if they go to the gym). Participants felt this would be too invasive of people's privacy.

## Key takeaways from focus group with forced migrants

### ■ Concerns that accessing essential services often involved sharing location data.

- For example, participants highlighted that sharing your address is required to receive some NHS services. Participants felt that some refugees and asylum seekers would not be comfortable sharing their address due to concerns about their privacy and security, and fears around how that information may be used by the government to inform decisions around asylum and refugee status.

### ■ Concerns regarding digital exclusion and isolation.

- This was due to how the fears outlined above may limit forced migrants' use of smartphones and data, which may result in cutting themselves off from friends, family, and society. Participants felt this was compounded by other forms of digital exclusion faced by this group, including language barriers to accessing information, and financial barriers to accessing a device and/or mobile data.

### ■ Desire for clearer information.

- Participants called for clearer information about what data is collected from and about forced migrants and how it is used (specifically by government organisations), so that people can make informed decisions about the services they use and the data they share.

## Key takeaways from focus group with women who have experienced abuse

### ■ Location data and social media.

- Participants felt that the way location data is shared through social media was the most relevant to them as women with experience of gender-based violence. This was because of the risk of being tracked by abusive partners or ex-partners.
- On the other hand, participants also flagged that location data can be used by survivors to avoid abusers or other individuals if they actively share their location.

### ■ Concerns about digital exclusion and data gaps.

- Participants raised concerns that privacy protecting behaviours could exclude the experiences of women from decision-making, and limit women's opportunities. Participants reflected on how it is harder to progress in your career if you don't share your location (for example on LinkedIn, or on your company's website).
- One participant noted that women opting out or keeping location data switched off for safety reasons can lead to women being excluded from data that informs decisions that affect them. Another participant stated that she never switched on her location due to fears about safety, and felt the trade-off (in terms of not having access to navigation maps) was worth it.

### ■ Concerns over data accuracy.

- Participants were concerned about the accuracy and precision of location data used by decision-makers, including the police. For example, if someone was assaulted on a train, their phone might say they were in a different carriage, which could hamper the investigation.

The focus groups with people from three specifically impacted groups highlight the need to actively consider and explore the concerns of different groups, to understand unintended consequences around the ways location data is collected and used. Groups for whom maintaining their privacy and personal safety is a key concern should be prioritised. As explored through this report, organisations being upfront and transparent about why they collect location data, and giving people more granular control over which of their data is collected, and how it is used and shared, can support greater trust.

## Privacy

Most participants expressed concern at some point in the dialogue about privacy, largely due to a perceived or experienced lack of clarity around the collection and ultimate use of their location data. They often raised concerns about how it might be used to identify individuals or be sold on to third parties for other uses without their consent. Participants generally felt that sharing their location data (particularly where an individual and their location can be identified) risked their privacy, and that as long as the data is identifiable, it would be hard to mitigate such risk.

Participants generally questioned why data collectors would need very specific location data (identifying a specific individual in a particular place), and felt more comfortable with the use of aggregate data. In considering the tensions between privacy and location data use, there were few circumstances in which participants were willing to forgo privacy, such as when emergency services need to know the whereabouts of a specific person.

“...it's easier to get behind this aggregate data because while it's probably for profit, it also does improve your experience without putting your personal data at risk. I think it's easier to get behind...I think it's something you can trust as opposed to seeing where one individual person is going. It's very different I feel.”

A few participants were also concerned that the collection and use of identifiable location data risked societal freedom and encroached on individual rights. For these few participants surveillance and the concept of 'big brother' was a concern, as they felt they were being watched and monitored in their daily lives.

Issues around privacy are explored in more depth in chapters 4 and 6.

**Participants felt uncomfortable with the collection and use of identifiable location data, except where it is used for emergency response and fraud prevention. They shared concerns about potential risks to privacy, freedom, and individual rights.**

## Exploring ethical issues

As outlined above, through these early discussions on benefits and risks, participants began to discuss some key ethical considerations, such as equity, privacy, and how to ensure the trusted and fair use of location data. As participants discussed these issues together in detail, they commented on the complex and inter-dependent nature of the questions surrounding the ethical use of location data.

Participants rarely used the language of ethics themselves, with many finding the term “ethics” to be vague and unhelpful. However, their focus on these topics emerged naturally and we used these emergent views to shape the themes for further discussion and to explore these conceptual issues in the remainder of the dialogue. Rather than using the language of ethical and unethical, participants often returned to the language of trustworthiness. Discussions around trustworthiness were often rooted in what participants considered to be good or ethical practice; therefore, their perception of ethical issues generally mirrored their recommendations for trustworthiness.

While they could connect with the individual use cases that were presented and discussed within the dialogue they often found moving from these discussions to broader, ethical considerations challenging. Public dialogue participants often find grappling with conceptual, societal issues difficult, but the inter-dependent nature of location data, and the perceived remoteness of some of the questions to eventual impacts on their lives perhaps made it more challenging for this topic.

Participants could most easily articulate their views, and potential recommendations, on subjects such as data security and privacy, as they could draw on tangible examples that they felt related to both them and wider society (see Chapter 4 for more detail). Participants found it more challenging to weigh up possible future benefits to wider society (such as more efficient urban planning) and consider ethical practice within such settings.

The following chapters provide a full exploration of the ethical issues discussed, culminating in a vision for ethical and trustworthy location data use in Chapter 7.

## 4. Findings: Data insecurity



### Summary

Data security was of great importance to most participants; however, they rarely spoke about data protection or data security measures in practical terms.

**Although most participants regularly spoke about data security and safety, this language was often used to convey feelings of insecurity, risk, or concern around how their data is being used and by whom.** Participants often spoke about their need to feel secure in how their data is used, and its potential ramifications, rather than making specific demands about data security practices.

Across participants' discussions, **concerns about the security of their data were tied to a sense of powerlessness and detachment from their data.** Participants' views were driven by frustrations about all forms of data collection, in addition to specific thoughts about location data. Those that collect the data hold all the power; data controllers determine what people's data is going to be used for, and how it is going to be used. Most participants expressed distrust of those with that power and want to regain control over their data about people. To most participants, personal control is fundamental to feeling secure. This was true both for location data and other forms of data. **This chapter explores participants' feelings of disempowerment and how feeling disempowered can lead to feeling less secure.** For a deeper exploration of the type of control participants envisioned, and the trade-off between more control and more burden on users, see chapter 6.

This chapter starts by examining participants' thoughts on how location data is collected and where the data goes from there. This chapter then examines participants' thoughts on the risks associated with their location data after the point of collection, which includes their thoughts on what could go wrong and what the consequences of data (mis)use could be.

The chapter then examines participants' feelings towards the different groups that have the power to use (or misuse) their data. In this section, we explore how **participants focused primarily on security concerns associated with the criminal misuse of data and data controllers' capacities for preventing this.** This section captures participants' additional reflections on data security in relation to private companies, policymakers, other public sector bodies, and foreign governments. The chapter ends by examining participants' thoughts about data protection methods and the inevitability of data breaches.

## Rationale for data collection

For most participants, there was a clear link between their feelings of security, and the clarity they felt around the rationale for the collection of their location data, and their ability to understand and consent to its use. Most participants expressed resignation about all forms of data collection, feeling that sharing data was an unavoidable part of the modern world. Although some participants recognised that they might give consent for the use and sale of their data when signing up for products or services, the ubiquity of technologies that demand access to their data, including location data, left some participants feeling that they had no choice but to sign up. This is discussed in more detail in chapter 6. Moreover, participants felt that the information about what they were signing up to was vague, which added to their sense of powerlessness. Most participants wanted more clarity about and control over who would use their data and for what purpose.

A few participants also expressed a general feeling that the interests of businesses were prioritised over their interests. Some participants referred to examples of technology that asked for access to location data that the service offered did not require, such as games requesting access when it did not form part of the gameplay experience. This left some participants feeling that location data collection is more about profit than about improving their experience of the services they use. This also led some participants to question the power data controllers had and their intentions.

“Don’t abuse it and I don’t like the idea of it being sold on because I don’t know who its being sold on to. I don’t like it being stored without our knowledge or with our request.”

Some participants expressed concerns about whether companies were acting in good faith when gaining their consent, or whether companies could retroactively alter the agreed terms and conditions to gain more freedom over the use of their data. When changing the purpose of data use, the General Data Protection Regulation (GDPR) requires organisations to ask for consent, or the use of a different lawful basis for data processing. However, these participants were expressing a more general distrust towards for-profit data controllers, which meant that these participants did not trust that these data controllers would be using their data in the way that they had specified.

“If I’m giving something I want to know what It’s being used for. These facts can be cherry picked of course.”

Overall, most participants felt their data was less secure when companies were using it for profit. These more general attitudes about data informed their attitudes about location data too. In particular, their concern over the monetisation of location data came out strongly during an activity designed to broadly categorise participants’ hopes and fears. When the benefits of location data use are clearly described, and participants feel that they benefit from its use, participants generally feel both more trusting and more secure in consenting to their location data being gathered.



**Participants felt that they often don't have a choice about using services which collect their data. Participants felt that for-profit businesses might prioritise profit over security. This impacted their perception of the security of their data.**

## Is security possible?

### Data breaches

During workshop 2, participants were invited to share the main risks they perceived around the collection and use of location data. Most participants were very aware of the potential consequences of different kinds of data breaches. They were particularly concerned about being victims of crime, such as fraud, identity theft, scams, or break-ins.



"[...] people are calling vulnerable people and they don't know what they are accepting. Thousands of pounds going down the drain. Families suffering because they trust these people that have phoned them, because they know their name and number and address. These are risks that occur for safeguarding and vulnerable people going through situations."

For some, their awareness was derived from personal experience, whether of simply being notified of a data breach, or being a victim of this kind of criminal activity. Some participants also referred to examples of prominent data breaches they had learned about from news coverage. Both personal experience and media coverage of breaches of various forms of data led most participants to express feelings of insecurity towards location data collection.

A few participants noted that although location data was not necessarily required for these crimes, it could help criminals acquire or make use of more sensitive data about people. For example, a participant highlighted how location data was used to add legitimacy to a phishing phone call they received. In their example, the phisher used information about the location of recent bank transactions to appear genuine. However, participants also spoke about the value of banks monitoring location data to help prevent fraud.

### Resignation and inevitability

Participants' concerns about the security of their location data centred around the capacities of data controllers to adequately protect their data and the capacities of criminals seeking to access data, which participants tied together. Some participants expressed a sense of inevitability and fatalism around data breaches as they felt data controllers would always be reactively responding to new threats to their data and would have difficulty in anticipating and preventing advances in the techniques used by criminals. Most participants emphasised the persistence and sophistication of criminals and drew attention to what they perceived to be a technological arms race between criminals and data controllers.



“One of the things I want to emphasise is that it's so hard to keep up with the tech and security settings. It's a society where geeks run around as bandits, and pretty well organised bandits now.”

Data breaches, therefore, were ultimately an unavoidable part of modern life. For a few participants, this sense of inevitability was informed by knowledge of previous data breaches, such as the 2017 Equifax data breach<sup>40</sup>.

“A couple of years ago I got a letter from Equifax, you don't have a choice but to use them. They sent me a letter that my information had been stolen. This is not an isolated case, had 3 separate occasions where this has happened. That is the biggest problem... if you can hack a company like Equifax. If that can be hacked, smaller companies don't have a chance. If they can't protect it from being stolen, that is where the real risk is. I haven't seen anyway where anybody can protect data effectively.”

## Individual data protection


Across the workshop discussions, some participants talked about data protection methods and procedures. Overall, participants' knowledge of data protection varied considerably. Generally, participants with more knowledge and experience of data protection practices were less concerned about the security of data. Some participants talked about encryption and emphasised that they felt it was an important part of data protection which they trusted. A few participants spoke about potential technologies, such as block-chain technology, which they felt could be used in the future to protect location data.

While discussing the data protection practices which they felt increased data security, most participants emphasised their desire for companies to proactively encourage and enable people to have more control over the security of their data. Some participants drew on workplace experiences and suggested that companies should implement mandatory password changes after set time limits. A few participants expressed a desire for two-factor authentication to be more widely used. Some participants wanted more regular security updates from companies, and to be reminded about what they could do to keep their data secure.

“The more control you have, the more secure you feel. With Snap Maps<sup>41</sup>, knowing you can turn it off is reassuring. The same with selecting what photos that your apps have access to.”

<sup>40</sup> Equifax (2018) 'Cybersecurity incident - information for UK consumers'. Available at: <https://www.equifax.co.uk/incident.html> (Accessed: 21 September 2021)

<sup>41</sup> <https://support.snapchat.com/en-GB/a/snap-map-about>



**Participants were concerned about the outcomes of data misuse, particularly personal impacts of criminal misuse.**

**Participants expressed a sense of inevitability and fatalism about data breaches.**

**Participants felt that criminals would always be one step ahead of data controllers.**

**Participants want technology to facilitate taking data security into their own hands.**

## Data (mis)use and power


Most participants' feelings of security were informed by their perceptions of the data controller, and the perceived intentions of these actors. Participants felt less secure when unable to access information to assess those responsible for their data and how it would be used, such as when it is used by unnamed third parties. In addition, the misuse of data (whether intentionally or unintentionally) seemingly affected people's trust in data collectors, and therefore impacted their feelings of security regarding their own data being collected and used.

A few participants did not feel particularly worried about the use or misuse of location data compared to the other forms of data about people with, in their opinion, clearer potential for misuse, such as bank details. Some participants also felt unconcerned by the use of aggregate anonymous data as, to these participants, it ensured anonymity and privacy which alleviated their security concerns. Nevertheless, most participants expressed some concern about the misuse of location data in some way.

## Data commodification

Most participants were frustrated by legal uses of data that they felt still had a negative effect on their lives. Some participants frequently expressed concerns about the intentions of companies that use their data for profit, particularly those whose business models centre around selling data. This reflected participants' more general reservations about the wider move towards the commodification of their data, and the development of data markets. Most participants talked about nuisance advertising, which they linked to the sale of their data to third parties, and the possibility of their data being sold to, and used by, companies in countries with less rigorous data protection laws.

Most participants were very aware of the role that data about people has in advertising. It is unsurprising that most participants often drew on advertising as an example, as it is commonplace and designed to grab peoples' attention. Therefore, although participants have probably given consent for advertisers to use their data at some point, these day-to-day negative experiences of data uses were still important drivers of participants' attitudes to location data.



"I don't like adverts that are constantly tagging me, trying to sell me stuff. If I wanted a particular object, I would search that, or find a restaurant that I want to eat at. I don't like being hounded by constant adverts."

Some participants expressed additional concerns about where their data might end up after being sold, and which third parties might have access to. In line with this, a few participants noted feeling that it was “creepy” when a company they had not interacted with before already had access to personal information about them. Even if this information was accessed legitimately from a secure database, it left these participants feeling insecure. One participant expressed this as a “distrust of the unknown” – there was a sense that, after collection, their data enters a mysterious, hidden realm where participants hold no power over the journey their data takes. Participants’ sense of risk and their feeling of insecurity about their data increased as their sense of control over its destiny decreased.

Overall, participants felt detached from their data and concerned about the journey it goes on. Their demands for more control over its use point to a desire to retain some form of ownership over their data after the point of collection, and after its commodification. A lack of control over the intended use of data, and distrust of organisations that seek to use data solely for profit, led to most participants feeling insecure. In addition, providing more detailed, transparent information about the journey their data will take could help to alleviate participants’ distrust.

## Data in the public sector

Some participants were also concerned about how government and other public sector bodies use location data. In workshop 2, a specialist talked to participants about an example where an artist had walked down an empty street with multiple mobile phones to trick Google Maps into displaying high traffic in the area<sup>42</sup>. While this was an unusual example of data misuse, it served to stimulate a discussion and raise concerns among participants about the extent to which location data can be unquestioningly relied upon, and the potential consequences of that data being flawed or incomplete.

For some participants, this example raised concerns about the reliability of location data and the extent to which policymakers may rely on location data to make decisions. Participants also used this example to highlight potential risks of incorporating location data technologies into local or national infrastructure; for example, a few participants were concerned that emergency service vehicles could be mis-directed, which highlighted safety and security concerns.

---

<sup>42</sup> The Guardian (2020) ‘Berlin artist uses 99 phones to trick Google into traffic jam alert’. Available at: <https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert> (Accessed: 21 September 2021)

A few participants also talked about the potential for human rights violations associated with police using location data technologies. A few participants were concerned about being accidentally associated with criminal behaviour through location data, and the resulting difficulties they might experience in challenging the accuracy of location data to prove their innocence. Some participants noted that invasive surveillance made them feel insecure, while recognising the potential security benefits from police being able to locate criminals more easily. In the second workshop, a specialist talked about the steps police go through to access data about people, which alleviated some concerns. These participants were surprised by the steps taken to limit the police's access to data about people and felt reassured by the overall data protection process.

“I am comfortable with police using location data, if they're investigating something bad that happened then I would be happy to assist in bringing about justice. I agree with [participant] that if it's anonymous and they just want to know how many passing through station that's fine. When more personalised apart from usages where it's about safety and they have powers, I would be comfortable sharing that. But otherwise, you should have a choice.”

Although uncommon, a few participants highlighted concerns about international use, such as data being used for espionage, to undermine the government, or generally manipulate people's attitudes. A few participants used the example of the Cambridge Analytica scandal<sup>43</sup>, in which data was collected without consent by a company specialising in microtargeted political advertisements, as evidence for these concerns.

**Participants feel that the destiny of personal data is controlled by organisations, not by data subjects. Participants' sense of inequality and powerlessness in the use of the data contributed to feelings of insecurity.**

**Once collected, participants felt disconnected from their data and as though controlling its journey is then beyond their reach.**

**Participants indicated that enabling people to exercise more control around who is going to use and access data could help people to feel more secure.**

**Some participants were concerned about policymakers' overreliance on location data technology, which participants felt could be inaccurate or manipulated.**

<sup>43</sup> BBC (2020) 'Facebook sued over Cambridge Analytica data scandal'. Available at: <https://www.bbc.co.uk/news/technology-54722362> (Accessed: 21 September 2021)

## 5. Findings: Accountability, agency, and governance



### Summary

In this chapter, we explore the views shared throughout the dialogue journey around the governance of location data: how participants think and feel about accountability, regulation, and transparency. **Systems of accountability that empower citizens to hold data controllers to account were a requirement for building trust and feeling safe.** To participants, accountability and transparency were intrinsically linked: both empower participants, which in turn helps them to feel more trusting and more secure.

When participants were discussing what regulators could do to help participants feel safe and secure, a lot of their conversations centred around accountability. For most participants, this means that those in control of their data would have to answer to regulators and citizens for data breaches or misuse.

This chapter first explores participants' demands for more direct lines of accountability. **Participants want to feel that those in control of their data are directly accountable to data subjects when something goes wrong.** For most participants, knowing that those in control of their data would be held to account for a data breach was crucial to feeling secure.

**Participants also want the information about the security of their data, how it will be used, and by whom, to be more accessible.** Participants feel that the information they need to make data safety-based decisions is currently too complex, too hidden, or otherwise too difficult for them to use. Simplifying this information would enable people to exercise choice, and therefore hold data controllers to account more easily.

In addition to requesting more direct lines of accountability, **most participants wanted regulation** to ensure that any organisations that **experienced a data breach would be sufficiently penalized.** A robust system of accountability should encourage data controllers to be responsible and take the appropriate steps to protect their data.

This chapter then explores what participants want from regulators and the government, and their thoughts on how they can ensure that private data controllers are held to account. Finally, this chapter examines participants' reflections on the UK's data protection laws.

## Accountability to citizens

### Private sector

Over the course of the workshops, most participants regularly expressed a need to feel more in control of their data, to feel empowered. This sentiment drove attitudes towards governance, regulation, and accountability. Most participants expressed a strong desire for more direct lines of accountability between themselves as data subjects and those responsible for their data, which this section explores.

Participants' discussions on regulation often focused on private companies, and how to hold them to account. Their suggestions, which are discussed throughout this section, centred on leveraging the power of the law and the market to both punish and deter private companies that experience data breaches. Most participants primarily focussed on how they could exercise their own agency and actively engage in accountability, and some participants wanted support from regulators and the government to do so.

“As it's my data I'd say that I'm the one that has to make the decision whether or not... If I was using Google Maps if I'm lost the risk of sharing the data are lower than the benefits I would get, I can make that choice given the nature of these apps. But if you are looking at things we don't know anything about, what the location data is going to be used for, who's going to make the decision, it's my data, I want the default to be I'm not going to share it unless it's my decision, the default seems to be they are taking it and I have to opt out if given the chance.”

### Using the law

Throughout the workshop discussions, some participants often linked together their desire to effectively pursue legal accountability for data breaches with their desire for more personal control. This included having the ability to sue, claim financial compensation, and being able to report companies to an independent body.

While some participants drew on experiences complaining to watchdogs and regulators from other bodies here, a few participants had prior experience with the Information Commissioner's Office (ICO) which informed these participants' views. Most participants found learning about the role of the ICO from specialists valuable, which again led to requests for more education about their role, how to use them, and what they can do when data is mismanaged. Participants with more knowledge about or prior experience with the ICO were more positive about the value of an independent regulatory body, although there was broad agreement that regulatory bodies were important.

### Using the market

Most participants wanted clearer, more accessible information about the competency of data controllers. They felt this would enable them to choose services provided by those with good data protection track records, and to avoid using the services of those with poor track records.

A few participants drew links to food hygiene ratings and suggested an analogous system for the use of data about people, which was a popular idea with other participants. They suggested this could include a form of certification or rating issued by a regulator that companies would have to show to data subjects when asking consent for data collection.

While companies can currently apply for certification against certain standards, such as ISO/IEC 27001<sup>44</sup>, this is not currently mandatory. Moreover, relying on ISO/IEC certification puts some of the onus on data subjects, as it relies on data subjects having knowledge of, and understanding what this certification means. Instead, these participants wanted a simple, easy to understand method for assessing the competency of data controllers that are asking for their data which data controllers are obliged to provide.

In addition to empowering participants to incorporate data safety-based information into their choices, participants also felt that this would be an effective punishment system and deterrent. If companies were forced to display this rating, those with poorer ratings might lose customers, which would harm their revenue. This also increases control without adding additional burden to the user.

“In a physical sense if you were going to buy jam you wouldn't buy one with the seal broken because you'd think you can't trust it and buy one with the seal on it because you'd trust it. What I meant in that context is I'd rather a seal from the government to tell us that these are properly checked companies than a brand in itself.”

Most participants indicated that they want to actively incorporate data safety information into the choices they make. However, participants feel that the information they need to make data safety-based decisions is currently too complex, too hidden, or otherwise too difficult for them to use. Simplifying this information would enable people to exercise choice, and therefore hold data controllers to account more easily.

In addition, some participants' trust in data controllers was driven by their openness to accountability. Openness from data controllers about accountability procedures helps to show that they are following the rules and have nothing to hide, which in turn signals that they are likely to have robust data security practices.

---

<sup>44</sup> ISO (2005) 'ISO/IEC 27001 Information security management'. Available at: <https://www.iso.org/isoiec-27001-information-security.html> (Accessed: 7 October 2021)



## Governmental and public sector bodies

### Trust and accountability

Across discussions about the accountability of the central government, participants often expressed views that were driven by their own personal political attitudes. Those participants who expressed less trusting, more negative attitudes towards the central government voiced concerns about the closeness of the government and other public sector actors to independent regulators. Some of these participants questioned whether regulatory bodies could hold public sector data controllers to account as effectively as they could hold private sector data controllers to account.

On the other hand, those with more positive attitudes towards the work that the central, local, and regional governments and public sector organisations do were also more positive about their accountability. Some of these participants highlighted that trust in government and public sector data controllers could be developed through access to transparent information. The information should include how their data was used, and whether its use would have benefits.

“Yeah, knowledge is power, the lack of awareness makes people jump to the worst conclusion, and not being told where information is going will always lead to mistrust. The best way to alleviate mistrust is to know how they're using this and what they're doing with it. It's about communication and education for me.”

In the final survey, after workshop 3, participants were asked the extent to which they trust different organisations to use their location data. On average, participants were more trusting of public sector and academic research uses of location data compared to private sector uses. However, the average (mean) reported trust for the local government and the UK government using location data fell between 'Not very much trust at all' and 'A fair amount of trust'. The full chart is in Appendix F, Figure 16.

### Democratic accountability and choice

Some participants discussed how the democratic accountability of ministers helped them to feel more comfortable about location data use. During these discussions, participants indicated that they felt it was generally easier to hold public sector and governmental data controllers to account, as the mechanisms for doing so are already built into society. If there was a data breach, or data was being misused, this may have political ramifications which could affect electoral outcomes, for example. When participants expressed feeling politically empowered, they were also more trusting towards public sector data controllers.

Some participants feel empowered through the democratic system, and able to use their choice as voters to hold ministers to account. This mirrored the emphasis that they placed on choice when considering how private, for-profit companies could be held to account. Similarly, participants wanted access to clearer information that enables them to vote with their wallet, and to use the free-market system to hold private sector data controllers to account. In both cases, participants want to feel empowered to actively engage and use their agency.

Participants would like clearer lines of accountability between data controllers and data subjects.

Participants feel that they should be able to use legal and regulatory routes of accountability, in addition to leveraging the power of the market to hold data controllers to account.

Participants felt that legally requiring companies to display information about their data security history, would help data subjects to more easily incorporate considerations about the safety of their data into the choices they make as consumers.

Openness from data controllers, particularly about accountability procedures, helped participants to feel trusting and secure.

Attitudes towards governmental and public sector data controllers was often informed by participants political attitudes.

## Accountability to the Government

When reflecting on the role of the central government in helping people make better, easier choices about sharing their data, some participants felt that people should be responsible for learning more about data security themselves. People could then take any concerns or demands to their representatives. Others felt that it was the responsibility of the government to inform and empower the public, particularly through education. A few participants discussed wanting a private umbrella organisation to enforce standards. Nevertheless, there was broad agreement that the central government could, and should, be doing more to hold private sector bodies to account.

"It's got to have power, like the ICO. There has to be someone in power, not some old Lord. Yes, they've got to have teeth. If you're going to set up these things, they have to be powerful."

### Private sector

When discussing regulation and accountability, some participants made strong demands for more government action. Throughout these discussions, it was clear that participants saw governmental power as part of their collective power as citizens. Participants wanted the central government to hold private sector organisations to account on behalf of, and in response to, their citizens.

"We are seeing growth of new businesses where the sole purpose is to collect data full stop. They are not the organisation to benefit from using the data like your supermarket may be doing, but simply collecting data to sell on, there's more and more of these companies appearing now. If these were the only people collecting data regulating them might be easier, but question their motives are purely financial, and use trick to get round every regulation and barrier that exists. Overall, I'm highly suspicious of their motives."

Participants' broad distrust of the motives of profit-driven companies drove their desire for more government action. Participants were sceptical that private companies would hold themselves to account or open themselves to public scrutiny and accountability. In addition to requesting some form of government-issued certification or ranking to indicate the data protection histories and capacities of private companies, participants wanted more legislation and more powerful regulators to rein in large for-profit companies. This is explored in more detail in the next section of this chapter.

However, most participants were pessimistic about the ability of the government to effectively regulate location data use by large companies. These participants were concerned about the size of modern multi-national corporations (MNCs) and the ability of the government to implement laws that would protect the data of UK citizens internationally. Some participants called for more international cooperation in this area to challenge the power of MNCs. Participants' concerns about the scale of MNCs was connected to their general feeling of disempowerment and their concerns about the increasing role technology plays in society. This is discussed in more detail in [Ubiquity and reliance](#) in the next chapter.

Over the course of the workshops, participants learned more about the ICO and how regulators and the government can hold other data controllers to account. This led to most participants reporting feeling safer and more trusting of data controllers. Similarly, some participants noted that more widely publicising enforcement examples in the news would help them to understand the power of regulators and the central government, which would in turn increase trust. Both examples indicate that organisations need to provide clearer information about data regulation to help people feel secure.

“I think when I started this, I had zero trust. But as I've come on and learnt that there is protection, I've started to trust it more... Which is strange for me. Knowing that those bodies are there, and they can be trusted, gives me more confidence. I see more of a need for it now, so I've changed my opinions. They've gained a bit of trust from me.”

## Rules, guidance, and regulations

### Reflections on the UK's data regulation regime

Most participants had some knowledge of the General Data Protection Regulation (GDPR) and saw it as the public face of the UK's data regulation regime. For this reason, when reflecting on the UK's data regulation regime, participants primarily spoke about the GDPR. As such, this section focuses on participant's thoughts on the GDPR.

Some participants were concerned that the GDPR was insufficient. Participants were concerned about the scope of the GDPR's jurisdiction, which was linked to concerns about the power and size of modern MNCs. Most participants felt that any UK data laws would not be able to protect their data once it was in the hands of data controllers based in other countries. This highlights the importance of ensuring that information about the GDPR is effectively communicated to the public. When participants learned about the extra-territorial effect of the GDPR, they spoke more positively about the GDPR.

“I would have put my whole trust in NHS and police and the government. But now with the leaks I'm starting to have a different aspect in the matter, how is the data being leaked? Nothing is secure it's a bit more obvious to me should I share this and should I give my information? Somewhere along the line the data is being breached and used for different purposes, how can that happen? Especially with GDPR, how is this still being leaked, how are people still getting hold of your data?”

However, some participants stated that the GDPR had ultimately failed to make them safer. These participants pointed to ongoing data breaches and a sense that the GDPR is not taken as seriously by those in charge of ensuring compliance now compared to when it came into force. Some of these participants noted feeling that GDPR compliance had become more of a nuisance, tick-box exercise rather than something that data controllers took seriously.

Participant experiences of the GDPR contributed to their attitudes here. For some participants, their only experience of the GDPR was cookie consent pop-ups, which they found to be annoying and intrusive. In turn, this led to negative attitudes towards the GDPR. Conversely, other participants had experience ensuring GDPR compliance in their jobs, which helped to make the GDPR feel more material and more meaningful. This ultimately led to more positive attitudes towards the GDPR. This demonstrates the importance of ensuring that implementing the GDPR leads to positive experiences for the end user.

### Enabling control

Throughout conversations about regulation, most participants expressed a desire for there to be more focus on informed consent. Some participants were concerned that companies were knowingly taking advantage of peoples' unwillingness to read long, technical terms and conditions to avoid ensuring that users knew exactly what they were signing up for. These participants emphasised the importance of being able to easily rectify their own complacency or mistakes. Participants wanted the option to easily and regularly monitor how their data was being used and to withdraw consent. In addition, they thought that further regulation to ensure that this process was easy could help participants to feel more secure.

“I’m the kind of person who clicks accept cookies all the time without reading what’s going on and I’m not really sure what kind of permission I’m giving. And I think sometimes people are in a rush and they tend not to read these kinds of things. [...] A lot of time I think they take advantage of that but obviously adding up stuff that maybe personally, if I knew at the start, I wouldn’t have shared in the first place.”

Moreover, some participants talked about data storage time limits providing a potential opportunity to review how the services they’re using collect their data. While participants felt that it was reasonable for certain types of data about people to be held for longer periods of time if it was used for safety purposes or it was in the public interest, most participants felt that private companies should be required to periodically destroy data and ask for consent again. In line with participant requests for more control without additional burdens, participants indicated that they wanted their phone’s operating system to help them to do this.

These participants disagreed on the length of time, with some feeling it depended on the type of data. The length of time suggested varied from three months to three years. However, in response to an example provided during workshop 2, participants largely agreed that Transport for London keeping data for 10 years was too long.

### Protecting people

Although some participants noted the challenges associated with tailoring something like the GDPR to different circumstances, most participants noted how different people might require different forms of protection. In response to one of the personas, where a child was using services that tracked location data (see Appendix C, Figure 6), some participants highlighted the importance of additional protection for children.

“As mentioned before, working in a secondary school, I strongly believe that parents should take more responsibility for their children because I think that mobile phones make parents’ lives easier.”

While some participants felt that protecting children was primarily the responsibility of parents, other participants felt that the government needed to do more to ensure that companies were not able to track children’s data. Participants wanted to ensure that age verification procedures were more thorough to prevent children and young people lying about their age. In addition to suggesting that schools should teach about data protection, some participants also wanted the government to do more to educate parents about data collection to ensure that they were able to make informed choices as parents.

These concerns extended to other groups that might find the information provided in the consent agreement harder to understand, such as those that speak English as a second language or people with learning disabilities, or those that might be more vulnerable to data misuse. Participants' conversations in these areas were typically prompted by the workshop activity exploring different personas. Participants from specifically impacted groups voiced similar concerns, both in response to personas and based on their own lived experiences.

Some participants were also concerned about which individual people have access to the data. A few participants drew on examples of women killed by police officers. This was informed in part by the murder of Sarah Everard<sup>45</sup>, which occurred while the workshops were running. Although location data misuse was not known to be a factor in Sarah Everard's murder, to participants this example highlighted the power imbalance between data subjects and the individual people within an organisation that might have access to their data. During this part of the discussion, participants suggested that the government or a regulatory body should ensure that all those with access to individual data were properly vetted.

**Participants were concerned about the ability of regulators and the central government to hold powerful multi-national companies to account.**

**Participants felt that organisations need to be doing more to ensure that the public is informed about the power of regulators and how they can be used.**

**Participants wanted data regulation around consent to facilitate more positive user experiences, rather than less positive user experiences.**

**Participants want more control over their data after its collection. They wanted to be able to easily withdraw consent and review the way their data is being collected and used. Consent expiry periods would provide an opportunity for this.**

**Participants felt that more needs to be done to ensure that children and young people understand terms and conditions and are prevented from signing up to age-restricted services.**

**Participants felt that those with access to individual data should be properly vetted.**

<sup>45</sup> BBC (2020) 'Sarah Everard: Met Police officers investigated over case file access'. Available at: <https://www.bbc.co.uk/news/uk-england-london-57146622> (Accessed: 21 September 2021)

## 6. Findings: Reliance on and choices about data



### Summary

Over the course of the workshops, most participants discussed the relationship between agency, transparency, and security. Throughout these discussions, they indicated that each was a prerequisite for feeling empowered, trusting, and, ultimately, safe.

This chapter opens by introducing **the importance of consent in participants' overall views**, before exploring what feeling in control of their location data means to participants. Participants often used choice and consent synonymously, e.g., participants want to be given the choice to consent to data collection. Sometimes, participants wanted more choice about what it is they consent to. In this case, consent and choice are still intertwined. When participants are asked by apps or services to consent to data collection and use, but their choices about which types of data they are happy to share or what uses are acceptable are limited, participants feel that their consent is undermined.

This section of the chapter then explores the tension between participants' demands for more active control, and simple, accessible services. **Participants want more control, but without it presenting any additional burden on the service user or any barriers to the use of the service.** Participants spoke positively of protection and controls built into operating systems rather than within each app, website, or service.

This chapter then considers participants' reflections on the changing role of technology in society. **Participants reported feeling resigned to use services that modern life demands, even when they dislike the way the organisation uses their data.** This chapter then examines participants' feelings of disempowerment and ambivalence about location data collection, before ending on participants' reflections about who should be responsible for empowering citizens.



## Consent and choice

### Consent as a top priority

To most participants, active, informed consent was a key requirement for most forms of individualised data collection. Consent was considered less essential for aggregate data or data used by the emergency services. However, when any type of individualised data is collected without a purpose that participants see as valid, such as for societal benefits or emergencies, it is through consent that the data becomes valid. In other words, when data collection and use does not benefit the data subject in a clear and obvious way, such as when a company is selling data to a third party for profit, participants feel that active consent is more important. In addition, the more private participants felt the data was, the more they valued choice and consent.

“Choice is key to build trust. Even before... it has to be a choice before accountability.”

The importance of consent highlights participants' needs to feel empowered, to feel in control, and to feel as though they have a meaningful choice in how their data is shared and used. For most participants, the freedom to exercise choice is the main driver of trust towards data collection and use. This reflects participants' weariness of both data security practices and the governance of data. In both cases, some participants felt that data about them was safer when they were able to exercise more control over it, particularly over how it was going to be used and by whom. For some participants, the only person that can be ultimately trusted is themselves; therefore, having the ability to exercise control, to make choices, drives feelings of trust and security.

### Conditions for feeling in control

“Why give us the option, if we can't use the app without clicking that box?”

In questionnaires given to participants prior to workshops 1 and following workshop 3, participants were asked whether they agree or disagree with the statement: 'I feel I have control over the personal information that I have shared online'. The results are displayed in Appendix F, Figure 13. In both surveys, more participants disagreed with the statement than agreed. Through the workshops, most participants indicated that they want more control over how location data was used.

When thinking about what it meant to freely exercise choice, participants highlighted certain requirements: access to simple, transparent information; granular, more detailed forms of consent; and specific consent for the sale of data.

First, and most importantly, participants wanted transparency. The public need to know, in simple terms, what data is being collected and how it will be used to feel secure. The accessibility of information was also crucial to participants. Most participants reported finding the information provided when asking for consent too long and technical, which resulted in people still not really understanding what it is they're signing up for.

“If I bought my nan a fitness watch and she loved it, she'd have no idea it knew exactly where she was at every point - is that ok? So many people scroll down to agree and there's so many words and its complicated, you just click agree. You want the watch to work, so is there really a choice?”

Most participants also wanted more granular forms of consent that ensure users can choose the exact types of data that can be collected, and how specifically that data can be used. These participants felt that forcing users to either provide a single, blanket consent or to not use the service did not actually provide a choice. Instead, it provided an illusion of choice, but kept the power in the hands of the company collecting data rather than empowering data subjects. Some participants were particularly vocal about the sale of their data to third parties and emphasised that this should always require active consent.

### Choice, without burden

Despite calls for increased agency, more detailed consent, and more options, some participants were also frustrated by the measures already in place to provide them with more opportunities for control. As most participants spoke negatively about the GDPR cookie consent popups, a broader analogous system for other forms of data is likely to be unpopular, too. Instead, participants want more control without additional burdens or barriers to using the services.

“It's so irritating having all these cookies. Do you want this or do you want that etc. Kind of feels like you're going through airport security sometimes online these days. Always in the centre of the page in your face can opt to turn it on or off as you wish.”

People spoke positively about recent changes to Apple's mobile phone operating system<sup>46</sup> to control the data that different apps could access. A few participants also highlighted the value of using Virtual Private Networks (VPNs) to stop tracking. This indicates that building more systems of control into the technology platforms that people use to access different services, such as operating systems or internet browsers, rather than into the service itself, such as websites or apps, might be a more popular solution. Overall, participants wanted organisations that provide technologies and services to make it easier for participants to exercise control.

<sup>46</sup> Apple (2021) 'If an app asks to track your activity'. Available at: <https://support.apple.com/en-gb/HT212025> (Accessed: 21 September 2021)



Participants felt that active consent was more important when participants do not benefit directly from location data use, or when the data collected is more sensitive or individualised.

Consent gives participants control over their data, which helps them to feel more secure, particularly when they feel distrust.

Participants wanted more granular forms of consent that offer more choice.

Participants wanted less intrusive ways of controlling their data, and wanted technology platforms to make this easier.



## Spotlight: Digital resignation

Participants' perspectives on the ubiquity of data in modern life, combined with their feelings of disempowerment and desire for more choice and control over data, reflect a phenomenon described by academics as **digital resignation**.

Defined by sociologists Draper and Turow in 2019, digital resignation is 'the condition produced when people desire to control the information digital entities have about them but feel unable to do so.'<sup>47</sup> In short, people feel resigned to the fact that the world is driven by data – not always to their complete benefit – and they have little agency to change that.

Draper and Turow developed the theory of digital resignation in response to several surveys and studies in the US, UK and Europe that reported a growing sentiment among the public that echoed this dialogue's participants' desires for greater agency over data but feelings of disempowerment. This sentiment emerged largely following events such as the Cambridge Analytica scandal, which raised awareness among the public of the role data can play in surveillance and influencing politics and society.

This sentiment is often described as the 'privacy paradox': 'the idea that although people say they care about information privacy, they often behave in ways that contradict those claims.'<sup>48</sup> Previous hypotheses to explain this paradox suggested a lack of awareness among the public about their data rights, or that people made the rational choice to share data because the benefits outweighed the cost. While both hypotheses may hold some truth, research by Draper, Turow and others suggests digital resignation is a more accurate explanation.

<sup>47</sup> Draper, N.A. and Turow, J. (2019) 'The corporate cultivation of digital resignation', *New Media & Society*, 21 (8), pp. 1824–1839. doi:[10.1177/1461444819833331](https://doi.org/10.1177/1461444819833331).

<sup>48</sup> Kokolakis, S. (2017) 'Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon.' *Computers & Security* 64: 122–134.

Digital resignation occurs when people feel data practices are unfair, and it risks undermining trust in the use of data.<sup>49</sup> Recent public dialogues in the UK also prompted Stilgoe and Cohen to draw a connection between digital resignation and 'reluctant acceptance': the feeling that some technologies aren't perfect or wholly good, but due to their role in society we have no choice but to rely on and accept them.<sup>50</sup> This reluctant acceptance helps understand why and how digital resignation occurs for many people when thinking about data use.

The concept of digital resignation is useful for understanding the dialogue participants' perspectives. It shows us that trustworthy location data use isn't only about providing more information about people's data rights, or just being more transparent about how and why location data is used. Both are vital, but alone they will not do enough to address feelings of digital resignation. Instead, developing ways for people to feel more empowered about how data about them is collected and used – giving them more choice and control in their everyday experiences of a data-driven world – is crucial to ensuring location data uses are trustworthy and ethical.

## Ubiquity and reliance

### Digital resignation

Over the course of the workshops, most participants expressed feelings of resignation. These participants highlighted the integral role technology plays in their day-to-day lives, and while some participants were more accepting of the ubiquity of data collection, others found it frustrating and disempowering. As mentioned in [Chapter 3](#), while participants recognised the benefits of increased convenience, they also highlighted a range of risks that they found complex, and difficult to resolve. Some participants expressed feeling trapped or forced to use modern technologies that collected and sold data in exchange for their services.

Most participants spoke about the extent to which they personally rely on services that collect location data. A few participants spoke about how using services was habit-forming, and that while they might have reservations or concerns about how their data is being used, they feel unable to stop using the services provided. These participants pointed to different barriers they might face in opting out of using different services. It could be more difficult to stay in touch with their friends and family, it might be more difficult to find a job, and navigating while travelling would be harder, for example. The cost of opting out extends beyond being unable to use the services provided, it could marginalise people and exclude them from different aspects of society.

---

<sup>49</sup> Kennedy, H., Elgesem, D. and Miguel, C. (2017) 'On fairness: User perspectives on social media data mining', *Convergence*, 23(3), pp. 270–288. doi:[10.1177/1354856515592507](https://doi.org/10.1177/1354856515592507); Draper and Turow (ibid).

<sup>50</sup> Stilgoe, J. and Cohen, T. (2021) 'Rejecting acceptance: learning from public dialogue on self-driving vehicles', *Science and Public Policy* [Preprint], (scab060). doi:[10.1093/scipol/scab060](https://doi.org/10.1093/scipol/scab060).

Some participants also highlighted that people often might not know when they are providing location data but do so inadvertently, particularly when providing location data is a secondary consequence of another more obvious aim. For example, participants want to use social media to keep up to date with friends and family, and this could include sharing holiday pictures. The primary aim is to share a photograph with friends and family, and sharing location data to the social media platform is an unavoidable consequence.

“I'm so reliant on Google and Facebook and other different mediums that I blindly trust them, but there's red flags. It's like being in a relationship. You rely on it, and you can see where it's not working, but at the same time, you're hooked.”

Participants' concerns about the habitual, addictive nature of the services appeared to be driven by their more general sense of distrust towards profit-driven data controllers. Some participants felt that data controllers were taking advantage of users' dependency on their services, as their dependency makes users complacent about what data is being collected and how it is being used. This reflected a similar sentiment participants expressed about the use of long, complex, jargon-laden language when gaining consent for data collection. Some participants felt that using inaccessible language discouraged people from engaging with the content in terms and conditions around data collection and use.

Participants' thoughts on proportionate uses of data were important here too. Participants recognised that technology was ubiquitous because it was so useful, whether for convenience or safety. As discussed in chapter 3, most participants felt more comfortable about for-profit location data collection when it provided obvious benefits to the user, such as making their lives more convenient. For some participants, seeing the obvious benefits of location data collection by for-profit companies made people feel more trusting. In turn, this made these participants less concerned when consenting to location data collection, even if they found the information inaccessible.

Conversely, for some other participants the ubiquity of technology amplified their feelings of being trapped, and forced into complacency about location data collection and use. Some participants reported feeling overwhelmed by the volume of data collection, too. A few participants highlighted that sometimes the amount of data sharing between different companies and advertisers, often highlighted by adverts that seem to follow users between services, made it feel inescapable and claustrophobic. To these participants, this again highlighted the power imbalance between data controllers and data subjects, and the lack of control data subjects have about how they experience data collection and use in their day-to-day lives.

Some participants highlighted examples of apps that they found to be intrusive based on the amount of location-based data they requested; for example, a few participants talked about Google Maps automatically asking for pictures and reviews of different locations people had visited. While a few participants highlighted the benefits of reviews linked to Google Maps search results, a few other participants felt that this app was asking too much of users too frequently.

## Reluctant acceptance

Most participants felt that society is moving towards a future where data collection is unavoidable and that this has been accelerated by the pandemic. Some participants pointed to the move to contactless and digital payment technologies to limit the spread of the virus, such as card-only payments and the use of digital transport tickets. As a result, the choice to avoid using technologies which collect location data are becoming increasingly limited.

“You don't really have a choice – you can't really pay by cash; you have to use debit card. If you haven't got Trace app, you have to fill in details manually. Unless you live in a cage, you will give your data away.”

As participants learned more about location data collection, some found it simultaneously unnerving but unavoidable and, in some cases, therefore acceptable. This is symptomatic of resignation and disempowerment. Participants feel both unable to control the growth of technology which relies on individual data collection, and unable to avoid opting in. Choosing to accept the inevitability of location data collection might make some participants feel a sense of regained control, as it becomes an active decision. This makes it feel as though they have provided active consent, even when they have not.

“I've decided I'm not worried about it at all. I'm not doing anything wrong, [such as] shopping for illegal substances, so it's OK. It's annoying but whatever. I suppose location data it is a bit disconcerting that people know everything that you live and breathe, but what choice have we got? We don't have any choice. I don't think they will ever give us the control back.”

Overall, participants often expressed ambivalence towards data collection. On the one hand, they often found any form of data collection disconcerting and unnerving. On the other hand, participants liked the services provided by companies that collect and sell their data, they saw how it could benefit them, and accepted its collection even if it made them feel uncomfortable. In some cases, this was symptomatic of digital resignation and reluctant acceptance. In other cases, some participants recognised this tension, but were unable to resolve it. As participants often spoke about their desire for more control, for-profit data controllers providing choices about how people's use of a service is monetised could help participants feel more comfortable with the commodification of their data.



Participants feel dependent on certain services and technologies, which limits their ability to opt out of data collection and creates a power imbalance between data subjects and data controllers.

This led to some participants feeling overwhelmed and disempowered.

Participants recognised that technology was ubiquitous because it was so useful, whether for convenience or safety. This made some participants feel more trusting, and some participants feel more trapped.

Some participants expressed simultaneous feelings of concern and acceptance, which reflects their feelings of resignation and disempowerment.



## 7. Conclusion

### Talking to the public about location data

**Participants recognised that the use of location data and potential consequences are complex, and that there are no easy answers for ensuring ethical practice.**

Most participants entered the dialogue feeling that they had little awareness of location data. They were generally surprised about how much they might be sharing and how little information they felt they had previously had on the topic, but by the end of the dialogue felt significantly more informed.

Through the dialogue, participations saw location data as a subset of their personal data, and many of their attitudes toward location data were rooted in their views and relationship with data and personal data more generally. Nevertheless, participants thought that location data could bring benefits to themselves and to wider society, but its use also raised concerns. Considerations about the opportunities and risks formed the basis for wider ethical discussions.

Participants' aspirations for location data centred around using it to help in emergencies, preventing and solving crime, supporting decision-making for public services, supporting better health and wellbeing, or combating environmental issues. Convenience was also important, but rarely framed as being aspirational or essential.

Participants' concerns centred around data breaches, data being sold on, risks to child safety, data misuse or manipulation, loss of privacy, discrimination, and perpetuating inequity.

Participants generally saw the opportunities of location data use through a lens of public benefit, while concerns were rooted in an individual perspective. Similarly, they felt more strongly about data that could identify people, and raised fewer concerns about location data that is not about people or is genuinely anonymous.

### A vision for ethical and trustworthy location data use

Participants acknowledged that the benefits and concerns of location data use often cannot be separated, as realising the potential benefits risks realising the concerns. When reflecting on these tensions participants did not suggest abandoning location data use, but wanted to see how their concerns could be mitigated, so the benefits could be maximised without accompanying harms.

**Participants reflected on the benefits and concerns to recommend various conditions for trustworthy location data use.** Trustworthiness was often rooted in what participants considered to be good or ethical practice; therefore, their perception of ethical issues generally mirrored their recommendations for trustworthiness.

Their reflections and recommendations suggest four components of ethical and trustworthy location data use.

## 1. Intent to benefit society



**Participants think that why location data is used and who benefits from it are important when considering whether location data use is ethical and trustworthy, and that benefits to members of the public or wider society should be prioritised.**

Participants recognised that for the benefits of location data to be realised, all kinds of organisations need to be involved, including those that may also have interests beyond only benefiting the public, such as generating profit for their business. Though not all participants considered such other interests to be inherently bad, many participants repeatedly shared concerns about how they feel location data – and data more broadly – is often used in ways that benefit data processors more than it benefits data subjects or wider society.

Moreover, they shared concerns that location data might not always benefit those who most need it. They felt that ensuring under-represented groups can experience the benefits is a fundamental requirement of ethical location data use. This is something many organisations think about when using data, but participants' views suggest that exactly how this is put into practice is not clear, and ensuring certain communities or people are not 'left out' of the societal benefits is crucial.

**Overall, participants felt most comfortable with the use of non-identifiable location data for public good, seeing that as the most ethical and trustworthy application.**

They generally considered 'for public good' to mean things that benefit society and communities, such as improving services, healthcare, or infrastructure. Although participants were concerned about location data use being primarily profit-driven, they did not equate 'for public good' to mean 'not making profit'.

## 2. Effective accountability



**Participants think data collectors should be accountable to regulators and data subjects, with consequences for breaches or misuse, and they questioned whether current governance is effective in achieving this.**

There exists an extensive data regulation regime in the UK. However, participants did not feel data protection laws, like the GDPR, were as effective as they could be. Many participants thought that existing regulation does not do enough to force data processors to act in their best interests, and it does not reassure people that data is held securely or used responsibly. These concerns were not due to a lack of awareness, as it remained after participants became more informed about data protection laws. Participants' perspectives about data protection laws were influenced by their reflections on their personal experiences, on the power of large technology companies, and on the actions of some small and medium sized firms.

### 3. Accessible transparency

**i** **Participants want data collectors to communicate in an accessible way what location data will be used for, who will have access, and how it will be stored, so people can make informed choices and ensure accountability.**

The topic of transparency cut across this dialogue. Many participants felt that current attempts to provide information are inadequate and far from user-led: terms and conditions relating to data are complex, cookie-notices are confusing, and there is a general lack of clear information about data use. Throughout the dialogue, participants shared how they wanted to know more about what location data is collected, what it's used for, and which organisations are involved.

However, it's clear that transparency is not about simply giving users more information, it's about presenting the relevant information in an accessible and usable way so that people feel more empowered – not more confused – about the choices they make about data. The dialogue findings also suggest that accessible transparency will support people to feel more reassured about where and when data use is genuinely in the best interests of people and society.

### 4. Enable agency



**Participants want more genuine ways to consent to and participate in ongoing data storage and use, and greater choice over how their data is used.**

Most participants felt disempowered when it comes to data use, which makes them feel less safe and more distrusting. To have more agency, participants wanted more accessible, simple, and honest mechanisms to engage with and make decisions about data collection and use.

Participants understood that providing mechanisms for accessible transparency and agency is not always simple. Nevertheless, they felt the burden should be on policymakers and data processors to provide simple information and enable people to have more choice and agency over data. This was especially important where personal data is collected and used; for data that is genuinely anonymous, participants were less concerned about the need to consent, assuming that the data was still used responsibly.

Participants shared how schemes like public charters or accreditation markers could help data subjects understand which data processes and practices are more worthy of trust, making it easier for them to make choices about their data.

## Realising the vision

Participants considered how the challenges for ethical and trustworthy location data use are part of a much larger set of issues relating to the increasing digitisation and datafication of society. They don't expect organisations to get it right overnight, but they do expect to see changes made to respond to the public's concerns.

Participants' views were shaped by various experiences, values, and principles both in and outside of the dialogue. In the face of digital resignation and data ubiquity in modern life, participants valued agency and sought ways to improve the power balance between data collectors and data subjects.

In this report, we have referred to people as 'data subjects', and in many ways, this reflects how participants felt – out of control and having things done to them rather than with them. **What participants ultimately want is to move toward being data citizens, able to feel more agency and control, and confident that uses of location data genuinely contribute to the betterment of society.**

## Next steps

We advise that the dialogue findings be held at the core of any future policy and strategy work, with stakeholders and policymakers reviewing the participants' recommendations, to ensure that resulting guidance reflects wider public interests.

While there has been a lot of qualitative, quantitative, and deliberative research on data generally, limited research has been done on public attitudes toward location data. This dialogue was among the first depth deliberative process in the UK on the use of location data. As such, it surfaced new questions and tensions which would be valuable to unpack through **further public engagement and research.**

- Participants were keen to continue engaging with the tensions and challenges they identified between technological and data ubiquity, digital resignation, and the benefits they saw from increased location data use. What are the right mechanisms for organisations innovating with location data to demonstrate their awareness and responsibility around these issues?
- How might organisations reframe the relationship with the public, giving them the opportunity to shift from being data subjects to data citizens, and providing choice over levels of involvement and engagement in their data choices?
- How might organisations (especially in the public sector) be clearer about how they have used location data to make decisions, or develop services that benefit people, so that the public can see the tangible impacts of location data use in their everyday lives?



Crown  
Commercial  
Service  
*Supplier*



TRAVERSE  
T

[www.traverse.ltd](http://www.traverse.ltd)

©2021 Traverse Ltd. Traverse is the trading name of Office for Public Management Limited a company registered in England and Wales. All rights reserved.