DARE UK Privacy Risk Assessment Methodology Project (PRiAM) Project: D4 Report v2.0

Public Engagement

Understanding private individuals' perspectives on privacy and privacy risk

UK Research and Innovation
HDRUK Health Data Research UK
ADRUK Data-driven change

DARE UK

Document Details

Date	16/10/23
Deliverable lead	University of Southampton
Version	2.0
Authors	Boniface, M., Carmichael, L., Hall, W., McMahon, J., Pickering, B., Surridge, M., Taylor, S., Baker, K. (University of Southampton) Atmaca, U-I., Epiphaniou, G., Maple, C. (University of Warwick) Murakonda, S., Weller, S. (Privitar Ltd)
Contact	m.j.boniface@soton.ac.uk
Dissemination level	Public

Funding statement

This work was funded by UK Research & Innovation [Grant Number MC_PC_21030] as part of Phase 1 of the DARE UK (Data and Analytics Research Environments UK) programme, delivered in partnership with Health Data Research UK (HDR UK) and ADR UK (Administrative Data Research UK).

Disclaimer

This document reflects only the authors' views — the DARE UK programme, HDR UK and ADR UK are not responsible for any use that may be made of the information it contains.

Publication Acknowledgement

This report is independent research supported by the National Institute for Health and Care Research ARC Wessex. The views expressed in this publication are those of the author(s) and not necessarily those of the National Institute for Health and Care Research or the Department of Health and Social Care.

Further dissemination

An overview of this work — entitled 'Towards a Socio-Technical Approach for Privacy Requirement Analysis for Next-Generation Trusted Research Environments' — was presented at the CADE 2022 Conference (Competitive Advantage in the Digital Economy) on 13 June 2022.

UK Research and Innovation

HDRUK Health Data Research UK

ADRUK

Executive Summary

This report summarises the results from engagement with one of the DARE UK PRiAM project's key stakeholders: the general public. The aim of DARE UK PRiAM has been work towards a standard privacy risk assessment framework for those seeking to operate a secure, trusted infrastructure environment within cross-council collaborative research networks. To complement this work, understanding private individuals' perspectives on privacy and privacy risk provides a significant contribution to how to articulate to those who might engage with those services or infrastructure environments.

Since the implementation of the (UK) GDPR, data subject rights have been brought to the fore, along with the obligations of those who might process their data. Guidance is available to ensure GDPR compliance. However, less is understood about how private individuals respond to their rights or to how a data controller or data processor uses their data.

A series of workshops were organised to capture the privacy attitudes of a group of 10 self-selecting individuals particularly interested in privacy assessment and risk. Their views were used in the first instance to understand the general public's views on privacy. Further, the results from the workshops were used to develop a privacy attitudes questionnaire for a larger, random cohort representative of the general public.

The workshops led to the creation of a conceptual model of how individuals make decisions about data sharing. This model may not map directly onto the provisions of data protection regulation, nor onto the traditional methods of communicating risks to help private individuals make informed decisions about sharing their data. Privacy perceptions of the public were observed:

- Participants are aware of processes and structures but feel overwhelmed.
- Participants are often driven by achieving a specific goal rather than concern about their privacy.
- Participants want transparency around the use of clinical and research data.
- Participants are concerned about 'context' (i.e., media reporting).
- Participants reported that they felt that structures and processes should be introduced to facilitate and enhance the secure handling of their data.

The questionnaire validated these findings. In addition, responses showed that private individuals believed themselves to understand the legislation and to make informed decision, whilst showing a lack of understanding of practical consequences of the legislation especially regarding their own rights.

From the PRiAM PRAF workshops, the questionnaire and the recommendations from the PRiAM Advisory Group of domain experts, themes supporting a more interpersonal approach emerge:

- What individuals claim regarding data protection legislation will be influenced by the specific context, what similar others say and think, and by what they perceive about a situation (i.e., what they want to achieve and how they can achieve it).
- Individuals may become overwhelmed by the amount of information (e.g., *privacy notice*) they are presented with especially if it interferes with their goals. The structures may be there, but they may not use them to make fully informed decisions.
- Individuals must believe that the risk to their privacy is relevant to them specifically and that they are responsible for dealing with it: they will then respond to perceived threat. Additionally, though, they need to feel that they are *capable* of acting appropriately to achieve their perceived privacy goals.

- How individuals decide to engage with a TRE – and share their data – may derive from different mechanisms than how regulators and domain experts evaluate the TRE and their privacy structures. Motivation to participate (and share data)

These suggest the following recommendations as a starting point:

- Privacy notices should be designed to be user-friendly rather than just legally compliant.
    - They should be brief and explicit about what rights a data subject has
    - They should indicate accessible, independent resources that are available when making decisions to share data.
- When individuals are asked to decide about privacy (i.e., privacy settings, cookie choices, and so forth), this should be
    - context aware to avoid users simply ignoring them and by default agreeing to data donation.
    - sensitive to reputation
    - any current cases being reported in the press
- We should reconsider how participation in research or clinical trials might be negotiated with participants. Taking the lead from medical ethics, it is perhaps time for ongoing negotiating of data use (Muirhead, 2011; Rubin, 2014).

These findings from the workshops and questionnaire should be used to enhance the privacy assessment framework for operators of trusted research environments. In the first instance, this relates to what needs to be communicated and what is currently either misunderstood or only partially appreciated. Finally, situating these findings within the behavioural sciences helps explain the apparent discrepancy between what the general public claim to know and their actions, leading to a suggestion about how to encourage engagement and data sharing.

Updated version 2.0

When carrying out further analyses on the survey responses, we discovered an error in transferring participant respondents from *Qualtrics.* We have now corrected this error and report here revised agreement / disagreement percentages in Section 2.3.1.4. This does not materially affect the general conclusions summarised above.

Table of Contents

List of Figures

List of Tables

Abbreviations

ICO	Information Commissioner's Office
PPIE	Patient and Public Involvement and Engagement
PRAF	Privacy Risk Assessment Forum
TRE	Trusted Research Environment

1. Introduction

1.1. Purpose

This report is Deliverable 4 (D4) *"Public Engagement: Understanding private individuals' perspectives on privacy and privacy risk"* of the DARE UK PRiAM project. The report is one in a series of four project reports, which together focus on working towards standardisation of privacy risk assessment for cross-domain access and re-use of sensitive data for research purposes.

1.2. About the DARE UK PRiAM project

The 'Privacy Risk Assessment Methodology' ("DARE UK PRiAM project") project was one of nine projects funded by UK Research and Innovation (UKRI), as part of its DARE UK (Data Analytics and Research Environments UK) Sprint Exemplar Project programme. The eight-month project commenced in January 2022 and completed in August 2022. This research project involved three partner organisations — University of Southampton, University of Warwick and Privitar Ltd — and brought together an interdisciplinary team of data governance, health data science, privacy, public patient and involvement, and security experts from ethics, law, technology and innovation, web science and digital health.

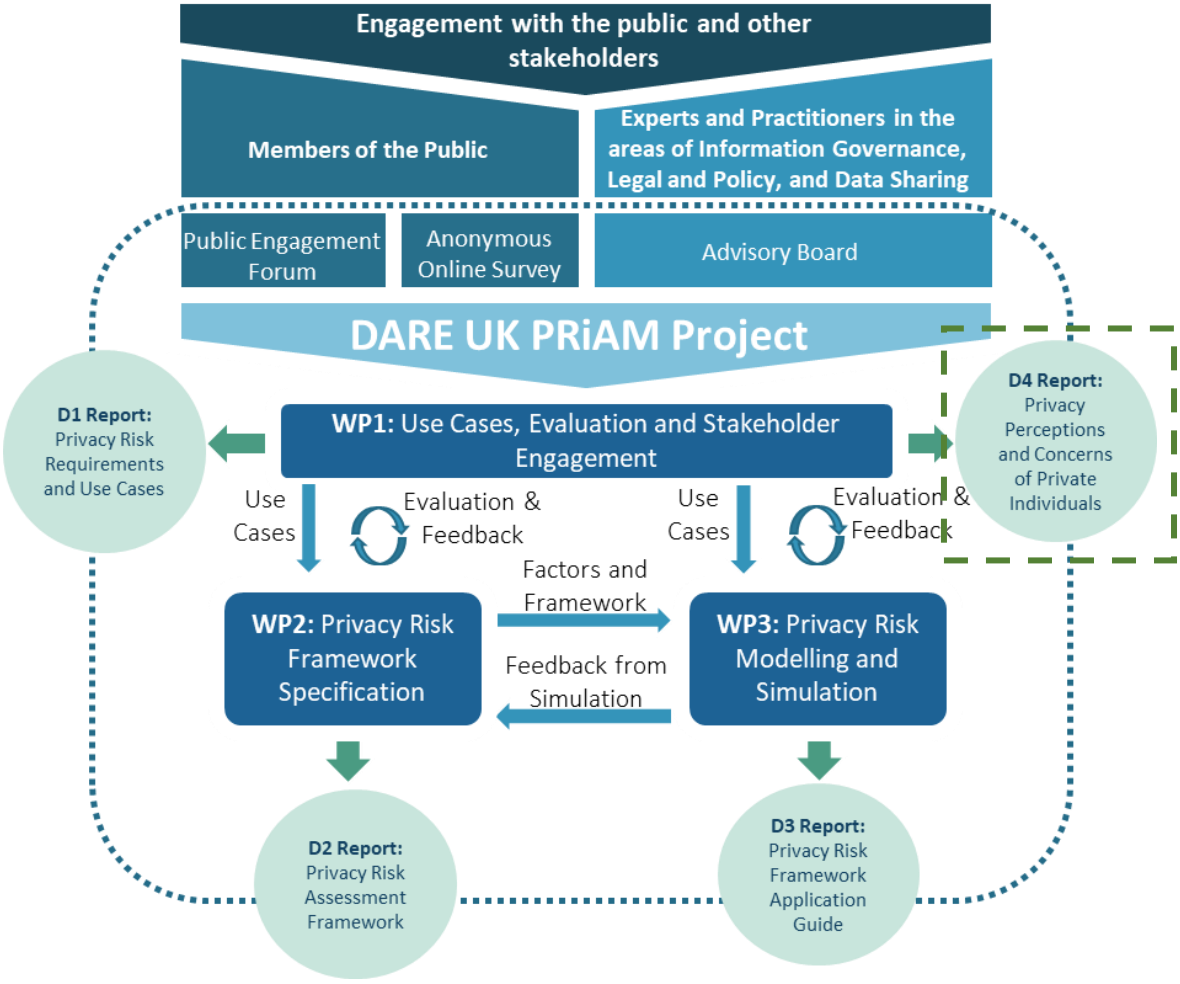

Figure 1: An Overview of the DARE UK PRiAM Project: Deliverables, Stakeholder Engagement and Work Packages

1.2.1. Motivation

Trustworthy and collaborative data sharing and re-usage for approved research purposes can help to advance public health and patient care. Data and analytics systems are changing and new ways to share and access data are emerging, including the potential for greater federation[1] of resources and services. Health and social care research often require combinations of data from multiple sources, including data from electronic health records, digital health applications and wearable technologies (e.g., Sharon & Lucivero, 2019). These changes are bringing about new and evolving risks. Organisations responsible for carrying out and facilitating such research activities must ensure that reasonable and acceptable levels of privacy protection are in place so that individuals, groups of people and wider society are not put at risk of undue harm.[2]

What remains vital is that people are protected from harms associated with data disclosure and re-use — and that public confidence and engagement in health and social care research are maintained. As such, the DARE UK PRiAM project aims to explore methods and tools that can support decision-makers, patients and the public to assess and manage privacy risk when considering emerging data access and re-usage scenarios, such as federation.[3]

1.2.2. Project objectives

This report is one in a series of four project reports, which together focus on working towards standardisation of privacy risk assessment for cross-domain access and re-use of sensitive data for research purposes. Our project objectives are as follows:

- Objective 1: Analyse **driver use cases** in public health prevention and integrated care.
- Objective 2: Identify **key factors contributing to privacy risks** within the Five Safes.
- Objective 3: Define a **risk tier classification framework** to provide a consistent methodology for privacy risk assessment.
- Objective 4: Assess privacy risks for use cases using a cyber security **risk modelling and simulation** platform, focusing on privacy risk (re-identification), threats (linking), adversarial conditions (motivations, capabilities and opportunity), controls (homomorphic encryption, parquet encryption).
- Objective 5: Evaluate the framework, modelling and simulation through **engagement with multidisciplinary stakeholders** (e.g., members of the public, research councils, information owners, regulators).

1.2.3. Project structure

Three work packages (WPs) address user needs, privacy risk framework and implementation:

- **WP1 "Use Cases, Evaluation & Stakeholder Engagement"** analyses use cases, requirements, conducts evaluation and captures/disseminates lessons learnt to maximise impact.
- **WP2 "Privacy Risk Framework Specification"** identifies privacy risks factors and develops the risk tier classification framework.

[1] As an example federative approach see the "open, federated and interoperable technology stack for trusted research environments" and "Federated Data Analytics Infrastructure - Capability Maturity Model" outlined by Health Data Research UK (HDR UK, 2021b).

[2] The objective of risk management is "not to eliminate risk, but to reduce the risk as fully as practical" by identifying "'appropriate' responses" that balance benefits and risks effectively and appropriately (Kuner et al., 2015). In other words, those responsible for research taking place as part of safe research collaborations can only offer "reasonable, not absolute, protection" (Shaw & Barrett, 2006) to individuals, communities and wider society.

[3] It is worthwhile to note that the importance of privacy preservation and privacy engineering has been recognised by the recently published "Goldacre Review" on 'using health data for research and analysis' commissioned by Secretary of State for Health and Social Care (Goldacre & Morley, 2022) For example, the following two recommendations were made by the review related to this point: "UKRI/NIHR should resource applied methods research into privacy preservation"; and "TRE 9. Evaluate new developments in privacy engineering; adapt accordingly" (Goldacre & Morley, 2022).

- **WP3 "Privacy Risk Modelling & Simulation"** models risk factors and assesses use cases using the ISO/IEC 27005 information security risk management methodology.

1.2.4. Engagement with the public and other stakeholders

The project has engaged domain experts and members of the public to ensure a broad range of stakeholder interests and opinions are considered. A **Public Engagement Forum** was established with 10 members of the public to explore privacy risk perceptions through a series of four workshops. The Forum discussions were thematically analysed to produce a **survey** for quantitative validation of opinion expressed. This survey was distributed across the UK, with participation from 500 respondents. The outcomes from the Forum and survey are reported in D4 "Privacy Risk Perceptions and Concerns of Private Individuals".

An **Advisory Board** was established consisting of 21 domain experts, including information governance practitioners, practitioners running or developing secure research facilities, legal professionals, oversight bodies, and academic experts. Using semi-structured interviews, the Advisory Board helped identify and understand the risk factors, controls and decisions related to privacy risk assessment. The outcomes of the Advisory Board are reported in report D2 "Privacy Risk Assessment Framework".

1.3. Scope of the D4 Report

Work Package 1 (WP1): Evaluation & Impact Maximisation. This Deliverable 4 (D4) report focuses on understanding private individuals' perspectives on privacy and privacy risk. This D4 report specifically concentrates on the following project objective:

> **Project objective 5 of 5**: Evaluate the framework, modelling and simulation through engagement (advisory board, public) with multidisciplinary stakeholders including research councils, information owners, regulators, and public (WP1, Outcome: evaluation and engaged network of info gov, legal & policy, practitioners and public stakeholders)

This D4 report is divided into the following sections:

- **Section 2** focuses specifically on identifying the perceptions and considerations of private individuals – the data subjects. These are explained in the context of what is known from the behavioural sciences.
- **Section 2.1** introduces our mixed methods approach, including workshops, the qualitative analysis of discussions at those workshops, and the development and analysis from a quantitative instrument derived from the workshops.
- **Section 2.4** compares these findings briefly with the outcome from engagement with the Advisory Board of domain experts, as documented in detail in PRiAM Report D2 Privacy Risk Assessment Framework.
- **ection 2.5** provides summary and recommendations based on the findings reported here.
- **Section 3** introduces some general reflections about this work, contextualised within what is known from the behavioural sciences. The empirical findings from the workshops and the survey complement the development of the PRiAM privacy risk assessment framework, suggesting that controlling for risks is the first step in encouraging data subject engagement.
- **Section 4** then concludes by summarising key points from the previous sections, and highlights further work in subsequent project reports.

2. General Public's Perceptions of Privacy and Privacy Risk

Private individuals' perceptions of privacy risk, risk in general and the sharing of data or simply how individuals decide to engage is well documented in the research literature. In the following sections, we

- Describe a mixed-methods approach implemented during PRiAM to establish and validate the private individual's perspective on privacy risk, including the development of a quantitative instrument (Section 2.1)
- Relate these empirical findings back to the perspectives provided by the Advisory Board consulted as part of WP2 and documented in PRiAM Report D2 (Section 2.2)
- Return to the empirical background from the behavioural sciences (Section 3).

The purpose of this section, therefore, is to capture and explain the perspective of the general public as potential data donors to a secure research environment.

2.1. Methodology

A series of four workshops was organised with self-selecting participants from the Privacy Risk Assessment Forum (PRAF) drawn from the southern England and London. They attended a series of four workshops (see below) moderated by two members of the PRiAM team. The overall aim was twofold:

1. To identify privacy risk perceptions from representative members of the general public;
2. To develop an attitude questionnaire to be shared with 500 members of the general public other than those who took part in the workshops.

The workshops were held virtually to a schedule agreed with participants and hosted via Microsoft Teams by the University of Southampton. The workshops were designed to investigate privacy risk perceptions, which would then be validated in an anonymous online questionnaire.

The workshops were analysed by two psychologists on the team to identify overriding themes and develop the anonymous questionnaire.

2.1.1. Recruitment and Participants[4]

Table 1 provides demographics of the PRAF members who agreed to take part in the workshops. Note that as members of the PRAF, there may be an expectation that they would be more privacy aware than the general public. With that in mind, one main aim of the workshops was the development of a questionnaire which could be distributed to the general public and validate what the PRAF members reported. In so doing, the intention was to capture the concerns and principles that in the future could be incorporated into guidelines as part of another project.

Table 1: Workshop Participant Demographics

CATEGORY	SELF-REPORTED CATEGORY	#

[4] The four workshops were approved by the Faculty of Engineering and Physical Sciences Research Ethics Committee (ERGO/FEPS/71408) at the University of Southampton.

Gender identity	Female	4
	Male	6
Workshop attendance	Four	6
	Three	3
	Two	1
Age Group	18 - 24	1
	25 - 34	2
	35 - 54	4
	55 - 64	1
	65 - 74	1
	75+	1
Ethnicity	Asian or Asian British	2
	Black, African, Caribbean, or Black British	2
	White	6

Participants were paid £50 per workshop to cover expenses up to a maximum of £150. Table 3 summarises the self-reported characteristics of the participants and attendance at the workshops[5]. Note that participants had identified themselves within a given category[6].

Participants gave research consent to take part before the workshops; they were asked if they would also provide data protection consent for the audio recording of the workshops. Microsoft Teams automatically generates a verbatim transcription of recorded sessions. The researchers analysing the workshops did not have access to the original recordings only the automatically generated verbatim transcriptions (see Section 2.2.3 below). No attempt was made to estimate the accuracy of the transcriptions.

2.1.2. Workshops

2.1.2.1. Workshop 1

The purpose of the this workshop was to identify the language used by the general public when discussing privacy and privacy concerns. Participants were introduced to five short seed scenarios (1-2 sentences) involving situations

[5] Even with a small cohort, the intention was to reflect the general population. As reported by the ONS for 2019 (https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/populationestimatesbyethnicgroupandreligionenglandandwales/2019#:~:text=As%20part%20of%20the%20White,points%20to%20an%20estimated%205.8%25.), we believe this cohort to be reasonably representative.

[6] Indeed, some differentiated higher level categories such as White with 'Welsh' or 'English'. We report only the higher level categories here.

with privacy risk including online shopping, vehicle navigation (SatNav), health tracking devices, COVID-19 track-n-trace, and secondary data research project. They were then asked to explore how they feel about privacy in relation to the scenarios presented. As the workshop progressed, it was clear that online shopping, health tracking devices and data research projects became the most significant.

2.1.2.2. Workshop 2

The purpose of this workshop was to explore **self-efficacy** (Bandura, 1982, 2012) in relation to privacy; that is whether they ***believe*** they have the ability to manage their privacy within the scenarios presented.

Participants were reminded of the final short scenarios used in the first workshop and were then encouraged to discuss the following:

- Do they know what to do to protect their privacy in each scenario?
- Do they believe they have the necessary skills to protect their privacy?
- Do they believe it is in their control to protect their information?
- Do they foresee any difficulties in protection of their privacy?

2.1.2.3. Workshop 3

The purpose of this workshop was to explore distribution of **privacy responsibilities** including those of individuals. Using the short scenarios used previously, participants were asked to explore:

- Who they believe responsible for protection of their information?
- What responsibility do they have for protection of their own information?
- Do they see different responsibilities in the scenarios described?
- Do they foresee changes to responsibilities in the future?

2.1.2.4. Workshop 4

The purpose of the final workshop was to review and test a proposed online survey derived from themes emerging in the previous workshops providing opportunity for participants to feedback and comment. Participants were asked to:

- Answer the questionnaire on their own
- Discuss pros and cons about their thoughts with the questionnaire
- Be asked how they'd improve the survey
- Be asked if they found helpful with the survey.

2.2. Qualitative Analysis

The analytical approach involved inductive thematic analysis (Braun & Clarke, 2006). At this stage, we believe we can claim saturation in that the ten participants were reasonable diverse but representative of the UK (English) population[2]. Additionally, we felt that the views expressed were consistent with evidence from other studies (see, for instance: Kokolakis, 2017), but that in adopting an inductive approach, we might claim the findings to be valid and informative in this field (Braun & Clarke, 2021).

For the first three workshops, two psychologists independently coded the first and third workshops and both coded the second. The codings from the second were discussed to establish the level of inter-coder reliability.

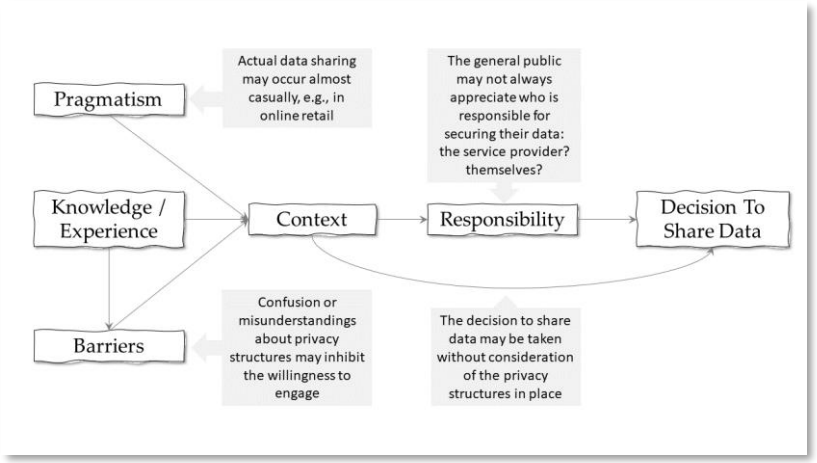

Figure 2: Thematic Map from Workshops 1 – 3

The thematic map in Figure 2 summarises the discussions from the first three workshops. A thematic map simply offers an interpretation of the relationships between the main topics ("themes") identified via discussion or literature review[7]. It therefore summarises a thematic analysis. It may subsequently be validated via empirical investigation to become a behavioural model. The *Decision To Share Data* within the context of privacy concerns represented by the scenarios (used as priming activities in the workshops depends largely on the *Context)*. However, as the figure shows, this dependency is mediated[8] by *Responsibility*; participants were not entirely sure who might have responsibility for assuring the appropriate processing of personal data. Nonetheless, they may still make decisions to share personal data with or without understanding who may be ultimately responsible for the implementation of appropriate privacy structures. For instance, they reported that when the target activity (e.g., an online purchase) might be delayed by reviewing a privacy notice or selecting cookie options, then the target activity overrode any privacy concerns (a possible variant of Uses and Gratification Theory (Lin, 1999; Ruggiero, 2000)).

That being said, *Context* may itself be moderated by *Pragmatism,* specific *Barriers* and participant *Knowledge* or *Experience*. Participants reported different behaviours, for instance, in different situations (labelled *Pragmatism*). As already stated, they would be less inclined to consider privacy risks in a retail environment because they wanted to make a purchase or complete a transaction. But in addition, within a clinical setting, perceived trust in a clinician may influence a decision to disclose.

At the same time, *Barriers* to making an informed decision were reported to include lengthy and incomprehensible privacy notices; concerns about data sharing; and about the re-use of data. Both *Barriers* and *Context* were moderated by participant *Knowledge* and *Experience*[9]: rather than actively seeking the information required in a specific situation to make an informed decision, participants would justify their behaviours based on their general

[7] The arrows therefore simply identify that there is a relationship between constructs, not the nature of that relationship.

[8] That is, once a given *context* has been identified, the *decision to share data* in that *context* is made via – in consideration of – who the data subject believes is responsible for their privacy. Note, however, there was also evidence that a *decision to share data* may be made directly and without consideration of who assumes responsibility for the privacy of the data.

[9] That is, an individual's *knowledge* (what they know from others or similar situations) and *experience* (what has happened in the past) may influence their judgement of the *context*.

perceptions and experience, including what they had read in the press or experienced in similar situations. This is summarised in the next section.

2.2.1. Privacy Perceptions of the General Public

The following summary observations can be made. Where appropriate, we link these observations to related research.

1. **Participants are aware of processes and structures but feel overwhelmed**. At the very least, *privacy notices* (including popups for cookies) need to be short and to the point. There were two main additions here:
    a. *Participants felt that privacy notices were structured to ensure regulatory compliance rather than to ensure informed consent;*
    b. *Participants suspected in some cases that privacy notices were deliberately made over complicated and long-winded to discourage data subjects from reading them*.

    Private individuals reporting that they feel overwhelmed may well be counterproductive (Witte, 1992; Witte & Allen, 2000).
2. **Participants are often driven by achieving a specific goal rather than concern about their privacy**. They frequently reported, especially in the context of retail, that they were more focused on making the purchase rather than considering the implications of sharing their data to do so. This may have relevance, of course, for the privacy paradox (Barth & De Jong, 2017): users are effectively distracted by their goals and do not engage with privacy risk assessment.
3. **Participants want transparency around the use of clinical and research data**. Notwithstanding issues of consent and what it means in a particular context (Pickering, 2021), there seems to be a clear misunderstanding of research and data subject rights (Acquisti et al., 2015).
4. **Participants are concerned about 'context'** (i.e., media reporting). As well general concerns about existing structures, participants reported a dichotomy exacerbating their data sharing decisions: on the one hand, they reported that media coverage tended to be negative (i.e., focusing on breaches and poor practice). In consequence, they found themselves increasingly reliant on their own experience and reports from trusted others (see for instance: McKnight et al., 2011; McKnight & Chervany, 2001).

These concerns need to be considered both in respect to what domain experts recommend (see Section 2.4 below) but also as they affect perceptions around privacy risk in general and the interpretation of the 5 Safes + 1 by data subjects. One final observation:

5. **Participants reported that they felt that structures and processes should be introduced to facilitate and enhance the secure handling of their data**. This was particularly challenging for the workshop moderators since what participants were asking for in terms of governance is largely available. For instance, there is an overall data protection authority (DPA, that is the ICO in the UK) responsible for checking compliance and auditing; except under specific circumstances, the data subjects retain significant control over their data (as set out in GDPR, Chapter 3, and DPA (2018) Part 3, Chapter 3[10]). As identified by other researchers, though, empowerment is not enough to support the general public in the information age (see Acquisti et al., 2015, p.514).

There was considerable agreement on these matters in the workshops. This will be investigated further in an online survey as described in Section 2.3 and 2.3.1.

2.2.2. A "Model" of Private Individual Privacy Risk Assessment

[10] See also: https://www.gov.uk/government/publications/data-protection-rights-for-data-subjects/data-protection-rights-for-data-subjects

What the workshops have shown is that privacy risk assessment from the perspective of the general public is different from the risk assessment frameworks and regulation which would typically, and quite rightly, be in place to inform and monitor research or service provider infrastructure and procedures. As summarised in Figure 2, the general public make privacy decisions such as the decision to share their data based on *context* and their perception of who carries *responsibility.* Therefore, they are influenced by what they perceive as barriers, their own experience, and a pragmatic assessment of what they want out of a given situation and will then consider who they believe to be responsible for the protection or management of their data. Decisions to engage or to share data may therefore be based on affect rather than a measured thought process (see Section 3.1 below). It is clear at this stage that how data subjects decide to share their personal data is non-trivial. How such decisions are reached should be investigated further in future.

2.3. Quantitative approach: Questionnaire development and validation

From the first three workshops, the two psychologists created a list of 137 assertions based on statements made by participants present: 54 from the first workshop, 37 from the second, and 46 from the third. These were then reviewed for duplicates or items which might be regarded as irrelevant or distracting, yielding a final list of 48 assertions.

These were randomly grouped into four sets of twelve assertions for presentation purposes (i.e., to avoid a participant being faced with a single list of 48 assertions to evaluate). Each assertion was coupled with a five-point Likert rating scale (*Strongly Agree* to *Strongly Disagree*), with some of the assertions reversed to mitigate against participants simply rating all assertions the same (Willits et al., 2016). The criticism that reverse valence items increases cognitive load (Suárez-Alvarez et al., 2018) does not apply here, we maintain, since the original assertions included negatively worded items anyway.

Each of the four blocks of twelve assertions was introduced with a series of 'slider' options: in response to a single statement, participants were asked to provide a rating for three associated choices. For example, with the introductory statement

> *How likely am I to share my information with*:

Participants could move separate sliders for *Online researchers, Retailers* and *Government* between 0 and 100, thus expressing their views about the context within which they might share their data (or information). The twelve assertions in each of the four blocks were presented in random order to address potential sequence effects. Six of the assertions across all 48 were reverse coded. This involved taking a positive assertion, for example, and turning it into the corresponding negative one:

> For example, ***I am concerned by media coverage of data breaches or losses*** was presented as ***I am not concerned by media coverage of data breaches or losses***

In consequence, and as is common with such an approach, participant assessment (i.e., *Strongly agree* to *Strongly disagree*) are also reversed.

At the fourth and final workshop, this draft questionnaire was discussed in terms of readability (were the assertions understandable?), the length of time to respond, and any general formatting concerns. Using this feedback, a final

version of the questionnaire was produced (see Section 5 below). After further ethics review[11], this was be distributed via the crowd-sourcing platform, *Prolific.co*. Participants were paid £1.65 for their responses[12,13].

2.3.1. Preliminary Results

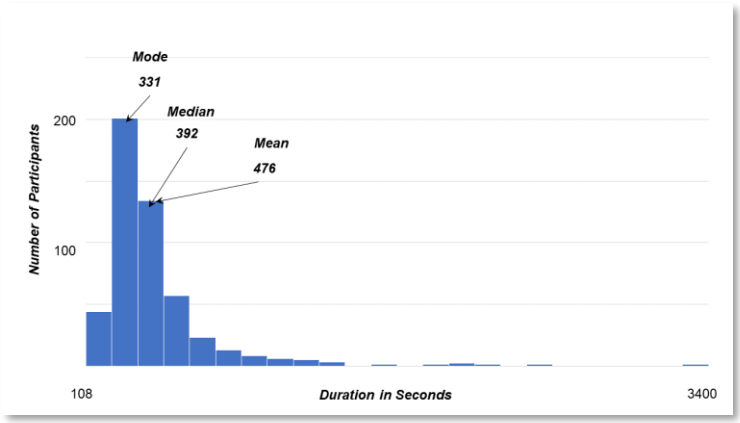

Figure 3: Distribution of the time take ("Duration") to complete the questionnaire

The questionnaire derived from the workshops received 500 responses. Some responses took very little time to complete (minimum duration 1.8 minutes) or conversely very long periods (maximum duration 56.6 minutes). Figure 3 shows the positive skew to the distribution of how long participants took to respond to the online questionnaire, with a modal value of 5.53 minutes[14]. The majority of durations (the time respondents took to answer the questionnaire) bunch together around the measures of central tendency suggests making it reasonable to assume the questionnaire did take significantly less time to complete than in the pre-release trial, i.e., around 5 to 6 minutes as opposed to 11 minutes. Further, it is reasonable to want to focus on responses clustered round this point, i.e., around 5 to 6 minutes are the most frequent responses (the distribution, though skewed, is peaky: the y values are greatest around this area). To remove outliers based on duration, 95% of responses below the ***modal*** value (the bottom 8 values) and above the modal value (the top 24 values) were removed. This yielded 470 responses, or 93.9% of responses from the original 500, preserving the modal duration and the distribution skewness, of course, but now the minimum duration was 3.27 minutes and maximum 17.40 minutes.

2.3.1.1. Demographics

Ethnicity was reported with the sample summary from *Prolific.co*, rather than captured explicitly within the questionnaire. Table 2 summarises the coverage.

Table 2: Ethnicity of Questionnaire Respondents

Registered Ethnicity	# in survey	%	
		Sample	UK Gov

[11] The original research ethics review (ERGO/FEPS/71408) covered the PPIE workshops only. The amendment (ERGO/FEPS/71408.A1) covered the derived online survey.

[12] An internal trial with colleagues resulted in an average time of just over 11 minutes to complete the survey; taking an hourly rate of £9.00 (which is just short of the UK minimum wage of £9.50/hour), (11/60*£9.00)=£1.65.

[13] It should be remembered that crowdsourcing platforms, such as *Prolific.co*, advertise surveys to registered users who therefore become experienced respondents.

[14] Mean value: 7.93 minutes; Median value: 6.53 minutes.

White	429	85.80	86.00
Asian	35	7.00	7.5
Black	16	3.20	3.3
Mixed	10	2.00	2.2
Other	10	2.00	1.0

The third (from *Prolific.co*) and from the UK census information from 2011[15] align well. Respondents therefore represent the ethnic mix of the UK population at this time.

Self-reported ***Sex*** (gender identity[16]) was captured directly in the questionnaire as well as available from *Prolific.co*. It is summarised in Table 3.

Table 3: Reported Gender Identity of Respondents

Gender Identity (*Sex*)	# from *Prolific.co*	% of 500	% from UK Gov[17]	# in survey	% of 470
Female	257	51.40	51.00	245	52.13
Male	243	48.60	49.00	225	47.87

The final two columns are reported from the extract without outliers (according to time taken on the survey). The figures across the columns correspond well: in all cases self-reported "Female" is slightly greater than "Male", including the extract of 470 reported here.

Age Group was also captured in the questionnaire and is summarised in Table 4. *Profilic.co* provides the actual age[18]; and the UK Census uses different groupings[19]. This makes direct comparison difficult. The Table is provided therefore for reference purposes only.

Table 4: Self-reported Age Group of respondents

Age Group	#	% of 470
18 to 27	78	16.60
28 to 42	127	27.02
43 to 62	178	37.87
63 to 76	83	17.66

15 https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/national-and-regional-populations/population-of-england-and-wales/latest accessed 24.viii.22

16 As shown below, the questionnaire allows categories "Third gender / non-binary" and "Prefer not to say". Both were 0 for the whole 500 respondent cohort.

17 https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/demographics/male-and-female-populations/latest accessed 24.viii.22

18 Minimum 19, Maximum 81

19 https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/demographics/age-groups/latest accessed on 24.viii.22

77 or over	4	0.85

2.3.1.2. General Feedback

The questionnaire including a free-form comment box at the end to capture any general thoughts. 49 comments were left; 26 were 'none' or equivalent (e.g., 'thanks'). Of the rest, respondents found:

- Thank you, the study was thought-provoking
- Very well thought out and thought provoking questionnaire
- A very topical study given the times we now find ourselves in...

The questionnaire was well received, therefore.

- I work in the InfoSec industry and I can say our footprint we leave online is being harvest by big tech giants like google, Microsoft, apple, other telecom companies
- most data about people is surface material, every time i go into a company i reject all cookies and every night i clear all cookies plus other data from my computer, and occasiona;;y i shut mu [sic.] computer and clean all programmes, it probably just makes myself feel better.
- My data is lost or stolen in breaches about tice [sic.] a year, that i'm aware of !
- Data has become so important in the world today because of its application to various aspects of life. It is sought after more now than ever.

Even to the extent that some are aware that personal data has already become so important that we seem to have to go to extreme lengths if we want to protect it. This seems to echo Item 4 in Section 2.2.1. Given how breaches are reported and an acceptance that personal data *are* desirable with commercial value, the general public are almost lost and rely on their own (subjective) strategies.

- The only data I really worry about is my financial data, I don't really care if other types of data (age, location, consumer preferences etc) are tracked.

Not everyone is concerned about the types of data that are require additional protection, that is *special category personal data*, but rather with data they see having a tangible impact on the data subjects. To some degree, this reflects the *pragmatism* reported in the workshops (see Items 2 and 3 in Section 2.2.1).

- Totally agree that the data protection paragraphs are not understood by myself or most other users
- we all need to be careful about sharing data and to take the time and trouble to find out relevant things before sharing data

There is an appreciation that the data subject has a responsibility to protect their own data, but perhaps a frustration that doing so is not easy. This was already evidenced in the workshops: participants recognise they have their part to play, but don't necessarily know how to respond or indeed what is available to them (Items 1, 3 and 5, Section 2.2.1).

- Shouldn't have to create accounts to buy things giving info and should be able to opt out of everything easily. Like all legal wording, they are so long nobody reads
- some investigation into why, after setting your preferences for someone like amazon or your bank, a few weeks later you are required to set them again, it's almost as if we're being bullied into [accept all] so companies have a free hand

- Usually the choice is to agree to the privacy notice or not use the site. There is no scope for negotiation about how my data is used.

The frustration extends to current practices which may be seen as weighted ***against*** the data subject. See items 1, 5 and possibly 3 from Section 2.2.1: like the workshop attendees, there is a general concern about being overwhelmed currently and a call for greater simplicity and transparency.

Although not everyone left a specific comment about the subject matter of privacy, there is evidence that views identified in the workshops may well reflect the concerns of the general public. For workshop participants and for members of the general public who commented here, there's a call for greater transparency, making data protection easy and directed towards the data subject and their level of understanding.

2.3.1.3. General Views on Data Sharing

The questionnaire included four general statements each with three options describing a group or circumstance related to the general statement. Respondents used a graphical slider to identify the agreement with the statement as it relates to the group or circumstance. The results are summarised for the 470 respondents in Table 5.

Table 5: General Views on data sharing relating to groups who might receive the personal data or the circumstances of the data sharing

How likely am I to share my information with (*extremely unlikely* to *extremely likely*)		
Retailers	Researchers	Government
53%	***64%***	59%
How do I decide to share my data? (labelled from *never* to *always*)		
I read the privacy notice	If I trust the organisation asking for my data	I just get on with what I'm doing and don't worry about privacy
43%	***61%***	47%
When deciding to share my data, I worry about (labelled from *not at all* to *a lot*)		
Organisations sharing my data with third parties	Researchers using my data for whatever they like	My data being used to make decisions about me or for me
73%	49%	63%
In general, I am concerned when sharing my personal data by (labelled from *not at all* to *completely*)		
The security of the data I contribute	The anonymity of the data I contribute	The onward sharing of the data I contribute
64%	60%	**73%**

In the case of *How likely [someone is] to share [their] information*, for instance, respondents reported that they are 53%, i.e., just above 50-50, to share data with a retailed; 64% - a little over 6 cases in 10 - with a researcher and 59% - a little shy of 6 cases in 10 - with the government.

From how respondents answered these questions, there is some evidence that private citizens base sharing decisions on a subjective response (trust 61% in response to *How do I decide…?*) rather than objective and formalised processes such as privacy notices. *Research* is generally well-perceived, by comparison to *retail*. Most importantly, though, the general public are most concerned about the onward sharing of their data, rather than specifics of the infrastructure (64% for '*The security of the data I contribute'*, and 60% for its anonymity; 63% for profiling or modelling, and 43% for research uses other than originally defined).

Regarding the 5 Safes (see Section 3), private citizens are therefore most concerned about Safe outputs (what will happen to their data) and possibly Safe people. The procedures around security and compliance are less important, perhaps, in that existing structures which provide details and allow individuals to assert their rights if they are concerned seem to be regarded either as overcomplicated, or weighted against them and in favour of the service provider / researcher.

2.3.1.4. Privacy Concerns: Responses to Assertions

To establish how the general public responds to the assertions of the questionnaire and therefore whether the views expressed by PRAF participants are a fair representation of the views of the general public:

- *Strongly agree* and *Somewhat agree* were summed and are reported in the following tables as **Agree** (see Table 6)
- *Strongly disagree* and *Somewhat disagree* were summed and are reported as **Disagree** (see Table 7)
- *Neither agree nor disagree* are reported as **Neutral** (see Table 8)

Where the assertions have been reverse-coded are highlighted as ***bold italic***. Thus, for *I don't need to be involved in any decisions about my data*, 88.06% disagreed with the assertion. By inference, the 88.06% would agree with the opposite assertion: *I need to be involved in any decisions about my data*. Assertions have been categorised as ***Agree*** *or* ***Disagree*** where the score represent values above 66%[20].

Assertions are shown in the table ordered by the percentage agreement except Table 8 showing the *Undecided* responses where percentages are ordered from high to low irrespective of *Agree, Disagree* and *Neutral*. The first column in each table identifies a construct from Figure 2 as follows:

B	Barriers	What gets in the way of sharing or controlling their data
C	Context	The domain in which data sharing may occur
KE	Knowledge / Experience	Individual's past experience and /or what they know about a given context
P	Pragmatism	Motivators specific to an individual occasion
R	Responsibility	Who controls the data / decision to share data

These constructs are listed for reference only and to provide a link back to the qualitative analysis reported above (see Section 2.2 and Figure 2). Further analysis of responses may provide insights any structure in the data. In turn, this may also provide subscales to allow for the release of the questionnaire as a standard privacy attitudes instrument.

[20] 66% would represent two-thirds agreement.

Agreement

Table 6 lists the 24 statements[20], or half, that two-thirds of participants in the online survey rated as *Strongly agree* and *Somewhat agree*.

*Table 6: Assertions that private individuals **agree** with*

	Assertion	Agree	Neutral	Dis-agree
R	Companies should be transparent about how they use data and who they share them with	95.96%	2.55%	1.49%
R	I should be asked before my data is used for a purpose I didn't originally agree to	94.89%	3.83%	1.28%
R	An independent authority should check that companies comply with the law	93.83%	4.04%	2.13%
C	***I [don't] need to be involved in any decisions about my data***	88.06%	6.61%	5.33%
R	Individuals responsible for breaches should be held accountable	88.03%	8.33%	3.63%
B	Technology should be developed to help us manage our data	87.66%	8.94%	3.40%
B	If my data is stored by a third party, the risk to my privacy increases	87.21%	10.23%	2.56%
C	Data for research should be anonymous and deleted when the project is finished	85.32%	9.36%	5.32%
R	The company I share my data with is responsible for my privacy	85.07%	9.59%	5.33%
B	I don't believe that firms always tell me what they're doing with my data	83.80%	8.53%	7.68%
R	The Government should be doing more to help people understand privacy and data sharing	83.37%	11.73%	4.90%
B	Companies deliberately make their privacy notices long and complicated so I won't read them	83.16%	9.81%	7.04%
KE	I feel I should be able to change the data that is stored about me	81.70%	15.11%	3.19%
KE	I don't always understand what made a company think I want their product or service	72.13%	14.68%	13.19%
B	I feel overwhelmed by all the regulations	72.13%	15.96%	11.91%
R	Companies who hold data have an ethical responsibility to use the data for the common good	71.91%	18.09%	10.00%
P	Everyday life is too fast to take time to understand all the choices and settings for privacy	71.28%	13.62%	15.11%

	Assertion	Agree	Neutral	Dis-agree
B	I feel decisions are being taken about me or for me without my knowing	71.28%	19.15%	9.57%
B	I feel overwhelmed by all the choices I have to do with privacy	70.15%	14.50%	15.35%
B	I don't have time to read all the information to help me decide when sharing my data is safe	69.57%	15.53%	14.89%
B	The younger generation are often tricked into giving their data because they want to do something	68.09%	23.82%	8.09%
P	Trying to understand all the privacy settings gets in the way of what I want to do online	67.95%	15.17%	16.88%
B	***I am [not] concerned by media coverage of data breaches or losses***	67.66%	17.23%	15.11%
C	If I use a service operating in a different country, different rules apply	67.23%	24.04%	8.72%

To a large extent, they agree with the original PRAF workshops. Specifically, data subjects:

- Do not understand their rights or the structures in place to support them
- Are concerned about the onward sharing of their data and their loss of control over their data
- That regulation is
    - too complicated,
    - has an adverse effect on research, and
    - there needs to be official (e.g., government) support to understand the context of data sharing.

What is perhaps most significant is that participants acknowledge they don't have enough time to seek out all of the relevant information to make an informed decision. Data sharing decisions are made in spite of regulation ("*Companies deliberately make their privacy notices long and complicated so I won't read them*", "*Everyday life is too fast to take time to understand all the choices and settings for privacy*", etc.), despite concerns about potential data breaches ("*I am [not] concerned by media coverage of data breaches or losses*"), and there is little practical appreciation of data subject rights ("*I should be asked before my data is used for a purpose I didn't originally agree to")* or even the regulatory structures in place to help protect data subjects ("*An independent authority should check that companies comply with the law*"). If private individuals will not take time to assess risk as presented in a privacy notice or PIS partly because there is too much information to process in time, there is clearly a disconnect between legislators and private individuals.

Disagreement

Table 7 lists where participants (members of the general public) disagreed with statements taken from the workshops[21]: only three out of the 48 assertions.

*Table 7: Assertions that private individuals **disagree** with*

[21] Note that this does not mean they disagree with PRAF members in the workshop. The statements were simply generated from the discussion at those workshops.

	Assertion	Agree	Neutral	Dis-agree
R	If a company or researcher uses my data that's different from what they said originally, they don't have to tell me	5.74%	10.64%	83.62%
C	Social networks need to sell my data so that they remain free	16.84%	13.86%	69.30%
B	If I agree to let a company or researcher use my data, I no longer have any rights to it	16.17%	15.11%	68.72%

In general, despite suggestions that data protection is not completely understood in Table 6, participants have some understanding that personal data may not simply be re-used or shared with others. More than two-thirds (68.72%) appear to believe they still have rights, and an overwhelming 83.62% claim they should be told if data are to be used for different purpose than originally agreed. It is unclear, therefore, whether they understand the legislation, but don't engage (i.e., by reading privacy notices), or they really don't understand the legislation even though they claim to (i.e., they don't understand their rights).

Undecided

Table 8 lists the 21 assertions where members of the general public who responded to the questionnaire showed ambivalent responses (i.e., less than two-thirds *agreed* or *disagreed* or remained *neutral*).

*Table 8: Assertions that private individuals were **undecided** about*

	Assertion	Agree	Neutral	Dis-agree
P	I just want to get done whatever it is, and so don't take time to read through all the privacy settings	65.74%	15.11%	19.15%
B	It worries me that I don't know enough to make informed decisions about my data	65.03%	18.98%	15.99%
B	I can't stop my data being shared	61.41%	19.62%	18.98%
R	Organisations like the NHS should not be penalised for data breaches as much as commercial companies	24.04%	14.89%	61.06%
KE	I don't know how to request access to my data	59.15%	15.11%	25.74%
R	I share responsibility for my data with whoever I release it to	58.33%	23.72%	17.95%
B	I am concerned about my data being processed with advanced technology	58.30%	23.83%	17.87%
KE	***Generally data protection regulations are [mis]understood***	9.38%	33.05%	57.57%
KE	I will only share my data with people I trust	53.83%	30.43%	15.74%
B	I feel I'm being watched when I'm online	52.67%	22.39%	24.95%

	Assertion	Agree	Neutral	Dis-agree
B	***I [don't] always know how data is stored and shared after a research study***	49.79%	20.00%	30.21%
KE	It's acceptable to share my data for the common good (like during COVID)	48.93%	24.57%	26.50%
KE	I believe the NHS sells my data without my permission	23.03%	29.21%	47.76%
R	I feel I make informed choices about privacy and data sharing	46.06%	30.28%	23.67%
C	Younger people are more tech-aware and so can look after themselves better	45.32%	24.68%	30.00%
P	I am not so careful about sharing data when shopping online	44.78%	21.96%	33.26%
KE	I can still be identified from anonymous data	44.23%	31.41%	24.36%
KE	Data protection regulation has a negative effect on research	15.57%	42.64%	41.79%
R	I am always responsible for my own data	42.34%	30.00%	27.66%
B	***I [don't] always understand the language when I'm being asked to give consent***	40.09%	17.91%	42.00%
B	***I [don't] keep control over data I provide as part of a research study***	29.85%	31.13%	39.02%

Here, there are clearly differences of opinion: roughly 42% both agree and disagree that *Data protection regulation has a negative effect on research*, for instance; and around 40% agree and disagree with *I [don't] always understand the language when I'm being asked to give consent.* At the same time, more than 60% agree with statements like "*I just want to get done whatever it is, and so don't take time to read through all the privacy settings*" (i.e., their motivation is transaction led), acknowledge they don't make use of all available information, "*It worries me that I don't know enough to make informed decisions about my data"* (i.e., they acknowledge that data controllers provide information, but they are not sure what is and isn't relevant), and even that they may be willing to disclose personal data even though they have no control ("*I can't stop my data being shared*"). Intriguingly, more than half (53.83%) agree and almost a third are equivocal about (30.43%) data sharing based on trust: "*I will only share my data with people I trust*". In the classic, social psychology sense, there is some indication therefore that people accept they are exposing themselves to vulnerability (Mayer et al., 1995; Rousseau et al., 1998)

The PRiAM privacy risk assessment framework helps service and infrastructure providers demonstrate regulatory compliance and risk mitigation processes. However, there is still some way to go before all data subjects use the available information to engage. As previously noted, there is scope in future to investigate the implications of private individual perspectives on privacy and how this might affect a privacy framework.

2.4. Comparison with Expert Perceptions

PRiAM also engaged with domain experts to create an Advisory Board in WP2 as documented in PRiAM report D2. The Advisory Board made a set of recommendations about privacy risk assessment and what they expected from a trusted research environment. For example, one of the recommendations from the Advisory Board states:

> An ideal risk assessment framework should be able to help communicate the process to non-experts and provide guidance to smaller organisations that are looking for advice regarding best practices

"Guidance to smaller organisations" is clear and a significant motivation for a privacy risk framework. Further, "communicat[ion] to non-experts" is also echoed in the ICO call for privacy notices to "to explain these points in writing in a way that's easy for people to understand"[6]. In Section 2.2.1, however, there is evidence that data subjects:

- Do not understand the current structures
- Struggle to understand all of the regulations
- Believe they need more help
- Don't always read (and understand) all of what they are told

The Advisory Board recommendation around communication with non-experts is therefore of high priority.

They also made the recommendation that:

> Understand the reasonable expectations of data subjects even if the processing has a clear legal basis

Something again echoed in the ICO guidance on privacy notices. Along with the comment that financial data and not special category data may be more important[22], data subjects do not believe:

- or understand that they retain some control (and rights)
- they can influence what happens to their data
- they can prevent the onward sharing (or sale) of their data

The Advisory Board recommendation about understanding data subject understanding should begin with an appreciation of what they (*data subjects)* currently believe.

The *legal basis* needs some thought. Although some respondents believe themselves and others in general to understand the legislation, it is unclear that they understand *consent*. As a legal basis, except under exceptional circumstances this gives them the right to require removal of data they are concerned is being used for unexpected purposes or by a third party[23].

Further, the Advisory Board mentions:

> Beyond concerns of re-identification[24], we need to think about the actual perceived harms and what else can be learned from the data

From responses received to the questionnaire, data subjects:

- are concerned that they are monitored and "profiled", especially via advanced technology
- do not believe they can influence

---

[22] "The only data I really worry about is my financial data, I don't really care if other types of data …"

[23] See, for instance, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ accessed 24.viii.22

[24] Incidentally, one of the recommendations from PRAF in workshop 4 was that the term "de-identification" should be replaced with "anonymisation". Although not technically equivalent, this does reinforce that the language may unwittingly be misunderstood.

- how their data are used
- who their data are shared with

The Advisory Board recommendation about understanding perceived harms (from the data subject's perspective) should include considerations both of being transparent about any additional processing and about data subject rights.

Finally, and although not completely agreed by the Advisory Board, reference was made to:

> Role of institutions/affiliations in trust/taking liability on behalf of individuals / determining the "safe" people …

Data subjects appear to:

- make data sharing decisions on the basis of trust (in the classic sense (Rousseau et al., 1998)) not contract, i.e., the 'lawful basis'
- be particularly concerned about the onward sharing of their data
- believe that they have no control ("responsibility") over their data once released to someone else (who then has complete control)

The Advisory Board comments on trust and responsibility should be understood in the context of data subject decision making (*based on trust, therefore an acceptance of vulnerability*) and responsibility (*i.e., who can make decisions about their data*).

As well as the recommendations of the Advisory Board, there are clear indications that the ICO guidance on privacy notices should be reviewed. For instance, though the ICO recommend a clear explanation of:

> people's information rights, including the right to withdraw consent, where that's your lawful basis (*loc. cit*)

The results of the questionnaire seem to indicate that data subjects may *believe* themselves informed, but it is clear from other observations that they do not understand their rights or how to exercise them.

2.5. Recommendations

Data sharing decisions reported here suggest there should be personal contact between participant and researcher / TRE operator. This is different from current practice based on privacy notices and / or participant information sheets. However, the evidence here suggests that:

- Data sharing is not based on informed consent;
- Data sharing is instead context-specific; and
- May be more akin to the social construct of interpersonal trust.

From the PRiAM PRAF workshops, the questionnaire and the recommendations from the PRiAM Advisory Group of domain experts, themes supporting a more interpersonal approach emerge:

- What individuals claim regarding data protection legislation will be influenced by the specific context, what similar others[25] say and think, and by what they perceive about a situation (i.e., what they want to achieve and how they can achieve it).

[25] The concept of 'similar others' or 'trusted others' refers to those individuals believe they share common traits and aspirations, i.e., their ingroup (see Giles, H., & Giles, J. (2012). Ingroups and outgroups. In A. Kurylo (Ed.), *Inter/Cultural communication: Representation and construction of culture.* (pp. 141-161). Sage Publications. http://www.sagepub.com/upm-data/48648_ch_7.pdf)

- Individuals may become overwhelmed by the amount of information (e.g., *privacy notice*) they are presented with especially if it interferes with their goals. The structures may be there, but they may not use them to make fully informed decisions.
- Individuals must believe that the risk to their privacy is relevant to them specifically and that they are responsible for dealing with it: they will then respond to perceived threat. Additionally, though, they need to feel that they are *capable* of acting appropriately to achieve their perceived privacy goals.
- How individuals decide to engage with a TRE – and share their data – may derive from different mechanisms than how regulators and domain experts evaluate the TRE and their privacy structures. Motivation to participate (and share data)

These suggest the following recommendations as a starting point:

- Privacy notices should be designed to be user-friendly rather than just legally compliant.
    - They should be brief and explicit about what rights a data subject has
    - They should indicate accessible, independent resources that are available when making decisions to share data.
- When individuals are asked to decide about privacy (i.e., privacy settings, cookie choices, and so forth), this should be
    - context aware to avoid users simply ignoring them and by default agreeing to data donation.
    - sensitive to reputation
    - any current cases being reported in the press
- We should reconsider how participation in research or clinical trials might be negotiated with participants. Taking the lead from medical ethics, it is perhaps time for ongoing negotiating of data use (Muirhead, 2011; Rubin, 2014).

3. General Reflections

The purpose of the investigation summarised in this report was to identify privacy perceptions of representative members of the general public. The general assumption for models such as the Five Safes is that the characteristics of a TRE, for instance, such as its governance structures are sufficient to encourage engagement with it, that is data sharing. Although the recommendations of the Advisory Board include the clear communication of processes to the non-expert (i.e., the general public), engaging with the PRAF and the general public with a general privacy attitude questionnaire, has revealed a different perspective. For instance, although respondents to the survey claimed to be informed, they were not clear about their rights as data subjects, nor that regulatory procedures are already in place to protect those rights, not least against the onward sharing of their data.

The general public therefore seem to make decisions to share data based on other criteria than specifically a privacy risk assessment akin to compliance with the Five Safes however well communicated. For example, in both the workshops and the survey, participants reported that they may make a decision to share data based on *trust*. In behavioural terms, trust is an acceptance of vulnerability based on perceptions of the trustworthiness characteristics of the would-be trustee and not the reliance on a contractual relationship like regulatory compliance (see also Luhmann, 2000). These trustworthiness characteristics are generally assumed to be:

- *integrity* – the trustee behaves in a way which the trustor believes to be appropriate
- *competence* – the trustee is able to do what the trustor expects, and
- *benevolence* – the trustee adopts a positive, beneficial attitude to the interests of the trustor;

(see Mayer et al., 1995; Rousseau et al., 1998; Schoorman et al., 2007). This suggests a social constructionist underpinning for engagement with a TRE, which has also been discussed in relation to AI (Rohlfing et al., 2020) and

consent (Pickering, 2021). In the next three sections, we contextualise the findings here within what is known from social psychology.

3.1. Risk Perception in general

From the literature, risk perception is assumed to result from the integration of emotional as well as more rational evaluation of what they are presented with (Paek & Hove, 2017). Looking at general risk perception, risk assessment is assumed to be a rational, measured process for experts, but more affect-driven for private individuals (Paek & Hove, 2017). Further, if individuals are to respond and apply measures to mitigate risk – such as take responsibility for the privacy of their data – they must perceive that they have a personal motivation to do *and* that this is not something with more general implications requiring attention from another (Paek & Hove, 2017; Tyler & Cook, 1984). It's possible therefore that the private individuals responding to our questionnaire do not believe themselves capable or directly responsible to take measures to reduce the privacy risk to their data (see also Acquisti et al., 2015).

Despite the availability of information, there's no guarantee that individuals will process it all (Smerecnik et al., 2012). Similarly, respondents reported that they were aware of privacy notices and regulations but did not demonstrate the consequences of the rights associated with them. Affect (Barrett & Bliss-Moreau, 2009) is known to influence judgement: a positive emotional state will reduce the perceived risk and conversely inflate perceived benefit (Finucane et al., 2000; Loewenstein et al., 2001; Slovic et al., 2004). At the same time, too much information might overwhelm (Bada et al., 2015), leading to an inability to act (Witte, 1992; Witte & Allen, 2000). There is evidence here that individuals do feel overwhelmed, or at least that they have other priorities because of time pressures or simply wanting to complete a transaction immediately.

What we know less about at this stage relates to individual differences. This is important as suggested by general behavioural models. The personal disposition of individuals is known to influence a willingness to respond to risk perceptions, for instance: where a risk is perceived to be high, coupled with low self-efficacy (the belief in one's own ability to act), they become *avoidant* and do not act. This may explain the assertion that they know about the legislation and so forth but feel overwhelmed about doing anything. Conversely, even if the risk is perceived to be high, if self-efficacy is also high, then they will take appropriate steps to mitigate the risk (Rimal & Real, 2003).

3.2. Privacy Concerns: *revisiting Westin*

Empirical work has already been reported which seeks to identify the privacy attitudes of the general public. Although situated specifically within marketing, traditionally members of the public[26] are categorised as one of three types regarding their willingness to share data (Westin, 2003):

1. *Privacy fundamentalists*: those who are very concerned and will always take measures to understand and protect their privacy
2. *Privacy pragmatists*: those who will adapt their attitude to the current situation
3. *Privacy unconcerned*: those who don't really care much about privacy.

Notwithstanding potential cultural differences as well as different regulatory contexts between the United States and the UK (Bennett, 2018; Cath et al., 2018), we have previously seen similar categories of reported behaviour regarding technology use and the spread of misinformation in a post-truth age (Pickering et al., 2020). If such categories are valid, then we would expect to see them represented in our engagement with the general public as part of PRiAM independently of the privacy controls in place. For example, some will report reading a privacy notice very carefully (the *privacy fundamentalists*), while others will not (the *privacy unconcerned*). Notwithstanding

[26] Specifically in the United States of America

context differences[27], if the Westin typology is assumed to be robust and more generally applicable, we would expect that the different types to emerge in the frequency distributions of some of the answers to the questionnaire. For instance, if we look at responses to the last two statements in Table 5, we would expect *privacy fundamentals* to group towards the higher end of the concern scale (towards 100% or "A lot" or "Completely"); *privacy unconcerned* respondents would group instead to the low end of the scale (lower percentages or "Not at all"). The frequency distributions would tend towards bimodal, therefore. The *privacy pragmatists* may appear anywhere along the scale, exaggerating one or other modal peak, or flattening the distribution.

To test this, consider first responses to the statement: *When deciding to share my data, I worry about.* Figure 4 shows the frequency distributions, with the abscissa for each panel showing the extent of concern: values to the right would be associated with increased concern or "A lot", to the left with little concern, tending towards "Not at all". The ordinate shows the frequency a given percentage was selected by the 470 respondents.

There is no clear evidence for a bi- or multi-modal distribution for any of three contexts. The bottom panel, concerning data being used for automatic decision-making, *may* tend towards a flattened distribution reflecting a less homogeneous cohort. However, there is little clear-cut evidence to support this.

[27] The Westin studies are targeted towards privacy within the use of personal data for marketing in the USA, whereas here we have identified privacy concerns of typical private citizens in the UK across different contexts.

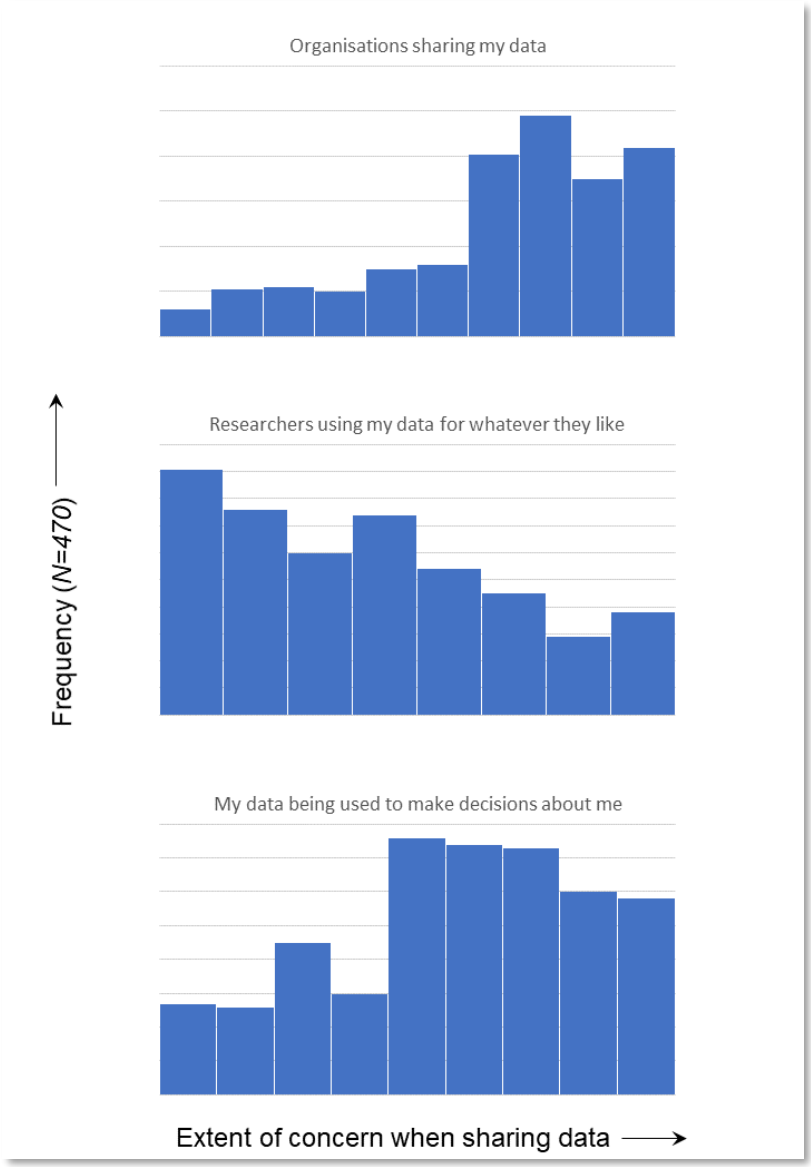

Figure 4: Frequency distribution for responses to the statement When deciding to share my data, I worry about...

By contrast, the top and middle panels are negatively and positively skewed respectively. Therefore, in response to the idea of organisations sharing personal data, responses bunch towards a significant level of concerns towards the right. ***Private citizens do not want their data shared.*** Similarly, in the middle panel, responses bunch towards the low end: ***Private citizens are not very concerned with the secondary use of their data by researchers.***

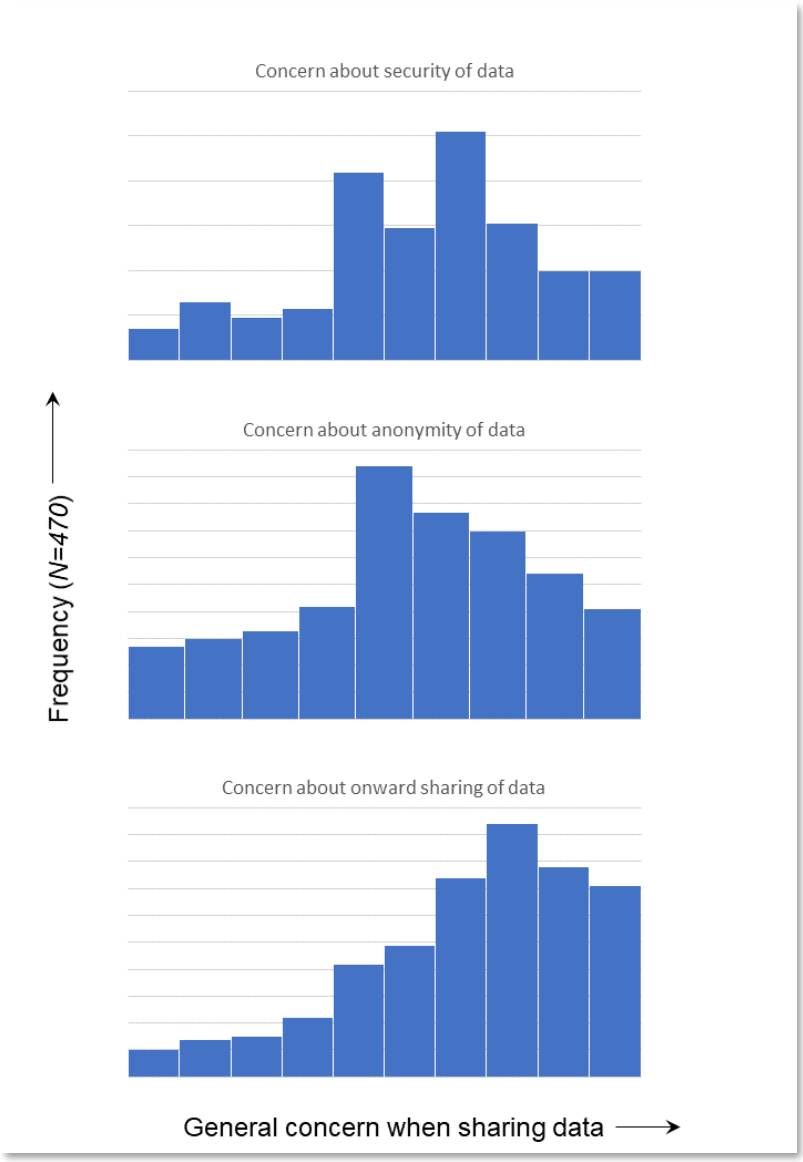

Figure 5: Frequency distribution in response to the statement In general, I'm concerned when sharing my personal data by…

A slightly different, though complementary picture emerges in response to *In general, I'm concerned when sharing my personal data by…* (Figure 5). There is *some* indication of a bimodal distribution in the top panel relating to the security of data. This may reflect differences in respondent awareness and experience with security. The modes, we suggest, are too close to suggest a Westin-style difference among respondents, though.

The bottom panel concerning data sharing confirms what is shown in the top panel of Figure 3 towards the "Completely" end of the scale validating that ***Private citizens are concerned about their data being shared***. The middle panel of Figure 4approaches a normal distribution. This suggests an equivocal response to anonymity: *some* (perhaps the majority) people are concerned, the rest are not.

Overall, though, there is little evidence ***in this part of the questionnaire*** that individual citizens conform to the Westin categories regarding privacy concern (though see Section 2.3.1.4 and the *Undecided* responses). Instead, and validating what was found in the workshops with the PRAF, they are uniformly and consistently concerned about the onward sharing of data. From Table 5, there is some indication that they base sharing decisions on trust rather than an objective evaluation of trustworthiness operationalised by policies or regulation. Indeed, the latter

seem to overwhelm the data subjects. Further, there is evidence that research is likely to encourage data sharing, but retail less so.

3.3. Behavioural Interpretation of Results

The main results from engagement with the general public via the workshops and the online questionnaire may be summarised as follows:

- ***Private individuals may be overwhelmed by the amount of information they believe they are expected to process to make privacy decisions***

  This type of response has been well-attested in the literature. For instance, Witte developed a behavioural model which describes a dual path in response to the perception of risk. So long as individuals believe they are in control – for instance, self-efficacy is high – then they will adopt suitable behaviours, such as making appropriate decisions to ensure the privacy of their own personal data. If this is not the case – for instance, when they believe they are unable to act – then they will not act at all or act in a way which may exacerbate risk (Witte, 1992; Witte & Allen, 2000). Therefore, as reflected in the Recommendations, it is not enough to comply with regulation in terms of privacy notice or participant information sheets and then assumed individuals are making informed decisions about sharing their data.

- ***There is an apparent contradiction between what private individuals claim (****e.g., that they understand regulation****) and what they believe or actually do (****e.g., the belief they have no control over data once shared****)***

  In behavioural terms, this has strong parallels with the discrepancy between the intention to act (e.g., to review a privacy notice or participant information sheet) before acting (i.e., making an informed decision about data sharing). This goes back to models of planned behaviour (Ajzen, 1991, 2011; Ajzen & Fishbein, 2005) and derivatives (see, for example, McKnight et al., 2011; McKnight et al., 2009), as well as specific research around the intention-behaviour gap (Sheeran & Webb, 2016). There are at least two different interpretations for the thematic analysis of the workshops and the online questionnaire, assuming that participants are not being dishonest. First, that they have decided to act based on invalid assumptions: they have read the regulations but have misinterpreted them. To address this would mean that operators of a TRE, for instance, would need to focus on what data donors understand about sharing their data. This is the clear communication that was highlighted by the Advisory Board as well as the constructs leading up to the *Context* in the thematic map in Figure 2. Secondly, this may instead mean focusing on the *motivation* to go from intention to action. That appears to be based on *trust* in the researchers or operators of the TRE, though there are additional behavioural models which would explain this (Deci & Ryan, 2000; Ryan & Deci, 2000a, 2000b).

- ***Concern about privacy does not necessarily predict data sharing behaviours***

  One specific discrepancy between intention and behaviour is the so-called privacy paradox: in particular, individuals claim to be concerned about privacy and yet share personal and sensitive data freely (Barth & De Jong, 2017; Dienlin & Trepte, 2015). Acquisti and his colleagues criticise the assumptions that regulation empowers individuals instead focusing on different motivators (Acquisti, 2012; Acquisti et al., 2015). There is also evidence from the PRAF workshops and the online questionnaire that private individuals make some sharing decisions based on task (e.g., retail goals) or trust (i.e., an acceptance of vulnerability, particularly in a research context; see Table 5). As in the previous case (a discrepancy

between intention and action), this needs further investigation and is consistent with Advisory Board recommendations about data subject / participant expectations[28]. The work reported here already provides a basis to explore this further.

3.4. Behavioural insights: *Concluding Remarks*

In this section, we have considered three main research strands from social psychology: general perceptions of risk, Westin's privacy categories, and behavioural models in general and specifically as they relate to data sharing. In the first instance, the themes and perspectives highlighted by the PRAF workshops and derived questionnaire are consistent with what is known from the behavioural sciences as shown. This also foregrounds a need to consider the perspectives of data subjects (in data protection terms) or participants (more generally) making decisions to share their data. Although we have focused here on data protection as one of the major themes participants brought up in the PRAF workshops, this emphasis on the data subject / participant brings back into focus the ethical perspective of data exploitation (Carroll et al., 2020) and participation (Antonia Vlahou et al., 2021; Hand, 2018)[29]. The DARE UK PRiAM project therefore provides empirical evidence to support this focus.

4. Conclusion

This report has documented engagement with private individuals within PRiAM as representatives of the general public in recognition of their role as significant stakeholders for institutions such as trusted research environments who need or ask for personal data. This included a set of workshops with a PRAF to explore privacy perceptions and concerns. The workshop discussions led to the development of an anonymous questionnaire which was distributed to the general public (500 respondents). The questionnaire largely validated the results from the PRAF workshops, suggesting that the privacy attitudes apply to the general population.

The results of engagement with the privacy attitudes of private individuals led to an exploration of well-known behavioural models to explain perceived behaviours. Further, it was suggested that although the privacy risk framework provides service and infrastructure providers with a mechanism to demonstrate trustworthiness to potential users (i.e., private individuals as data subjects), to motivate the public's engagement would need to ensure they do not feel overwhelmed (in terms of effort required), but instead get a sense of belonging with other users and with the service provider in their management of privacy.

This report therefore complements other PRiAM deliverables. Additionally, it has provided empirical data (in terms of public responses to recognised privacy issues) to be investigated further in support of public engagement involving the sharing of their personal data.

[28] For instance: "Understand the reasonable expectations of data subjects even if the processing has a clear legal basis" and "… we need to think about the actual perceived harms …"

[29] Note: the PRiAM Advisory Group do make a recommendation on research ethics, though this is specifically about governance and oversight rather than more general ethical principles such as autonomy and equanimity.

5. Appendix: Final Questionnaire

Each of the slider questions (number Q2.1, Q3.1, Q4.1, and Q5.1) has the form:

The twelve assertions in each section (Q2.2, Q3.2, Q4.2 ad Q5.2) are randomised.

Q2.1 **How likely am I to share my information with**

Options: Online retailers, Researchers, the Government
Slider: 0 -100, *end points*: Extremely Unlikely, Extremely Likely

Q2.2 **Please read the following statements and tell us whether you agree or not**

An independent authority should check that companies comply with the law

Data protection regulation has a negative effect on research

Social networks need to sell my data so that they remain free

Technology should be developed to help us manage our data

I keep control over data I provide as part of a research study

I don't need to be involved in any decisions about my data

Everyday life is too fast to take time to understand all the choices and settings for privacy

I don't have time to read all the information to help me decide when sharing my data is safe

I share responsibility for my data with whoever I release it to

It worries me that I don't know enough to make informed decisions about my data

I believe the NHS sells my data without my permission

I feel overwhelmed by all the choices I have to do with privacy

Q3.1 **How do I decide to share my data?**

Options: I read the privacy notice, If I trust the organisation asking for my data, I just get on with what I'm doing and don't worry about privacy
Slider: 0 -100, *end points*: Never, Always

Q3.2 **Please tell us if you agree with the following views**

Companies deliberately make their privacy notices long and complicated so I won't read them
I am not concerned by media coverage of data breaches or losses
Data for research should be anonymous and deleted when the project is finished
I don't always understand what made a company think I want their product or service
I feel decisions are being taken about me or for me without my knowing
I just want to get done whatever it is, and so don't take time to read through all the privacy settings
Individuals responsible for breaches should be held accountable
The Government should be doing more to help people understand privacy and data sharing
I feel I'm being watched when I'm online
Trying to understand all the privacy settings gets in the way of what I want to do online
I always understand the language when I'm being asked to give consent
Generally data protection regulations are misunderstood

Q4.1 **When deciding to share my data, I worry about**

Options: Organisations sharing my data with third parties, Researchers using my data for whatever they like, My data being used to make decisions about me or for me
Slider: 0 -100, *end points*: Not at all, A lot

Q4.2 **And now, how correct do you think the following statements are**

Younger people are more tech-aware and so can look after themselves better
Companies should be transparent about how they use data and who they share them with
I can still be identified from anonymous data
If a company or researcher uses my data that's different from what they said originally, they don't have to tell me
I always know how data is stored and shared after a research study
I will only share my data with people I trust
I feel I make informed choices about privacy and data sharing
I am not so careful about sharing data when shopping online
Companies who hold data have an ethical responsibility to use the data for the common good
The company I share my data with is responsible for my privacy
The younger generation are often tricked into giving their data because they want to do something
I am concerned about my data being processed with advanced technology

Q5.1 **In general, I am concerned when sharing my personal data by**

Options: The security of the data I contribute, the anonymity of the data I contribute, the onward sharing of the data I contribute
Slider: 0 -100, *end points*: Not at all, Completely

Q5.2 **Finally, have a look at the following and tell us what you think**

I feel I should be able to change the data that is stored about me
I don't know how to request access to my data
I feel overwhelmed by all the regulations
I should be asked before my data is used for a purpose I didn't originally agree to
I am always responsible for my own data
If I agree to let a company or researcher use my data, I no longer have any rights to it
I don't believe that firms always tell me what they're doing with my data
If I use a service operating in a different country, different rules apply
Organisations like the NHS should not be penalised for data breaches as much as commercial companies
If my data is stored by a third party, the risk to my privacy increases
I can't stop my data being shared
It's acceptable to share my data for the common good (like during COVID)

6. References

Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. *Digital Enlightenment Yearbook 2012*, 193-197. https://doi.org/10.1109/MSP.2009.163

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & health*, *26*(9), 1113-1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I., & Fishbein, M. (2005). The Influence of Attitudes on Behavior. In D. Albarracín, B. T. Johnson, & M. P. Zanna (Eds.), *The handbook of attitudes* (pp. 173-221). Lawrence Erlbaum Associates Publishers.

Antonia Vlahou, Dara Hallinan, Rolf Apweiler, Angel Argiles, Joachim Beige, Ariela Benigni, Rainer Bischoff, Peter C. Black, Franziska Boehm, Jocelyn Céraline, George P. Chrousos, Christian Delles, Pieter Evenepoel, Ivo Fridolin, Griet Glorieux, Alain J. van Gool, Isabel Heidegger, John P.A. Ioannidis, Joachim Jankowski, . . . Vanholder, R. (2021). Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics? *Hypertension*. https://doi.org/https://doi.org/10.1161/HYPERTENSIONAHA.120.16340

Bada, M., Sasse, M. A., & Nurse, J. R. (2015, 26 Feb 2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* International Conference on Cyber Security for Sustainable Society, Coventry, UK.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122. https://doi.org/10.1037/0003-066X.37.2.122

Bandura, A. (2012). On the Functional Properties of Perceived Self-Efficacy Revisited. *Journal of management*, *38*(1), 9-44. https://doi.org/10.1177/0149206311410606

Barrett, L. F., & Bliss-Moreau, E. (2009). Affect as a Psychological Primitive. *Adv Exp Soc Psychol*, *41*, 167-218. https://doi.org/10.1016/s0065-2601(08)00404-8

Barth, S., & De Jong, M. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bennett, C. J. (2018). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press. https://doi.org/10.7591/9781501722134

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in sport, exercise and health*, *13*(2), 201-216. https://doi.org/10.1080/2159676X.2019.1704846

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). The CARE Principles for Indigenous Data Governance. *Data Science Journal*, *19*(43), 1-12. https://doi.org/https://doi.org/10.5334/dsj-2020-043

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. *Science and engineering ethics*, *24*(2), 505-528.

Deci, E. L., & Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, *11*(4), 227-268. https://doi.org/https://doi.org/10.1207/S15327965PLI1104_01

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *48*, 285-297. https://doi.org/10.1002/ejsp.2049

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The Affect Heuristic in Judgments of Risks and Benefits. *Journal of Behavioral Decision Making*, *13*, 1-17. https://doi.org/10.1002/(SICI)1099-0771(200001/03)13:1<1::AID-BDM333>3.0.CO;2-S

Giles, H., & Giles, J. (2012). Ingroups and outgroups. In A. Kurylo (Ed.), *Inter/Cultural communication: Representation and construction of culture.* (pp. 141-161). Sage Publications. http://www.sagepub.com/upm-data/48648_ch_7.pdf

Hand, D. J. (2018). Aspects of Data Ethics in a Changing World: Where Are We Now? *Big Data*, *6*(3), 176-190. https://doi.org/10.1089/big.2018.0083

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *computers & security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Lin, C. A. (1999). Uses and gratifications. In G. Stone, M. Singletary, & V. P. Richmond (Eds.), *Clarifying Communication Theories: A Hands-On Approach* (pp. 199-208). Iowa State University Press.

Loewenstein, G., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as Feelings. *Psychological bulletin*, *127*(2), 267-286. https://doi.org/10.1037/0033-2909.127.2.267

Luhmann, N. (2000). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 94-107).

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709-734. https://doi.org/10.5465/AMR.1995.9508080335

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, *2*(2), 1-25. https://doi.org/10.1145/1985347.1985353

McKnight, D. H., & Chervany, N. (2001). Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, M. Singh, & Y.-H. Tan (Eds.), *Trust in Cyber-societies* (Vol. 2246, pp. 27-54). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45547-7_3

McKnight, H., Carter, M., & Clay, P. (2009). Trust in technology: development of a set of constructs and measures.

Muirhead, W. (2011). When four principles are too many: bloodgate, integrity and an action-guiding model of ethical decision making in clinical practice. *Clinical Ethics*, *38*, 195-196. https://doi.org/10.1136/medethics-2011-100136

Paek, H.-J., & Hove, T. (2017). Risk Perceptions and Risk Characteristics. In *Oxford Research Encyclopedia of Communication*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.283

Pickering, B. (2021). Trust, But Verify: Informed Consent, AI Technologies, and Public Health Emergencies. *Future Internet*, *13*(5). https://doi.org/10.3390/fi13050132

Pickering, B., Taylor, S., & Boniface, M. (2020). *Private Citizen Perceptions of Fake News, Echo Chambers and Populism* 7th European Conference on Social Media, Larnaca, Cyprus.

Rimal, R. N., & Real, K. (2003). Perceived Risk and Efficacy Beliefs as Motivators of Change. *Human Communication Research*, *29*(3), 370-399. https://doi.org/10.1111/j.1468-2958.2003.tb00844.x

Rohlfing, K. J., Cimiano, P., Scharlau, I., Matzner, T., Buhl, H. M., Buschmeier, H., Esposito, E., Grimminger, A., Hammer, B., Häb-Umbach, R., Horwath, I., Hüllermeier, E., Kern, F., Kopp, S., Thommes, K., Ngomo, A.-C. N., Schulte, C., Wachsmuth, H., Wagner, P., & Wrede, B. (2020). Explanation as a social practice: Toward a conceptual framework for the social design of AI systems. *IEEE Transactions on Cognitive and Developmental Systems*, 1-1. https://doi.org/10.1109/TCDS.2020.3044366

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, *23*(3), 393-404. https://doi.org/10.5465/AMR.1998.926617

Rubin, M. A. (2014). The Collaborative Autonomy Model of Medical Decision-Making [journal article]. *Neurocritical Care*, *20*(2), 311-318. https://doi.org/10.1007/s12028-013-9922-2

Ruggiero, T. E. (2000). Uses and Gratifications Theory in the 21st Century. *Mass Communication & Society*, *3*(1), 3-37. https://doi.org/10.1207/S15327825MCS0301_02

Ryan, R. M., & Deci, E. L. (2000a). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary educational psychology*, *25*(1), 54-67. https://doi.org/10.1006/ceps.1999.1020

Ryan, R. M., & Deci, E. L. (2000b). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68. https://doi.org/10.1037/0003-066X.55.1.68

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of management review*, *32*(2), 344-354. https://doi.org/10.5465/AMR.2007.24348410

Sheeran, P., & Webb, T. L. (2016). The Intention-Behaviour Gap. *Social and Personality Psychology Compass*, *10*(9), 503-518. https://doi.org/10.1111/spc3.12265

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis*, *24*(2), 311-322. https://doi.org/10.1111/j.0272-4332.2004.00433.x

Smerecnik, C. M. R., Mesters, I., Candel, M. J. J. M., De Vries, H., & De Vries, N. K. (2012). Risk Perception and Information Processing: The Development and Validation of a Questionnaire to Assess Self-Reported Information Processing. *Risk analysis*, *32*(1), 54-66. https://doi.org/10.1111/j.1539-6924.2011.01651.x

Suárez-Alvarez, J., Pedrosa, I., Lozano, L. M., García-Cueto, E., Cuesta, M., & Muñiz, J. (2018). Using reversed items in Likert scales: A questionable practice. *Psicothema*, *30*(2), 149-158. https://doi.org/10.7334/psicothema2018.33

Tyler, T. R., & Cook, F. L. (1984). The mass media and judgments of risk: Distinguishing impact on personal and societal level judgments. *Journal of Personality and Social Psychology*, *47*(4), 693.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431-453. https://doi.org/10.1111/1540-4560.00072

Willits, F. K., Theodori, G. L., & Luloff, A. E. (2016). Another Look at Likert Scales. *Journal of Rural Social Sciences*, *31*(3), 126-139. https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1073&context=jrss

Witte, K. (1992). Putting the Fear back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, *59*(4), 329-349.

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health education & behavior*, *27*(5), 591-615. https://doi.org/10.1177/109019810002700506