Person-Centred Data Sharing:
Empirical Studies in Private Individuals' Attitudes

Authors and affiliations

Brian Pickering (ORCID 0000-0002-6815-2938)[1,2]
Michael Boniface (ORCID 0000-0002-9281-6095)[1]
Silke Roth (0000-0002-8760-0505)[3]
Katie Baker (ORCID 0009-0004-4151-7732)[4]
Steve Taylor (ORCID 0000-0002-9937-1762)[1]

[1]IT Innovation, Electronics and Computer Science, University of Southampton, Southampton. SO17 1BJ. UK
[2]Corresponding author (j.b.pickering@soton.ac.uk)
[3]Department of Sociology, Social Policy and Criminology, University of Southampton, Southampton. SO17 1BJ. UK
[4]School of Psychology, University of Southampton, Southampton. SO17 1BJ. UK

Abstract

Recognising the power of data analytics, researchers are anxious to gain access to personal data either directly from data subjects or via research data sets. Processing such data requires a secure environment, sometimes referred to as a trusted research environment (TRE). However, it is unclear how the data subjects themselves would regard sharing their data with TREs, especially if the outcome of such research was difficult to specify upfront making the idea of *informed consent* difficult to manage. In this paper, we review three empirical studies about data sharing to throw some light on private individual attitudes to sharing data, especially health data. The first focuses on cybersecurity, demonstrating that private individuals can make decisions about security measures though usually assume that the recipient of their personal data to be responsible for all aspects of keeping the data safe. The second asks how private individuals make decisions to share their data, and highlights that individuals are aware of risks but are motivated to share their data based on different contextual assumptions. The third looks at the incidental sharing of sensitive data during a saliva testing pilot during the SARS-CoV-2 pandemic and highlights prosocial motivations which override even the potential benefit of such testing. Taken together, these studies contribute to the complex set of motivations which encourage data sharing in general and highlight eight specific challenges for those wishing to manage a trusted research environment.

Keywords

Trusted Research Environment; cybersecurity awareness**;** privacy attitudes**;** data sharing**;** 5 Safes**;** FAIR; CARE; mixed methods

Introduction

Recognising the power of data analytics in appropriately processing the ever-increasing volumes of people-centric data available, the Toronto Declaration (Amnesty International and AccessNow, 2018, Art.25) highlighted the need for continued emphasis on the fundamental human rights of data subjects, especially those felt to be particularly vulnerable. The UK Government Digital Services (UK Government, 2020) formalised this perspective in their Data Ethics Framework, while the EU has outlined their Data Governance Act which among other things outlines a vision for data sharing in support of data innovation (European Commission, 2022). Both champion the overarching principles of transparency, accountability, and fairness. As well as compliance with relevant law, the framework focuses on balancing community needs against individual rights, whilst constantly reviewing those individual rights. In response to increased artificial intelligence (AI) deployment in health and social care, both the European Commission (European Commission, 2019) and the UK Department of Health and Social Care (UK Government, 2021) continue to emphasise respect for individual rights within the context of potential community benefit, accountability, fairness and transparency. Official statements like these inform the governance structures for the safe and secure handling of data, especially the types of datasets typically used for modelling population-level effects (for example: Luo et al., 2015; Sushmita et al., 2015), advisory predictions (e.g., during the SARS-CoV-2 pandemic; such as: Alsunaidi et al. (2021)) and diagnosis (Dilsizian & Siegel, 2014; Ronmark et al., 2022).

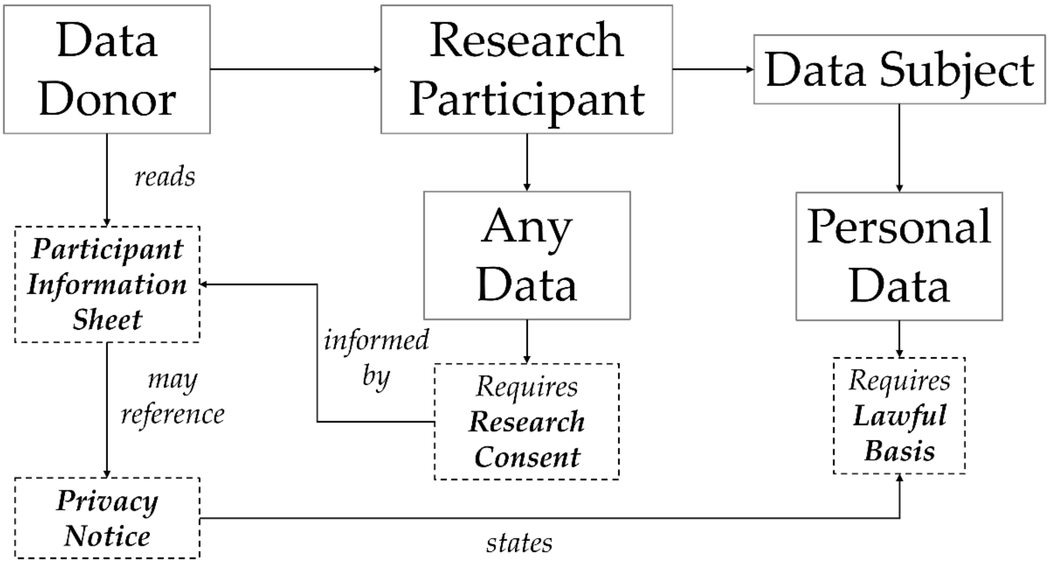

Figure 1: Consent to take part in research

Figure 1 summarises the typical process for an individual (a data donor) to agree to share data for research purposes. Data donation has been defined as "the act of an individual actively consenting to donate their personal data for research" (Skatova & Goulding, 2019). In this paper and for simplicity, we distinguish *primary data sharing* whereby donors share their data on a one-off basis as part of a specific research project from *secondary data sharing* where they release their data to a data repository such as a biobank for unspecified though controlled research activities. A participant information sheet (PIS) is provided for the donor to understand what is involved in the research and what is required of them and their data. For *primary data* collection and regardless of the data they provide, the data donor is a *research participant*. They give informed research consent based on the PIS and having been able to ask for clarification of anything they do not understand. If the data they share is personal data, it is also subject to data protection laws. Therefore, there needs to be an appropriate reason, a lawful basis, for processing the data. In addition to the PIS, the researcher should provide information about this processing in a privacy notice (PN). For *secondary data* use, where a researcher uses pre-donated data, the donor may only have seen a general PN for the repository holding their data.

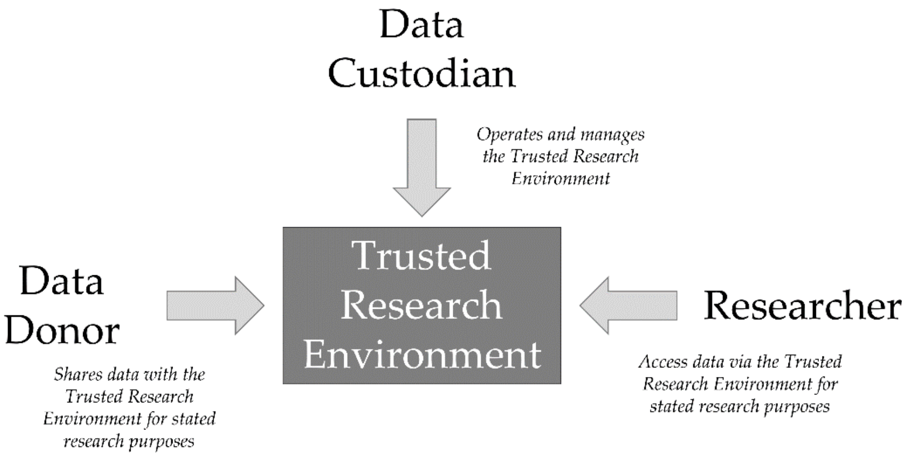
Data Custodian
Operates and manages the Trusted Research Environment
Data Donor
Shares data with the Trusted Research Environment for stated research purposes
Trusted Research Environment
Researcher
Access data via the Trusted Research Environment for stated research purposes

Figure 2: Trusted research environment

In data protection terms, the research participant is referred to as a data subject. For data donors to consent to the use of their personal data, they would expect their data to be used appropriately, kept securely and only shared with other parties with their explicit agreement. The PIS and PN together provide such reassurance. Part of any such reassurance includes the environment, such as a university server or similar platform, where the data will be stored and interrogated. Data donors (research participants) want to know that they can trust the research environment where their data will be processed. Figure 2 summarises the concept of a Trusted Research Environment (TRE; UK Health Data Research Alliance, 2021). A TRE is intended to provide a safe and trustworthy environment where researchers may access and exploit a single or multiple datasets. The data donor shares their data or authorises access to their data via the TRE operated by a data custodian. The latter has a responsibility to the donor for the secure handling of their data (*Safe settings* according to the 5 Safes +1 framework) and to ensure appropriate use by researchers (*Safe people, Safe projects,* and so forth) However, there is another imperative which more readily reflects the focus on individual and community rights introduced with the Toronto Declaration (Amnesty International and AccessNow, 2018) and Floridi's information ethics (Floridi & Taddeo, 2016): the benefits of access to data for research should be shared across all stakeholders, including artificial agents. In practical terms, stakeholder interests should be respected and managed by an Operations Board acting as data custodian to provide oversight of research activities involving the TRE and an independent, PPI-style participant advocate, representing research participant interests (whether or not they are also data subjects[1]). As well as secure infrastructure and governance, therefore, there is also a need for the ethical distribution of research benefit. Whether the addition of *safe return* (UK Health Data Research Alliance, 2020; UK Health Data Research Alliance, 2021) is sufficient is a moot point. The Southampton Social Data Foundation (SDF) which embraces the 5+1 Safes (Desai et al., 2016; UK Health Data Research Alliance, 2020) and the Research Data Alliance TRUST recommendations (Lin et al., 2020) has developed a model for a TRE and gone some way locally to implementing such a model (Boniface, Carmichael, Hall, Pickering, et al., 2022).

Another way to ensure appropriate stakeholder representation, but especially of the data donors (or research participants), would be to incorporate the CARE Principles[2] for research data oversight. Originally conceived to respect data sovereignty amongst indigenous peoples (Carroll et al., 2020), these principles reposition research participants as "self-determining users of data for development and wellbeing" (Carroll et al., 2020; p.2) which in turn ensures that all stakeholders across the research data lifecycle are well represented and will potentially benefit from research outcomes. At the same time, the research participants retain control over the data they provide. Although regulatory compliance is essential, the TRE should therefore assign equal weight to the rights and expectations of individuals and the communities they represent, therefore, not just through the implementation of the Five Safes + 1, but also by respecting the wishes and rights of the community of research participants in the spirit of CARE Full data exploitation (Carroll et al., 2020).

The question now is how potential data donors (research participants in research settings and potentially data subjects in data protection terms) respond to such measures, and a TRE like the Social Data Foundation (Boniface, Carmichael, Hall, Pickering, et al., 2022) might "earn, build and sustain public trust" (UK Health Data Research Alliance, 2020, p.24). Ultimately, private individuals' perceptions will significantly influence any such data donation decisions. With that in mind, the purpose of bringing together the research studies reported below is to identify the parameters which may affect private individuals in their trust decisions. This would at least provide a checklist for potential data donors when considering whether to share data with a TRE or reviewers when assessing project proposals accessing data via a TRE. Additionally, it may be possible to use checklist items to develop a survey to explore public trust in TREs.

Trust and Trustworthiness

Implicit within TREs is the assumption that governance practices aimed at increasing trustworthiness, such as the Five Safes + 1, will automatically trigger trust in potential research participants. It's worth remembering that this is not necessarily the case. On the one hand, decisions are usually made within the context of personal predisposition (in this case, the propensity to trust; see: Ashleigh et al. (2012); Körber (2019)) as well as or rather directly influenced by the views of significant others (trust transfer (Stewart, 2003) and social norms (Jiang et al., 2022)) which may vary over time and context (from experience with others (Glanville & Paxton, 2007)) and individual familiarity (Körber, 2019). This would be predicted by early behavioural models such as the Theory of Planned Behaviour and their constructs of *normative beliefs* and *subjective norms* (Ajzen, 1991), and has more recently been shown to be context sensitive (Baer et al., 2018). Trust is not therefore simply a response to trustworthiness (see also: Körber, 2019). Understanding the context within which data sharing decisions are made is important in the design and publication of the

[1] In this paper, *research participant* is used to mean anyone sharing data in a research context, whether or not those data are personal: i.e., it includes *data subjects*. The latter term (*data subject*) is used solely if personal data are shared.
[2] https://www.gida-global.org/care

governance and operation of TREs if the intention is to encourage personal data donation or permitting access to those data.

Secondly, trust has long been associated with the acceptance of risk. The original Mayer et al. model (1995) makes this explicit along with an iterative, empirically based re-evaluation of trustworthiness: depending on the experience of the trustee's behaviour, the trustor will update their perceptions of trustee competence, integrity and benevolence. This has led to a classic definition of trust as the trustor's willingness to expose themselves to vulnerability at the hands of the trustee (Rousseau et al., 1998). This approach accepts the fallibility of the trustee, but also accommodates trust repair (Bachmann et al., 2015; Bansal & Zahedi, 2015; Memery et al., 2019; Schoorman et al., 2007). A trust-based relationship in this sense such as allowing access to personal data for research purposes encourages an ongoing commitment to communication and sharing experience. The research participant as trustor becomes actively engaged in the governance of their data (Carroll et al., 2020).

This definition also means that reliance on a contract or legal obligation precludes trust-based interactions (see: Luhmann, 2000). A TRE demonstrating compliance to the GDPR, for instance, and specifically data protection by design and by default (European Commission, 2016, Art. 25), removes the need for trust as defined above, though may not obviate the need for trust in a more general sense. Specifically, if the data subject suspects a breach, then they have a legal right to redress (European Commission, 2016, Chapter 3): they do not expect to be exposed to vulnerability. Whether they are aware of such rights is a different matter (Acquisti et al., 2015). At any event, a TRE cannot necessarily rely on regulatory compliance to encourage trust in potential users. There has to be something more, akin to a willingness to co-operate with a potential trustor on an ongoing basis (Pickering, 2021).

One aspect of regulatory compliance typically leads to the publication of a PN[3]. The notice should provide details of any personal data collected, on what basis those data are processed, who has access to it, and who to contact in the case of concern[4]. Often, the assumption would be that a potential data subject would read and understand the PN, and on that basis, provide consent as a lawful basis for processing their data (see Figure 1 above). Within the context of TRE, it is not clear who should provide the PN. In a research context, the trust relationship has historically been between the research participant as data donor and the researcher. But if the data are to be shared and accessed via a TRE, it is reasonable for the data donor to seek assurance that the mediation of the TRE will not undermine this relationship. The question, therefore, is whether a TRE should make available a PN to the data donor or the researcher should assume responsibility for ensuring that the TRE meets their needs and that they (the researcher) are confident that they can fulfil the commitments they have made to the data donor[5]?

Relying on a PN, whoever publishes it, is problematic for various reasons. First, there is no guarantee that data subjects would read the PN at all (Mulder & Tudorica, 2019; Obar & Oeldorf-Hirsch, 2020). Secondly, they and researchers may confuse what is intended by *consent* (Pickering, 2021). For instance, research consent is required even if the data are completely anonymous; and the data to be collected and how they are used would typically be covered in a PIS albeit via a link to a generic PN (as shown in Figure 1). Data protection consent covers only personal data and is a rather restrictive lawful basis. Research institutions, however, may use a different lawful basis if using personal data (e.g., public task: European Commission (2016, Art. 6(e)) at the same time as requesting research consent[6] and benefit under data protection law from specific exemptions (European Commission, 2016; Art. 89).

[3] For instance, both NHS Digital at https://digital.nhs.uk/about-nhs-digital/privacy-and-cookies and the UK Biobank at https://www.ukbiobank.ac.uk/privacy-policy provide PNs.

[4] From a data protection perspective, there is a need for clarity here. The data controller is responsible for producing a suitable PN. In the case of a research study via a TRE, especially involving data visitation, there would presumably be joint controllers: the data custodian at the TRE and the researcher. Both would need appropriate PNs.

[5] This is further complicated, of course, if the data donor has released data for ongoing, unspecified (though ethically approved) research purposes (e.g., to a biobank).

[6] There is a further challenge which is why we distinguish the secondary use of data: individuals who have donated data in the past without knowing what those data may be used for in the future as mentioned previously. See *Understandings and consent* for the UK Biobank, for instance, (https://www.ukbiobank.ac.uk/media/0xsbmfmw/egf.pdf)

It is beyond the scope of this study to revisit these issues in any detail or to suggest a more effective mechanism to deal with *consent.* Instead, using three different and unrelated empirical studies, the aim is to identify private citizen behaviours and attitudes which may be relevant in the decision-making process of those wanting to share personal data. In so doing, a set of considerations for potential data donors may be drawn up which highlights specific issues or concerns which would be provided as a checklist for a TRE for a given project to share and discuss with potential data subjects and researchers.

Three Empirical Case Studies

In the context of accountability, transparency and fairness (European Commission, 2022; UK Government, 2020), private individuals' attitudes to explicit or implicit data sharing may provide some insight into developing data donor trust (Balapour et al., 2020; Kim et al., 2015; Skatova et al., 2014)[7]. For instance, when explicitly sharing their data, do individuals understand how their data will be secured (*Safe settings*) or who is responsible for data governance (accountability and transparency)? Do they always understand who will access their data (accountability and transparency)? Or when implicitly sharing their data as part of an overarching study or some other activity like healthcare or retail, do individuals perceive the benefit of how their data are to be used (fairness, not least in the sense of community and personal benefit)? Some researchers have already suggested a link between trust and a willingness to share personal data based on context (Mamonov & Benbunan-Fich, 2018; Skatova & Goulding, 2019). Further, data donation studies have identified that community benefit is a significant predictor as is the type of organisation who might use the data for research, whilst, however, personal reward has a negative effect (Skatova & Goulding, 2019).

It is tempting for infrastructure providers to focus solely on security when handling personal data. After all, it is required by law (European Commission, 2016, Art. 25) and defined by internationally accepted standards (International Organization for Standardization, 2018a, 2018b). This therefore provides a useful starting point (Balapour et al., 2020; Kim et al., 2015). However, this is essentially only *Safe setting*. The consequences and perceptions of a secure infrastructure need to be considered too. In that regard, privacy is also required by law (European Commission, 2002, 2016), and relates directly to *Safe data* and *Safe outputs*, and perhaps indirectly to *Safe projects* and *Safe people*. Empirically, though, this does not always predict data sharing behaviours (Barth & De Jong, 2017). Beyond security, therefore, and even though security and privacy are related (Balapour et al., 2020) and may even be a response to similar traits (Egelman & Peer, 2015), it is important to consider attitudes towards personal privacy in regard to the willingness to share personal data either for research or in the context of commerce and similar transactions (Ioannou et al., 2021; Kim et al., 2015; Mamonov & Benbunan-Fich, 2018; Skatova et al., 2014). It's also worth remembering that data donation in the sense of simply agreeing that data can be used for any ethically approved research is much more likely with an assurance of anonymity (Kim et al., 2015). Even so, the sharing of sensitive data for research purposes should also be examined, not least because prosociality may override privacy concerns (Kim et al., 2015; Skatova & Goulding, 2019; Skatova et al., 2014). Security, privacy and motivations to share data are all important, therefore.

Table 1: Empirical Studies related to Security, Privacy and Data Sharing

Domain	Participants	Method	Aim
Cybersecurity	800 UK citizen via a crowdsourcing platform[8], and paid a nominal amount[9] to complete the survey.	Anonymous online survey (Pickering & Taylor, 2023)	Members of the general public in the UK read a passage about cybersecurity and were then randomly asked to identify threats (context i), controls (ii), to match controls with threats (iii), or to identify those responsible for implementing the controls (iv). They then responded to 45 assertions on a 6-point Likert scale about cybersecurity specifically when sharing their health

[7] https://understandingpatientdata.org.uk/news/what-why-trusted-research-environments
[8] Prolific.co https://www.prolific.co/
[9] The survey had been piloted with colleagues and based on the average time for them to respond, an amount was calculated based on the UK minimum wage at the time.

Domain	Participants	Method	Aim
			data.
Privacy	500 members of the general public were recruited via a crowd-sourcing platform[8], and paid a nominal amount[9] to complete the survey.	Anonymous online survey to evaluate assertions generated from a series of focus-group workshops about data privacy attitudes (Pickering et al., 2023)	The assertions were grouped into four sets of twelve, preceded in each case by a 'how likely' question of the type: *How likely are you to share your data with…?* data custodians like *researchers, the government*, or *retailers*. Responses to these introductory questions were expressed typically from *Never* to *Always*; the twelve assertions were assessed on a 5-point Likert scale. (See Boniface, Carmichael, Hall, Mcmahon, et al. (2022)).
Attitudes to data sharing	During the SARS-CoV-2 pandemic, 1086 students at a Russell Group university in the UK took part in the survey, of whom 943 responded to all questions.	Anonymous online survey assessing a diagnostic test to identify those infected with the coronavirus[10] (Pickering et al., 2024)	Study captured participant experiences with the diagnostic test under review. At the same time, they were potentially sensitive health status data. (See *Note 1* and *Note 2* below.)

Note 1: Regulations were in place, of course, during public health emergencies covering the sharing of diagnostic results (see, for instance: UK Government, 2002)[11].
Note 2: the trial was very much a research study where results may not be as robust as mainstream NHS testing at the time.

To understand private individuals' potential attitudes towards a TRE regarding these three factors (security, privacy and motivations to share data), we review three separate studies not specifically designed to test the willingness to engage and share data but covering different aspects of engagement with ICT-based services or infrastructures like security and accountability, data governance or privacy, transparency and community benefit, and why data sharing is appropriate (related to fairness). The findings of such research have the potential to inform the development of a suitable instrument to gauge the public's view of sharing their data via TREs and likely interaction with them. They may also guide further review of related work. The empirical studies are summarised in Table 1.

Cybersecurity: *General Awareness of Security*

There was reasonable consensus for the ranking and matching cohorts (contexts (i), (ii) and (iii)). This implies that private individuals can make judgements about threats and controls, including deciding about which control might be effective for which threat. Additionally, they identified the data custodian (in this case the UK National Health Service (NHS) or a hospital since the scenario was health data sharing) as responsible 67% (365/545) of the time on average for implementing five out of seven possible controls. One exception was with managing their own devices: then private individuals accepted they had a responsibility 55% (60/109) of the time on average. The second was for continuous monitoring of threats and then automatic updated controls installed: this was assumed to be the responsibility of the manufacturer or app developer 49.5% (54/109) of the time for the specific control associated with automatic updates.

Typically, in their freeform comments, participants highlighted concern around cybersecurity in general and the need for co-operation between users and a service provider, such as an employer:

> "Emphasis should be on user. My workplace was hacked and my personal data taken, despite me taking personal measures to not share my info."

[10] Participants were told explicitly that the study aimed "to assess the feasibility of at-home saliva testing for COVID-19 has been launched in [CITY] and some of you will shortly be invited to participate" (July 2020)
[11] See also https://www.gov.uk/guidance/notifiable-diseases-and-causative-organisms-how-to-report

or other users:

> "Health care apps used by carers are the one of the worst for data breach [*sic.*] …"

though ultimately, there may be a general concern about security and the level of communication:

> "I do not believe I am properly informed if my data/passwords/information is stolen in a cyber attack …"

and the steps required to remain secure where the private individual does not believe that they have complete control:

> "Me taking security measures doesn't stop hacking/risk it just reduces the risk a bit. Also sometimes it becomes a nuisance - e.g. my credit card have improved security so that for an online purchase I have to enter a code only I know and also get sent a OTP[12]."

It's worth noting the apparent reluctance here to implement controls which are perceived as cumbersome.

In terms of the basic security of a TRE, therefore, private citizens can understand security measures or controls (*Safe setting*) as well as making decisions about where responsibility for implementing those controls lies (*Safe projects, Safe people*). Having access to a TRE's stance *vis-à-vis* the Five Safes + 1 may well inform any trust decision though will not be the primary motivator as discussed previously. However, there is a more generalised concern around a broader socio-technical context for a given service and who might be involved. Such actors may directly or indirectly affect the overall trustworthiness of the secure handling of data. It would be important, therefore, to ask potential participants how they perceive the wider research context as this affects their perception of how secure data might be. Specifically, they would need to know who would be involved in handling research data within the TRE.

This study highlights at least one of the challenges for a TRE demonstrating appropriate governance measures to a potential research participant sharing data or allowing access to their data: although this information should already be available (such as via a PN or PIS), research participants may not fully understand the implications or indeed act on that information. There may need to be a more explicit conversation with research participants or data custodians to ensure proper understanding of how data will be exploited; and this is an ongoing, dynamic process not a one-off interaction (e.g., Kadam, 2017). The survey itself illustrates an *awareness* of security measures. The freeform comments, however, start to highlight that *such awareness does not necessarily translate into satisfactory practice*. If trust in the TRE requires a negotiated acceptance of vulnerability, then perhaps we need to look more closely at private individual perceptions about the security of the data they share.

Privacy: *General Attitudes to Sharing Data*

The second survey summarised here looks specifically at attitudes towards privacy including how private individuals arrive at a decision to share their personal data. Table 2 summarises the highest-ranking responses by percentage agreement from 470 participants once outliers had been removed. The groupings (Transparency, Accountability and Fairness) have been added *post hoc* regarding the principles from government guidance (European Commission, 2019; UK Government, 2021). Interestingly, these correspond to Westin's filter questions (Woodruff et al., 2014, their Figure 1)[13]

Table 2: Highest Ranking Agreement to Assertions about the Privacy of Personal and / or Research Data. Note: A Percentage in Brackets in the 3rd Column represents Disagreement with the Assertion

Area	Assertion	Agree (Disagree)
Transparency	Companies should be transparent about how they use data and who they share them with	95.96

[12] One-time password

[13] Transparency relates to what they call *Businesses behave well*, Accountability to *Laws protect*, and Fairness to *Loss of control*, suggesting validation here of broader privacy issues.

Area	Assertion	Agree (Disagree)
	I don't believe that firms always tell me what they're doing with my data	83.80
	Companies deliberately make their privacy notices long and complicated so I won't read them	83.16
Accountability	An independent authority should check that companies comply with the law	93.83
	Individuals responsible for breaches should be held accountable	88.03
	The company I share my data with is responsible for my privacy	85.07
Fairness	I should be asked before my data is used for a purpose I didn't originally agree to	94.89
	I [don't] need to be involved in any decisions about my data * [14]	88.06
	If a company or researcher uses my data that's different from what they said originally, they don't have to tell me	(83.62)

It's worth adding here that, in response to *In general, I am concerned when sharing my personal data by…* 64.21% of respondents said: *the security of the data I contribute*. This was a different cohort to the one in the first survey responding to cybersecurity questions but echoes their awareness that security (*Safe setting* at least) is important. Interestingly, all of the issues in Table 2 are covered by existing regulation. Indeed, it's worth highlighting responses to the following assertions:

> The Government should be doing more to help people understand privacy and data sharing

83.37% agreed with this statement: this is precisely what data protection regulation is intended for. For instance, one of the purposes of the (UK) GDPR was to make explicit data subject rights. Further, 87.66% agree that:

> Technology should be developed to help us manage our data

Finally, almost all respondents believe:

> An independent authority should check that companies comply with the law

(93.83% agree). This is what a Supervisory Authority under the GDPR does (European Commission, 2016, Art. 51); in the UK, the Supervisory Authority is the Information Commissioner's Office. Research participants seem to want to maintain control over their data and for regulatory structures to be in place, and yet they do not act on the rights they have been given or perhaps don't fully understand what structures are in place. A TRE asserting its compliance with data protection regulation and publishing a PN to make this explicit may not therefore be responding to private citizen perceptions of how data sharing is handled.

As noted in Table 2, groups of twelve assertions were separated by a general statement and three options. So, in response to *How do I decide to share my data?* for example, 60.61% say that their data sharing decisions is based on trust in the organisation requesting the data as opposed to 42.79% who read the PN, and 46.50% who just get on with whatever they were doing. This is significant in that whatever regulatory structures may be in place (data subject rights, informed consent and so forth), data sharing decisions are made largely based on trust, which may be an emotional rather than entirely considered choice. Nevertheless, there is still a concern about how those data are used. For example, participants still voiced concern about the possibility of onward sharing of their data: 73.08% agreed onward data sharing would be a concern in response to *When deciding to share my data, I worry about…;* and 73.38% in response to *In general, I am concerned when sharing my personal data.* Although issues like transparency, accountability and fairness are relevant to respondents as summarised in the table, therefore, there is an affective dimension which needs to be considered (they decide on trust, rather than a PN or PIS) and especially about the possibility that data may be shared with others (which would be covered in documents like the PN and PIS).

[14] In common with other studies using Likert scales, some assertions are reversed to check respondent attention. Scoring is also then reversed to establish how much the respondent agrees with the reversed statement. In this example, 88.06% were agreeing that they *do* "need to be involved in any decisions about [their] data", therefore.

The apparent contradictions between making informed decisions, being concerned about onward sharing, and a lack of understanding or engagement with PNs and PISs all need to be investigated further to be understood and appropriate steps to be taken. The assumption that private citizens are making informed decisions based on current practice including the publication of a PN and/or a PIS is difficult to justify from the privacy survey. Despite existing regulatory frameworks, and although private citizens wish to be able to rely on the mechanisms regulation provides, they are still unaware that they have rights and that there are structures in place to protect those rights. Instead, decisions appear to be made based on an affective response to the data custodian – a TRE; assuming an informed decision based on the information in a PN or PIS is not supported here, though; more than that, individuals assume (83.16% of respondents) that PNs at least are deliberately obfuscating. Informed consent has to be a negotiated, ongoing and dynamic process (Grady, 2015; Kadam, 2017; Pickering, 2021).

Saliva testing for Coronavirus: *Indirect Data Sharing in the Real World*

From the previous two studies, therefore, private individuals are clearly capable of making decisions about the security of an infrastructure or rather they make assumptions based on their perception of the data custodian (Survey 1 on cybersecurity). Additionally, although they would like the confidence that regulation provides, they make decisions about data sharing mainly based on their trust of the data custodian and are most particularly concerned about data sharing (Survey 2 on privacy attitudes). In the third study, respondents took part in a diagnostic test trial which involved the consequent sharing of personal and special category personal data.

For the study, it was made explicit from the start that this was not a substitute for official testing; and that this was a collaborative study between the university, the local NHS trust and the city council. There was the potential at least, therefore, that and personal and even special category personal data may be shared between three partners and not just kept within the university itself. Participants would be sharing their data indirectly: that is, by dint of participation, data would be collected about them to identify the samples and the diagnostic result[15].

This third survey included four opportunities to leave free form comments for participants to record what they thought was (i) positive about the trial, (ii) what they liked or disliked, (iii) what improvements would be useful, and finally, (iv) any general comments or observations. Of the 1086 participants, 846 left a total of 2320 comments; 239 left none. The 2320 comments were reduced to 2161 by removing responses like "N/A" (not applicable), or "nothing" or "none" and so forth. From the 2161 comments remaining, six themes were identified as summarised in Table 3.

Table 3: Themes extracted from participant free form comments

Theme	Description	Incidence
Accuracy	Concerns about the accuracy of the saliva test by comparison to the NHS swab test. Often in response to hearsay.	156
Participation	Gratitude for the study. Pride in the institution for carrying out the study.	72
Prosociality	Concern for both significant others and strangers especially if asymptomatic	121
Reassurance	Peace of mind from knowing coronavirus status	286
Rule bending	Concern about misuse of test results to ignore social distancing	7
Widening participation	Call to include others in the study not least because that would mean more people being tested within those the participant is in contact with	78

The final column of Table 3, *Incidence*, records the number of participants who mention anything to do with this theme in one or more of any comments they left[16]. So, of the 846 participants leaving comments, 286 (33.8%) mentioned a feeling of *Reassurance* from taking part in the study, while 78 (9.2%) also mentioned that they thought it would be helpful to *Widen participation*. Of those leaving comments (846 of the original

[15] Though the survey itself was entirely anonymous.

[16] i.e., of a total of 846 participants leaving comments rather than the 2161 actual comments

1085), 382 did not contribute to any of the themes. Their comments were of the type:

> "Easy and fast" commenting on the saliva test itself, or "Not enough drop off sites" commenting on the organisation of the test.

Of the remaining 464 participants (846 – 382), 263 contributed to a single theme, 154 to 2 themes, 39 to 3, and 8 to four themes.

Table 4: Participants contributing to two themes

	Acc	**Par**	**Pro**	**Rea**	**Rul**	**Wid**
Accuracy (**Acc**)	-	11	26	***52***	4	13
Participation (**Par**)		-	12	***40***	1	11
Prosociality (**Pro**)			-	***95***	0	14
Reassurance (**Rea**)				-	***4***	***35***
Rule bending (**Rul**)					-	1
Widening participation (**Wid**)						-

Table 4 summarises typical (two-way) combinations of themes. For instance, 26 participants mentioned both *Accuracy* and *Prosociality*, while 95 talked of both *Prosociality* and feelings of *Reassurance*. Indeed, the vast majority of participants who contributed to two themes include *Reassurance* as one of those themes: 52 in combination with concerns about *Accuracy,* 40 with feelings of gratitude for their *Participation,* 95 with *Prosociality* (the beneficial impact of testing on significant others and strangers), and 35 in connection with calls to open participation to more people (*Widening participation).* Remembering that the original invitation to take part in the saliva testing study explicitly describes the aim *"to assess the feasibility of at-home saliva testing" (*Vice Chancellor's communication, July 2020), it is surprising that so many participants talk about feelings of *Reassurance*. Even more so, because 52 participants mention both *Reassurance* along with concerns about *Accuracy*: they were comforted by the test even though they reported doubts about the accuracy of the results.

In some cases here, they also spoke about a third theme (39 participants) or even a fourth one (8 participants): that is, their comments contributed to three or four themes, in addition to the two themes summarised in Table 4 above. Table 5 therefore summarises combinations of three or four themes from the comments of a single participant. 19 participants who contribute to three of the themes include *Accuracy* as one of the themes; and all 8 participants whose comments contribute to four of the six themes include *Reassurance* as one of the themes they discuss.

Table 5: Themes involved in combinations of three or four themes

Involved in:	**Acc**	**Par**	**Pro**	**Rea**	**Rul**	**Wid**
Three themes (39)	19	13	30	37	1	17
Four themes (8)	6	6	6	8	1	5

Once again, participants contributing to three or four themes mention *Reassurance*: 37 of the 39 participants whose comments contribute to three themes include *Reassurance,* and all 8 participants for four themes include it. Participants in the saliva testing feasibility study are aware of relative accuracy (saliva testing *versus* standard NHS swab testing) but are more focused on the benefits they might derive from such a programme. They also believe participation should be *Widened* (78 overall, see Table 3) and express gratitude for their *Participation* (72 overall).

For this third study, participants were not specifically asked to share data, of course. This was, however, an obvious consequence of participation, and their agreement to engage was based on standard procedures to support informed consent. However, it is perhaps significant here that participants, having agreed to take part, are concerned more about the wider context and how they see themselves within that context rather than specific issues relating to their data. Indeed, they will share sensitive and special category personal data, motivated by what they get (*Reassurance* and gratitude for being able to take part, *Participation*) and the implications of the study (*Prosociality* and a desire for *Widened participation*). This is a utilitarian perspective: the means (allowing data to be collected and shared) is justified if the outputs are beneficial (the results are positive for participants or those important to them).

Such a utilitarian focus towards research outcomes speaks directly to the CARE principles (Carroll et al., 2020), extending the construct of *collective benefit* beyond indigenous populations to any research cohort, especially the social ingroup of the participant (Giles & Giles, 2012). In this case, and despite concerns around the accuracy of the testing, participants are apparently looking specifically for positive outcomes not just for themselves but also for significant others. Where data are shared with researchers almost as an indirect consequence of participation, participants are looking at the wider context of the research. In this specific case, and despite the explicit statement that this was a *feasibility* study and not a tried-and-tested substitute for existing and approved diagnostic methods, participants are responding about ease of use and utility, as well as real benefit (the theme: *reassurance*) but also that maximising that benefit needs extension beyond the limited cohort (the theme: *widen participation*).

What the saliva testing survey shows is the engagement of research participants based on broader understanding of goals and potential, and not just a narrow focus on what happens to the data needed as part of the research nor the security of those data. Just as the original CARE principles set out, participants here seek involvement to promote the collective interests of their community (Carroll et al., 2020; p.8).

Discussion

Table 6 summarises the main conclusions from each of the three studies reported here. For the infrastructure and security of the data (*Study I* in the table), individuals have expectations around security specifically around securing personal data. Most significantly, private individuals have their own view on who is responsible for implementing those security measures. That private individuals maintain independent attitudes towards their data becomes more important when considering privacy (*Study II*). This is not about claiming one thing and then doing something else (as evidenced by the privacy paradox: Barth and De Jong (2017)), nor about being motivated by explicit compliance to regulation which they may not understand (Acquisti et al., 2015), data sharing seems to be motivated in appreciation of communal benefit (*Study III*; see also Böckler et al. (2018)).

Table 6: Considerations for TRE operators derived from the three empirical studies

What needs to be made clear	Motivation
I: Security of the Infrastructure	
What steps is the TRE taking to protect the data it makes available for research?	This establishes where the responsibility is assumed to lie independently of consent or privacy notice, and encourages the research participant (when data is collected directly from them) or the data custodian (where data are managed by an intermediary and may be used for secondary analysis)
How many people will be able to access the data?	Since the more people involved with a project, if not all are managed appropriately[17], the higher the potential risk of disclosure, it is important that all stakeholders understand who will have access to research data. For example, a research participant donating data to a biobank may be influenced by how many and what type of organisations will be able to use their data. The dynamic, ongoing informed consent process may become more complex for such secondary use of data via a TRE, but that is not an excuse to avoid informing data subjects about what may happen with their data.
II: Privacy of Data	
Do research participants really understand what will happen to their data?	From the study reported here, it is clear research participants do not always know what will happen with their data, even though they are clearly concerned about the onward sharing of those data. For the TRE operator, it must be made clear who will have access to the data, what for and how long the data will be kept. Any planned onward sharing would appear to be particularly important.
Do researchers or data custodians know what happens to the data the manage?	Correspondingly, researchers should be clear how they intend to use data (either primary or secondary use). This is important for the TRE to assess the researchers' *Safe* status (*Safe project, Safe people, Safe output*, etc.) but also, *in loco* participant, satisfy their own obligations *vis-à-vis* the participant

[17] Such as being subject to the same governance principles which applied to the original data collection

What needs to be made clear	Motivation
	to protect and manage their data appropriately.
In the case of personal data, do data subjects understand their rights and the structures in place to protect those rights?	Existing structures exist which protect the rights of individuals not only to privacy, but also to correct their data, prevent processing they do not agree with, and prevent decisions being made automatically about them based on data from them and similar others. It is clear, however, in this and other empirical studies that data subjects can describe what they would like to be in place but do not know of or exploit what is already there. Regulation such as the GDPR has failed to empower data subjects as such. From a TRE perspective, it should therefore be made abundantly clear to researchers and to data subjects when donating data directly just what their rights on, especially to remove data and to prevent onward sharing.
III: Benefits of Data Sharing	
What is the potential benefit of data sharing to the individual research participant (data subject)?	Although the third study reported here might be regarded a special case (students may be anxious because of uncertainties around lockdown), it highlights that research participants may well engage and share their data if they particularly perceive a benefit to them or to similar others. This may well supersede any specific concerns are security and privacy.
What is the potential benefit of data sharing to the ingroup / significant others of the research participant (data subject)?	That being said, those sharing data may also be motivated if there is clear potential benefit to those that research participants (data subjects) care about. Such prosocial behaviour may well be a significant motivator, as in this study: indeed, in many drug trials, it has to be made clear to a participant that they may not derive direct benefit, but others could.
What are the motivators for participation?	Beyond any specific benefit for individuals and notwithstanding issues of accuracy for the diagnostic test under review, there may well be other motivators for participation even when this involves sharing special category personal data. For example, one of the themes identified involved pride in the organising institution: to be seen to be part of an activity with such obvious potential. Although clearly not a substitute for more traditional governance and informed research procedures, identifying social motivators (doing something good for the community in this case) alongside personal motivators for self or significant others should be considered in order to be able to highlight what the participant would see as a reason to engage.

The third survey is an extreme case in that the students were studying during the first half of the SARS-CoV-2 pandemic and had been or were going through successive lockdowns, altering their university experience. Away from home in many cases, the student cohort would perhaps be emotionally vulnerable. Further, there was an existing relationship between the students and the university; and the public response to the NHS was very positive at the time (Manthorpe et al., 2022). There might be an expectation, therefore, that data sharing decisions would be made based on the assumed student reliance on a perceived duty of care. However, this was also a period of uncertainty and increased scepticism about the government's handling of the situation. This might also affect the willingness of individuals to engage with contact tracing, for instance (Rowe et al., 2020), unless a specific and individual benefit is apparent (Velicia-Martin et al., 2021; Walrave et al., 2020). What therefore might the students' responses to the survey reveal about their willingness to take part in a research study involving the indirect sharing of sensitive data? By extension, how would this inform decisions to share data with a TRE if informed consent is not ethically unambiguous?

The studies summarised here seem to indicate that the *Safes* may be important alongside constructs such as transparency, accountability and fairness in assessing the trustworthiness of a TRE, but there is something more akin to the CARE principles: there is a *prosocial* element to engaging with research or allowing one's own data to be used for research which acts as a motivator and which even mitigates potential concerns around efficacy and traditional constructs such as usability and so forth. Exploring motivation may well explain why awareness around cybersecurity and an unwillingness or inability to explore privacy regulation – do not necessarily reflect willingness to share data. Such features are assumed to add credibility to a TRE and inform decisions to take part in research or donate data, but are only part of the story which in turn may suggest a reassessment of informed consent processes (Corrigan, 2003; Pickering, 2021; Sugarman et al., 2005; Wiles et al., 2007). In research ethics terms, this moves consent (and trust in a TRE) away from respect of individual rights and towards justice or the sharing of benefit.

Limitations and Future Work

In presenting the findings from the three surveys cited here, the focus has been on transparency, accountability and fairness as expressed in government guidance, but without making explicit how these terms should be interpreted, implemented beyond existing regulation, or attempting to identify how private citizens might interpret these concepts when making decisions to share their data via a TRE. Our findings are therefore a *post hoc* interpretation of how research participants reacted when explicitly asked about security and privacy, or when asked to share data in the context of a broader public health emergency. In the latter case, since our participants were self-selecting and represented only a small proportion of the student population invited to take part, we can only speculate about those who chose not to participate in the study, who may have had more concerns about direct and indirect data sharing which prevented them from participating in the saliva study itself and in the survey about the participation in the saliva study.

On that note, we made no distinction here between primary and secondary data sharing: the former represents sharing within an explicit context which would generally involve specific research questions and boundaries for data use, as well as *quasi* direct contact between research participant and researcher. That is important because of the emphasis on *trust* in the privacy study. By contrast, the latter though in the context of biobanks, for example, or the publication of research data often now required by public funders, has no specific aims or boundaries beyond a separate review by a research ethics committee and an assumption that those providing the data in such a context *might* find acceptable. Further, the data subjects may have no oversight on how their data will be used, having to trust therefore that appropriate governance is in place when deciding to donate data. Similarly, researchers may not be able to predict the benefit which might derive from using those data. They too can only agree to respect the general governance stance of the TRE providing access to the data. Nonetheless, and as TREs become more prevalent (Carmichael et al., 2022), surveys of this kind provide an important perspective from the data subjects. Further, the recommendations we have provided can then be explicitly tested with research participants, researchers and TRE data custodians to inform how they might operate to build and develop trust.

Conclusion

In this paper, we have presented summaries of three different and unconnected surveys, each of which sought to examine a perspective from private individuals relating to the handling of their data and data sharing. The first aimed at identifying attitudes and understanding of cybersecurity, the second to the privacy of their data and data sharing activities, and the final one to the indirect sharing of (sensitive and special category) personal data in the context of the SARS-CoV-9 social restrictions. Bringing the individual survey results together, it is clear that there are tensions between private individual understanding and how they behave. Within the context of TREs, this has implications for three main stakeholders: those whose data may be used as part of a research study hosted on or via a TRE, the corresponding researchers exploiting those data, and the data custodians responsible for the data governance of the TRE itself. The findings suggest a set of specific challenges, identified as a set of eight items (two on infrastructure, three on data sharing, and three on participant perspectives). These are tabulated as a checklist for data custodians and researchers to base negotiation about participant data sharing via TREs. They may also provide some guidance for those reviewing applications for research projects to be run on TREs, namely research ethics committees.

Data and software availability

The cybersecurity survey dataset (Pickering & Taylor, 2023) is available at https://doi.org/10.5258/SOTON/D2946; the privacy survey dataset (Pickering et al., 2023) at https://doi.org/10.5258/SOTON/D2947; and the saliva testing dataset (Pickering et al., 2024) at https://doi.org/10.5258/SOTON/D2952

Competing interests

No competing interests were disclosed.

Ethics

Study 1 on cybersecurity awareness involved two cohorts (500 + 300 participants) and was approved by the Faculty of Engineering and Physical Sciences research ethics committee and the University of Southampton, reference numbers: ERGO/FEPS/67628 and ERGO/FEPS/69107 respectively. The second survey exploring privacy attitudes was approved by the Faculty of Engineering and Physical Sciences at the University of Southampton (reference ERGO/FEPS/71408). The survey as part of the saliva testing was approved by the Faculty of Social Sciences research ethics committee at the University of Southampton, reference: ERGO/FSS/61445.A1

Grant information

The original Cybersecurity study was supported under H2020 ProTego project (GA 826284). The Privacy Perceptions survey was originally supported by the DARE UK PRiAM project (UK Research and Innovation: DARE: Creating the blueprint for a federated network of next generation, cross-council Trusted Research Environments. (MC_PC_21028))

Acknowledgements

Professor Jane Falkingham at the University of Southampton was the institutional sponsor for the third study reported here.

References

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

Alsunaidi, S. J., Almuhaideb, A. M., Ibrahim, N. M., Shaikh, F. S., Alqudaihi, K. S., Alhaidari, F. A., Khan, I. U., Aslam, N., & Alshahrani, M. S. (2021). Applications of big data analytics to control COVID-19 pandemic. *Sensors*, *21*(7), 2282. https://doi.org/10.3390/s21072282

Amnesty International and AccessNow. (2018). *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*. https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf

Ashleigh, M. J., Higgs, M., & Dulewicz, V. (2012). A new propensity to trust scale and its relationship with individual well-being: implications for HRM policies and practices. *Human Resource Management Journal*, *22*(4), 360-376. https://doi.org/10.1111/1748-8583.12007

Bachmann, R., Gillespie, N., & Priem, R. (2015). Repairing Trust in Organizations and Institutions: Toward a Conceptual Framework. *Organization studies*, *36*(9), 1123-1142. https://doi.org/10.1177/0170840615599334

Baer, M. D., Matta, F. K., Kim, J. K., Welsh, D. T., & Garud, N. (2018). It's not you, it's them: Social influences on trust propensity and trust dynamics. *Personnel Psychology*, *71*(3), 423-455. https://doi.org/https://doi.org/10.1111/peps.12265

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62-77. https://doi.org/10.1016/j.dss.2015.01.009

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

Böckler, A., Tusche, A., & Singer, T. (2018). The Structure of Human Prosociality Revisited: Corrigendum and Addendum to Böckler, Tusche, and Singer (2016). *Social Psychological and Personality Science*, *9*(6), 754-759. https://doi.org/10.1177/1948550617722200

Boniface, M., Carmichael, L., Hall, W., Mcmahon, J. P., Pickering, B., Surridge, M., Taylor, S., Baker, K., Atmaca, U. I., & Epiphaniou, G. (2022). DARE UK PRiAM Project D4 Report-Public Engagement: Understanding private individuals' perspectives on privacy and privacy risk (1.0). https://doi.org/https://zenodo.org/records/10363875

Boniface, M., Carmichael, L., Hall, W., Pickering, B., Stalla-Bourdillon, S., & Taylor, S. (2022). The Social Data Foundation model: Facilitating health and social care transformation through datatrust services. *Data & Policy*, *4*, e6, Article e6. https://doi.org/10.1017/dap.2022.1

Carmichael, L., Atmaca, U. I., Maple, C., Taylor, S., Pickering, B., Surridge, M., Epiphaniou, G., Le, A. T., Murakonda, S. K., & Weller, S. (2022). Towards a socio-technical approach for privacy requirements analysis for next-generation trusted research environments. https://doi.org/10.1049/icp.2022.2061

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

Corrigan, O. (2003). Empty ethics: the problem with informed consent. *Sociology of health & illness*, *25*(7), 768-792. https://doi.org/10.1046/j.1467-9566.2003.00369.x

Desai, T., Ritchie, F., & Welpton, R. (2016). *Five Safes: designing data access for research* (Economics Working Paper Series, Issue.

Dilsizian, S. E., & Siegel, E. L. (2014). Artifical Intelligence in Medicine and Cardiac Imaging: Harnessing Big Data and Advanced Computing to Provide Personalised Medical Diagnosis and Treatment. *Current Cardiology Report*, *16*(441). https://doi.org/10.1007/s11886-013-0441-8

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *ACM SIGCAS Computers and Society*, *45*(1), 22-28. https://doi.org/10.1145/2738210.2738215

European Commission. (2002). DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE

COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

European Commission. (2019). *Ethics guidelines for trustworthy AI*. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

European Commission. (2022). *European Data Governance Act*. Retrieved October from https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosphical Transactions of the Royal Society*. https://doi.org/10.1098/rsta.2016.0360

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

Glanville, J. L., & Paxton, P. (2007). How do we learn to trust? A confirmatory tetrad analysis of the sources of generalized trust. *Social Psychology Quarterly*, *70*(3), 230-242. https://doi.org/10.1177/019027250707000303

Grady, C. (2015). Enduring and Emerging Challenges of Informed Consent. *The New England Journal of Medicines*, *372*(9), 855-862. https://doi.org/10.1056/NEJMra1411250

International Organization for Standardization. (2018a). ISO/IEC 27000:2018. In *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

International Organization for Standardization. (2018b). ISO/IEC 27005:2020. In *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.

Ioannou, A., Tussyadiah, I., & Marsham, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing*, *38*(10), 1629-1862. https://doi.org/10.1002/mar.21529

Jiang, X., Hwang, J., Shah, D. V., Ghosh, S., & Brauer, M. (2022). News attention and social-distancing behavior amid covid-19: How media trust and social norms moderate a mediated relationship. *Health communication*, *37*(6), 768-777. https://doi.org/10.1080/10410236.2020.1868064

Kadam, R. A. (2017). Informed consent process: A step further towards making it meaningful! *Perspect Clin Res*, *8*(3), 107-112. https://doi.org/10.4103/picr.PICR_147_16

Kim, K. K., Joseph, J. G., & Ohno-Machado, L. (2015). Comparison of consumers' views on electronic data sharing for healthcare and research. *Journal of the American Medical Informatics Association*, *22*(4), 821-830. https://doi.org/10.1093/jamia/ocv014

Körber, M. (2019). Theoretical considerations and development of a questionnaire to measure trust in automation. Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018) Volume VI: Transport Ergonomics and Human Factors (TEHF), Aerospace Human Factors and Ergonomics 20,

Lin, D., Crabtree, J., Dillo, I., Downs, R. R., Edmunds, R., Giaretta, D., De Giusti, M., L'Hours, H., Hugo, W., Jenkyns, R., Khodiyar, V., Martone, M. E., Mokrane, M., Navale, V., Petters, J., Sierman, B., Sokolova, D. V., Stockhause, M., & Westbrook, J. (2020). The TRUST Principles for digital repositories. *Scientific data*, *7*(1), 144. https://doi.org/10.1038/s41597-020-0486-7

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

Luo, W., Nguyen, T., Nichols, M., Tran, T., Rana, S., Gupta, S., Phung, D., Venkatesh, S., & Allender, S. (2015). Is Demography Destiny? Application of Machine Learning Techniques to Accurately Predict Population Health Outcomes from a Minimal Demographic Dataset. *PloS one*, *10*(5), e0125602. https://doi.org/10.1371/journal.pone.0125602

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44. https://doi.org/https://doi.org/10.1016/j.chb.2018.01.028

Manthorpe, J., Iliffe, S., Gillen, P., Moriarty, J., Mallett, J., Schroder, H., Currie, D., Ravalier, J., & McFadden, P. (2022). Clapping for carers in the Covid-19 crisis: Carers' reflections in a UK survey. *Health Soc Care Community*, *30*(4), 1442-1449. https://doi.org/10.1111/hsc.13474

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

Memery, J., Robson, J., & Birch-Chapman, S. (2019). *Conceptualising a Multi-level Integrative Model for Trust Repair* European Marketing Academy (EMAC), Glasgow, UK.

Mulder, T., & Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, *28*(3), 261-274. https://doi.org/10.1080/13600834.2019.1644068

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

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., Baker, K., Boniface, M., & McMahon, J. (2023). *Privacy Perspectives Survey (Version 1)*. https://doi.org/10.5281/zenodo.7589522

Pickering, B., Roth, S., Tyers, R., & Falkingham, J. (2024). *Anonymous Survey of Student Participation in a COVID-19 Testing Programme (saliva testing programme)*. https://doi.org/10.5281/zenodo.10618606

Pickering, B., & Taylor, S. (2023). *Cybersecurity Survey (Version 1)*. https://doi.org/10.5281/zenodo.7589508

Ronmark, E., Hoffmann, R., Skokic, V., de Klerk-Starmans, M., Jaderling, F., Vos, P., Gayet, M. C., Hofstraat, H., Janssen, M., & Akre, O. (2022). The effect of digital-enabled multidisciplinary therapy conferences on efficiency and quality of the decision making in prostate-cancer care. *medRxiv*, 2022.2002. 2023.21268241.

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

Rowe, F., Ngwenyama, O., & Richet, J.-L. (2020). Contact-tracing apps and alienation in the age of COVID-19. *European Journal of Information Systems*, *29*(5), 545-562. https://doi.org/https://doi.org/10.1080/0960085X.2020.1803155

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

Skatova, A., & Goulding, J. (2019). Psychology of personal data donation. *PLoS ONE 14*(11), e0224240. https://doi.org/10.1371/journal.pone.0224240

Skatova, A., Ng, E., & Goulding, J. (2014). *Data Donation: Sharing Personal Data for Public Good?* Application of Digital Innovation, London, UK.

Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization Science*, *14*(1), 5-17. https://doi.org/10.1287/orsc.14.1.5.12810

Sugarman, J., Lavori, P. W., Boeger, M., Cain, C., Edson, R., Morrison, V., & Yeh, S. S. (2005). Evaluating the quality of informed consent. *Clincal Trials*, *2*(1), 34-41. https://doi.org/https://doi.org/10.1191/1740774505cn066oa

Sushmita, S., Newman, S., Marquardt, J., Ram, P., Prasad, V., Cock, M. D., & Teredesai, A. (2015). Population cost prediction on public healthcare datasets. Proceedings of the 5th international conference on digital health 2015,

The Health Service (Control of Patient Information) Regulations 2002, (2002). https://www.legislation.gov.uk/uksi/2002/1438/contents/made

UK Government. (2020). *Data Ethics Framework*. Retrieved from https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020

UK Government. (2021). *A guide to good practice for digital and data-driven health technologies*. Retrieved from https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/

UK Health Data Research Alliance. (2020). *Trusted Research Environments (TRE). A strategy to build public trust and meet changing health data science needs*. https://ukhealthdata.org/wp-content/uploads/2020/07/200723-Alliance-Board_Paper-E_TRE-Green-Paper.pdf

UK Health Data Research Alliance, N. (2021). *Building Trusted Research Environments - Principles and Best Practices; Towards TRE ecosystems (1.0)*.

Velicia-Martin, F., Cabrera-Sanchez, J.-P., Gil-Cordero, E., & Palos-Sanchez, P. R. (2021). Researching COVID-19 tracing app acceptance: incorporating theory from the technological acceptance model. *PeerJ Computer Science*, *7*, e316. https://doi.org/https://doi.org/10.7717/peerj-cs.316

Walrave, M., Waeterloos, C., & Ponnet, K. (2020). Ready or Not for Contact Tracing? Investigating the Adoption Intention of COVID-19 Contact-Tracing Technology Using an Extended Unified Theory of Acceptance and Use of Technology Model. *Cyberpsychology, Behavior, and Social Networking*. https://doi.org/https://doi.org/10.1089/cyber.2020.0483

Wiles, R., Crow, G., Charles, V., & Heath, S. (2007). Informed consent and the research process: Following rules or striking balances? *Sociological Research Online*, *12*(2).

Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., & Acquisti, A. (2014). Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. Symposium on Usable Privacy and Security (SOUPS),