The tensions of data sharing for human rights: A modern slavery case study

Jamie Hancock
The Alan Turing Institute
London, United Kingdom

Sarada Mahesh
The Alan Turing Institute
London, United Kingdom

Jennifer Cobbe
University of Cambridge
Cambridge, United Kingdom

Jatinder Singh
University of Cambridge
Cambridge, United Kingdom
The Alan Turing Institute
London, United Kingdom

Anjali Mazumder
The Alan Turing Institute
London, United Kingdom

ABSTRACT

There are calls for greater data sharing to address human rights issues. Advocates claim this will provide an evidence-base to increase transparency, improve accountability, enhance decision-making, identify abuses, and offer remedies for rights violations. However, these well-intentioned efforts have been found to sometimes enable harms against the people they seek to protect. This paper shows issues relating to fairness, accountability, or transparency (FAccT) in and around data sharing can produce such 'ironic' consequences. It does so using an empirical case study: efforts to tackle modern slavery and human trafficking in the UK. We draw on a qualitative analysis of expert interviews, workshops, ecosystem mapping exercises, and a desk-based review. The findings show how, in the UK, a large ecosystem of data providers, hubs, and users emerged to process and exchange data from across the country. We identify how issues including legal uncertainties, non-transparent sharing procedures, and limited accountability regarding downstream uses of data may undermine efforts to tackle modern slavery and place victims of abuses at risk of further harms. Our findings help explain why data sharing activities can have negative consequences for human rights, even within human rights initiatives. Moreover, our analysis offers a window into how FAccT principles for technology relate to the human rights implications of data sharing. Finally, we discuss why these tensions may be echoed in other areas where data sharing is pursued for human rights concerns, identifying common features which may lead to similar results, especially where sensitive data is shared to achieve social goods or policy objectives.

CCS CONCEPTS

• **Applied computing** → *Sociology*; **Law**; • **Social and professional topics** → **Governmental regulations**; **Privacy policies**; • **Security and privacy** → **Social aspects of security and privacy**; • **Information systems** → **Data exchange**.

FAccT '24, June 03–06, 2024, Rio de Janeiro, Brazil

ACM ISBN 979-8-4007-0450-5/24/06
https://doi.org/10.1145/3630106.3658949

KEYWORDS

Data sharing, data governance, human rights, modern slavery, fairness, transparency, accountability

ACM Reference Format:
Jamie Hancock, Sarada Mahesh, Jennifer Cobbe, Jatinder Singh, and Anjali Mazumder. 2024. The tensions of data sharing for human rights: A modern slavery case study. In *The 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24), June 03–06, 2024, Rio de Janeiro, Brazil.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3630106.3658949

1 INTRODUCTION

Recent years have seen growing interest in sharing data, often across sectors, to improve decision-making, collaboration and transparency [24, 37, 83, 95, 114, 125]. Calls for data sharing within human rights work, and in similar fields such as the humanitarian sector, have followed these patterns [35, 100, 126, 127]. Advocates for sharing argue that data relevant for addressing human rights issues is often fragmented across disparate sectors, organisations, and databases. Data sharing, they believe, will increase transparency, improve accountability, enhance decision-making, identify abuses, and offer remedies for rights violations. Yet, these efforts may enable harms against those they seek to protect (e.g., [45]).

This paper examines how issues relating to fairness, accountability, or transparency (FAccT) in and around human rights data sharing can produce such 'ironic' consequences. We present an empirical case study: examining tensions in data sharing to address *modern slavery and human trafficking* (MSHT) in the United Kingdom (UK). Our analysis identifies several issues in human rights data sharing which help explain why such activities can raise additional rights concerns which run counter to the aims of those engaging in sharing. In contexts where sensitive data is shared, all involved must be aware of the pathways which can produce negative unintended outcomes. This awareness is necessary to ensure the effects of data sharing are fair, just, and equitable. It is especially important in human rights contexts, which typically feature extremely sensitive data on vulnerable communities.

1.1 Examining data sharing within human rights contexts

We explore a critical question for data sharing in human rights contexts: how and why can these activities create risks of additional,

even unanticipated, harms? This topic is important given the severe effects abuses wreak on human life and dignity, the sensitivity of the data that may be shared, and the impact that human rights practice can have on wider society. Human rights initiatives feed into social movements, cultural shifts, legal cases, and national policy decisions. Data and information technologies have "creat[ed] a wealth of new opportunities as well as a variety of new risks for human rights practice" [80]. Yet there remains a need for more research that scrutinises how data is shared within human rights practice. We contribute insights into why data sharing activities within human rights practice can undermine transparency and accountability rather than promote them, potentially leading to further rights violations.

Here, we define *human rights practice* as activities which seek to achieve one or more of the following goals: (1) promote adherence to human rights frameworks, such as the Universal Declaration of Human Rights (UDHR) [119]; (2) prevent abuses of people's human rights; (3) support people affected by human rights abuses.

Drawing on Gelhaar et al. [29], we analyse the data sharing relationships organisations formed as a data ecosystem: a complex socio-technical network through which case details, intelligence, and statistics flow. Actors involved in the ecosystem included victims, non-government organisations (NGOs), law enforcement agencies, and government bodies. Our results indicate an ecosystem characterised by legal uncertainties, inequalities, distrust, non-consensual data extraction, and, fundamentally, sharp power disparities – despite the altruistic aspirations of many of those involved. As such, it appears vulnerable communities were placed at heightened risk of further mistreatment including surveillance, privacy violations, discrimination, detention, deportation, and violations of the right to asylum. Ironically those with lived experience of MSHT, the people the system is intended to safeguard, were those most at risk.

Our findings are of use for human rights practitioners, researchers, policymakers, and decision-makers interested in data governance. In particular, we identify the importance of balancing the risks of sharing data versus not sharing it, as well as the tensions this balance brings about when human rights and public interests are at stake. We identify key concerns and challenges that appear to shape data sharing to address MSHT. For practitioners and researchers interested in the wider human rights sector, we outline how and why the issues raised are likely to translate to other human rights contexts. And for scholars of data governance in general, we supply empirical detail regarding how data handling and human rights practices can interact to produce unintended consequences. We note how features of our case parallel data sharing in contexts besides human rights work, such as in humanitarian and international development settings, public digital services and infrastructures, and public health and safety situations. These characteristics include the involvement of sensitive data, the risks posed if the data is misused, whether the parties involved in sharing are socially and/or organisationally similar, and pressure to balance privacy rights with policy objectives.

1.2 Context and Case Study

To explore how and why issues of fairness, transparency, and accountability in human rights data sharing activities may create risks of additional harms, we take MSHT in the UK as an illustrative case study. Our analysis is grounded in interviews and workshops with key actors in the ecosystem, ecosystem mapping exercises, and a desk-based review. Our participants were people and organisations involved directly in generating and/or using MSHT data in the UK. We focus on these participants' activities and perspectives as these actors were instrumental in directing data sharing on MSHT across the UK. Engaging directly with victims of MSHT or affected communities was out of scope.

1.2.1 What is 'modern slavery'? Under international law, 'modern slavery' and 'human trafficking' (MSHT) comprise a category of human rights violations that involve the illegal exploitation of people for personal or commercial gain [19, 54]. MSHT is referenced by Article 4 of the UDHR [119]; it encompasses forced labour, coerced criminality, sexual exploitation, and human trafficking. Ending slavery is enshrined in Target 8.7 of the United Nations 2030 Sustainable Development Goals (SDGs) [120] and is a key part of the International Labour Organisation's work [53]. A 2021 global estimate placed up to 50 million people were in MSHT at any given time [52, 129]. However, due to the "hidden" nature of MSHT, it is difficult estimate [4, 71, 122]: abusers operate in secret and observers have difficulty detecting abuses, making it challenging to determine the scale and nature of the problem. The desire for access to high-quality data to enable interventions [68, 81, 82] is often undermined by a lack of accessible, reliable data. This situation is said to leave investigators, caseworkers, and policymakers with knowledge gaps that create "intractable" challenges [68].

1.2.2 Why focus on modern slavery data sharing in the UK?. Identifying and tackling MSHT is a significant challenge for policy makers, frontline agencies serving victims, and decision-makers across many sectors. Like other rights abuses, MSHT tends not to respect legal, political, social, or other structural borders. MSHT is a complex phenomenon traversing multiple policy and political spheres: human rights, humanitarian, criminal justice, immigration, commercial, public health and others. Therefore, responses to MSHT often involve partnerships and coalitions between diverse sets of actors. Data sharing by those working to tackle modern slavery in the UK provides an excellent case study for human rights data sharing as a whole. First, MSHT is a prominent human rights abuse and is the focus of a large number of rights initiatives worldwide. Second, it typifies many of the issues human rights practitioners face regarding data quality, data scarcity, working at scale, and collaborating across social or professional divides. Third, the UK has been the site of intensive efforts to tackle MSHT, particularly with the ratification of the Modern Slavery Act 2015 which requires some organisations operating in the UK to publish statements demonstrating measures to prevent MSHT in their business and supply chains[39, 116]. Data has been positioned as central to the country's efforts, with some influential actors presenting data sharing as an important way of improving transparency and accountability,

decision-making, and the accuracy of knowledge about MSHT. Finally, these efforts have also been the subject of criticisms that data sharing carries human rights risks, including for victims of MSHT.

1.2.3 Terminology. We use the following terminology. **'Modern Slavery and Human Trafficking' (MSHT)**: the UK government uses 'modern slavery' as an umbrella term which encompasses human trafficking and slavery, servitude, and forced or compulsory labour. However, we use the acronym MSHT to emphasise the equal importance of modern slavery and human trafficking. We recognise the term 'modern slavery' is insensitive to the histories of chattel slavery, colonialism, and other institutions which legalised enslavement. Human trafficking is defined as an illegal criminal enterprise. **'Victim'** is a legal term used within the criminal justice system and other legal frameworks. **'Survivor'** is used as a term of empowerment, giving agency to victims under the law. Here we refer to people who experience MSHT primarily as **'victims'** as reflected in the law. We use the term **'vulnerable communities'** to recognise groups of people whose human rights may risk being unprotected, jeopardising their dignity and security. A person or group may shift in and out of vulnerability due to their context.

1.3 Paper overview

§2 summarises relevant literature, provides background and outlines our conceptual framework. §3 details the case study's design. §4 presents our empirical findings, including: (1) an overview of the UK's MSHT data ecosystem and the intended purposes behind data sharing; (2) the issues our participant engagements and desk-based review raised. §5 discusses how these findings relate to issues of fairness, accountability and transparency; how they may have contributed to additional human rights risks; and similar environments where these tensions are likely to be echoed. §6 concludes by discussing why issues surrounding FAccT in data sharing may feed tensions and have ironic consequences.

2 DEFINITIONS AND CONCEPTUAL FRAMEWORK

This section provides context for our conceptual approach and the relevant literature for our analysis. We introduce key concepts from Science and Technology Studies (STS), Critical Data Studies (CDS), and research on data ecosystems. We then describe how data usage and sharing have been discussed so far within a human rights context.

2.1 Fairness, accountability, and transparency

Our approach to FAccT principles is grounded in perspectives from Science and Technology Studies (STS) and Critical Data Studies (CDS). Following prominent theorists from STS, such as Latour [69], Bowker and Star [10], we view data sharing as a relational and socio-technical practice (also [75]). We emphasise that 'FAccT' regarding technology cannot be reduced to either a social or technical problem [102]. Per Selbst et al., "fairness and justice are properties of social and legal systems [...] not properties of the technical tools within" [102]. Similarly, we consider FAccT principles to be context-dependent: whether something is 'fair', 'accountable', or 'transparent' depends on the situation, the actors involved, and the principles which are prioritised. It is vital to ask: fairness, accountability, and transparency *to whom*, *about what*, *when*, and *how*? Answers to these questions are normative. As Laufer et al. write regarding how 'optimisation' is invoked, "normative choices and assumptions" are inevitable whenever such concepts are utilised [70]. All three terms revolve around power: who holds it, how should it be exercised, and how can it be held to account?

To capture the multiple meanings *fairness* has acquired [62, 102], our study examines fairness in three ways [102]: (1) distributions of power and resources; (2) the treatment of people within formal procedures; (3) the outcomes of those processes. By 'formal procedures', we refer to decision-making procedures in both organisational settings *and* technical systems. Fairness is highly contextual [72] and always involves a normative justification for why a situation is fair. Empirical cases of data sharing rarely fit a neat binary of 'fair' versus 'unfair': there tend to be many perspectives, needs, and interests to be balanced. Meanwhile, we adopt Boven's concept of "accountability as a mechanism": "an institutional relation or arrangement by which an actor can be held to account by a forum" [9, 77]). Being held to account necessitates procedures whereby actors must "justify their actions, field questions from others, and face appropriate consequences" [22]. Accountability mechanisms may be based on formal legal frameworks—such as provisions giving data subjects certain rights over their personal data—as well as technical systems [17, 18]. Finally, we draw on Turilli and Floridi's definition of transparency as "information *visibility*" (original emphasis): "the possibility of accessing information, intentions or behaviours that have been intentionally revealed through a process of disclosure" [113]. It "depends on factors such as the availability of information, the conditions of its accessibility and how the information, which has been made transparent, may pragmatically or epistemically support the user's decision-making process" [113]. Transparency is a necessary but insufficient condition for accountability in any socio-technical system: holding an actor accountable requires other actors to have accurate knowledge about that actor.

However, this does not mean that transparency is universally beneficial. Instead, we follow boyd's argument that "transparency is not enough" [11]. Information disclosures may be implemented in ways which are misleading, distracting, or which undermine people's rights. When pressured by transparency requirements, actors may disclose accurate information in formats which are inaccessible or even simply overwhelming for would-be users [87] – as when organisations only provide raw data logs, hide incriminating information within vast data 'dumps', or time data releases to minimise scrutiny [2, 6, 22, 87]. These behaviours can result in obfuscation performed in the guise of transparency, described by Heald [36] as a kind of "transparency illusion". This can result in a "transparency paradox", according to Stohl et al. [106]: disclosures may lead to more "visibility" whilst decreasing understanding (e.g. by overwhelming a recipient). Moreover, as Edwards and Veale write, "the difficulty in finding 'meaningful' explanations" for complex technical systems such as machine learning tools mean that "transparency [...] may be a non-fruitful path to take" to achieve a "solution to algorithmic concerns such as unfairness and discrimination" [22]. Trade-offs may also be made between ensuring transparency and protecting people's rights to privacy and related

concerns [34, 104, 132]. Hence, transparency is not a cure-all for injustice and inequity [22].

2.2 Data sharing and data ecosystems

We use the European Commission's definition of data sharing: "the collection of practices, technology, cultural elements and legal frameworks that are relevant to transactions in any kind of information digitally" [23]. Here, "data sharing practices" refer to "legal, technical or [...] professional procedures that are observable in the space of data sharing" [24, 29, 31, 32, 56, 90]. Data sharing is often conceptualised as occurring within 'data ecosystems': "networks composed of autonomous actors that directly or indirectly consume, produce or provide data and other related resources" [90].

To date, research in data governance has paid particular attention to how data sharing can be improved via legal and technical designs (e.g., [20, 67, 78, 131]). This work has found data sharing to be an integral component of contemporary data economies and infrastructures. It is an essential practice within domains as disparate as digital advertising [7, 18, 92], national security [63, 74], public policy [8, 114], healthcare [8, 103], and academia [59, 128]. Researchers have studied fields adjacent to human rights, such as on data sharing by humanitarian organisations (e.g., [28, 61, 66, 133]). But whilst these studies provide insights into how data sharing occurs in environments similar to human rights practice, or where human rights are at stake, such topics should not be conflated with research on data sharing in human rights practice *per se*. More work is needed that critically examines how data sharing occurs within human rights initiatives.

3 STUDY DESIGN

Our study sought to understand the legal, technical and sociocultural issues affecting data sharing in a human rights context, with a specific focus on MSHT in the UK. We use the UK's MSHT data ecosystem as a case study to explore how issues of fairness, accountability, and transparency in and around human rights data sharing can have further rights implications. We used four data collection methods: a desk-based review, an ecosystem mapping exercise, and semi-structured interviews and workshops with key actors. Our participants were people and organisations involved directly in gathering and sharing data related to MSHT in the UK.

We first conducted a desk-based review of existing literature on data sharing, data practices within human rights environments, and initiatives to tackle MSHT in the UK. This included an examination of the relevant laws, policies, and guidance by UK authorities. Then, between 2021 and 2022, we conducted sessions with key actors addressing MSHT identified in the UK ecosystem under the Chatham House Rule. These sessions consisted of workshops (3 workshops; N = 16) and semi-structured interviews (N = 37). The interviews were useful for elucidating participants' perspectives on their work and the challenges they experienced around data sharing [12]. The workshops provided feedback at different stages of the study and allowed participants to interact amongst themselves [60, 84].

Participants were recruited via three non-probability sampling strategies: convenience, purposive, and snowball sampling [94, 101]. Convenience sampling—i.e., using existing contacts in the field [26]—allowed us to use prior research relationships and connections as entry points [109]. Snowball sampling enabled us to leverage participants' knowledge of their own networks [91, 94]: by expanding the sample pool using interviewees' recommendations, we followed the social ties spanning the sharing ecosystem. Our sample is not statistically representative of the actors tackling MSHT in the UK; instead, it captures the views of prominent figures in this ecosystem (Table 1). All participants provided informed consent in accordance with our institute's ethics review process. Their names and details have been anonymised (Table 2)

Type	Examples	Count
Non-profit sector	Front line service providers	11
Law enforcement	Police forces, central agencies	10
Public sector	Civil servants, local government	7
Private sector	Manufacturers, consultancies	6
Research	Academics, independent researchers	3
	Total	37

Table 1: Breakdown of interviewee sectors and counts

Name	Sector	Organisation type
Participant 1	Private sector	Consultancy
Participant 2	Private sector	Research
Participant 3	Private sector	Independent contractor
Participant 4	NGO	Research
Participant 5, 6 (group interview)	NGO	Research
Participant 7	NGO	Frontline service provider
Participant 8	NGO	Frontline service provider
Participant 9	NGO	Frontline service provider
Participant 10	Law enforcement	Police
Participant 11	Law enforcement	Police
Participant 12	Law enforcement	Police
Participant 13	Law enforcement	Central agency
Participant 14	Public sector	Health care
Participant 15	Public sector	Government department
Participant 16	Public sector	Government department
Participant 17	Public sector	Government department
Participant 18, 19, 20 (group interview)	Public sector	Government department

Table 2: Codenames and details for quoted participants

The interview and workshop transcripts were coded using thematic analysis [5, 16] and discourse analysis [111]. These methods were selected to identify: (1) common topics and views shared by participants; (2) the discourses they invoked. Thematic coding is based on annotating and categorising qualitative data according to thematic 'codes' [110, 130]. Discourse analysis, meanwhile, examines how language is used to construct meaning and mould social reality [111]. Multiple team members reviewed our analyses independently to check for intercoder reliability [5]. Our final results are presented in §4. The workshops also included an ecosystem mapping exercise wherein participants recounted the data sharing relationships they knew of. Our approach to data ecosystem

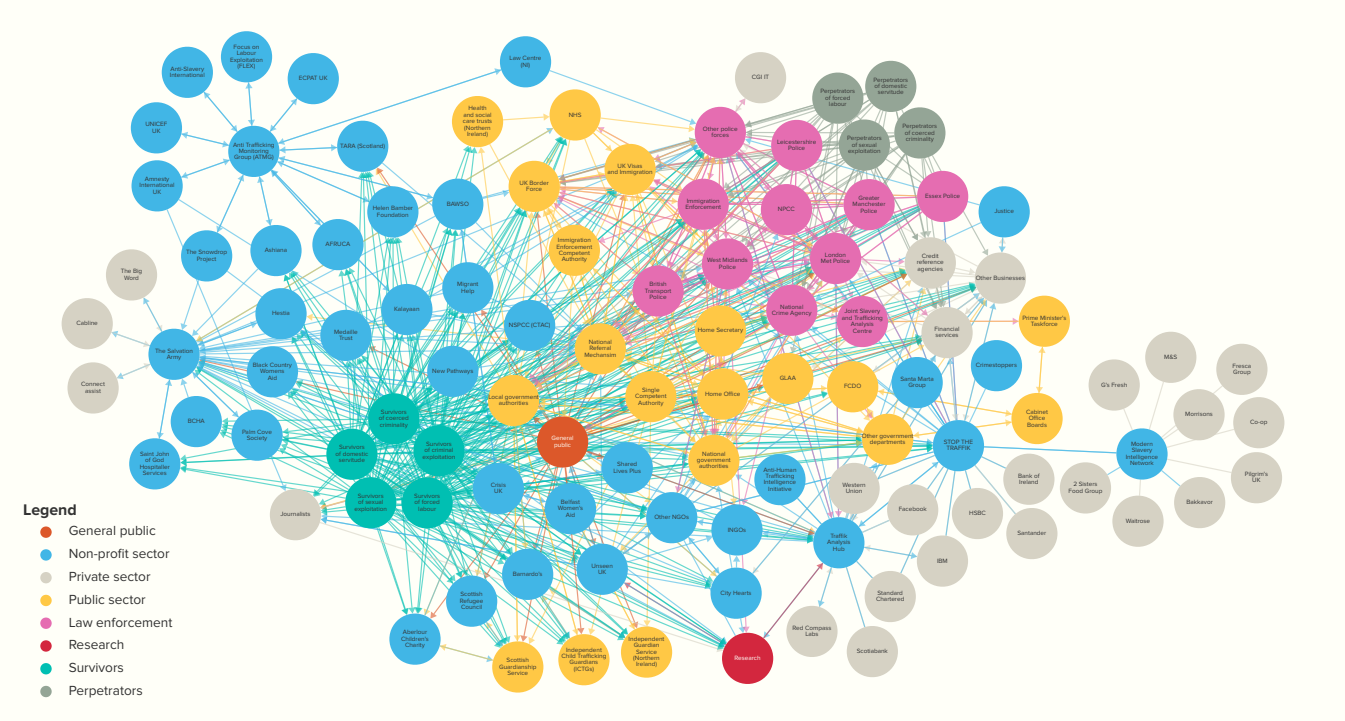

Figure 1: A map of the UK's modern slavery and human trafficking data ecosystem. Interactive version: https://embed.kumu.io/42466830b6b3374e56ec21ce10965714.

mapping followed the methods established by Oliveira et al. [89], Jaspersen and Stein [57], and others [79, 88, 124]: (1) attendees described the actors and data sharing relationships they were aware of; (2) attendees collaborated to produce a map based on these recollections, which gave them an opportunity to further discuss their perspective; (3) we followed up with post-workshop and post-interview survey to elicit final responses; and (4) we contributed data sharing relationships found through our desk-based review. Figure 1 visualises the complete set of descriptions of relationships identified.

4 CASE STUDY: DATA SHARING IN THE UK'S MODERN SLAVERY ECOSYSTEM

We now summarise our findings. After mapping the MSHT data ecosystem and outlining the goals behind its creation, we examine the main themes raised: law issues, technical systems, procedures, downstream governance, and distrust.

4.1 The UK's Modern Slavery and Human Trafficking data ecosystem

Data relating to MSHT in the UK was gathered within a complex ecosystem formed from many kinds of sharing relationships. From interviews and organisations' public modern slavery statements, we identified data sharing parties in the following sectors: non-profit NGOs, businesses, public services, police forces, and government departments. Key actors included the Home Office—the UK's lead government department responsible for immigration and passports, crime and policing, fire, and counter-terrorism [42]—and NGOS such as The Salvation Army. These held central positions in the MSHT data ecosystem and acted as 'hubs' managing dataflows between other actors. The prominence of such was a direct result of policymaking. The National Referral Mechanism for Modern Slavery and Human trafficking (NRM) is a UK-wide framework (and data system) for identifying and referring potential victims of MSHT and ensuring they receive the appropriate support [43]: it is a unit within the Home Office that is responsible for integrating and storing data and producing statistics from statutory and non-statutory first responders across the UK, including police forces, border force, local government, helplines and support services run by NGOs [21]. The Salvation Army, at the time of this study, held the contract for managing the support to identified victims. Actors on the ecosystem's periphery—i.e., ones which only engaged in sharing to a limited extent and/or interacted with comparatively few other actors—included small NGOs, local government services, businesses, and companies providing data analysis products (e.g. IBM [112]).

Many different sources and types of data were processed, analysed, shared, and repackaged for further use within the ecosystem. They included: victim testimonies; witness reports; calls to helplines; public tipoffs; inspections; financial records; and, occasionally, from social media. Victims of MSHT and the general public appeared to be the most common initial sources for data. Such data would enter into the ecosystem via a set of 'front-line' actors such

as service providers and police forces, as well as businesses. From there, it passed through a series of mediating hubs like the NRM, which collated, processed, and aggregated data for downstream use. At the end of the chain of exchanges, data tended be acquired by a small group of core organisations (e.g., the Home Office).

Figure 1 visualises the MSHT data ecosystem. Actors are colour-coded according to their sectors. Connections represent established exchange relationships, through which the actors provided raw data, statistics, datasets, metadata, verified intelligence, or other relevant material. Arrows point in the direction data travels from one actor to the other, in the colour of the sending party. Actors towards the middle have more connections (both sharing and receiving) and are therefore presented as more central. For an interactive version of the map see here.

The desk-based review and engagement activities indicated the ecosystem was governed by a complicated lattice of legal infrastructures, contracts, and sharing agreements, in which the Modern Slavery Act 2015 was pivotal. Organisations subject to the Act were required to publish an annual 'Modern Slavery Statement' (MSS) demonstrating the measures being taken to prevent MSHT in their businesses and supply chains to a government registry [40, 44, 116]. These disclosures were designed to establish transparency, encourage preventative approaches, and assist the criminal justice system in targeting perpetrators and protecting victims. Other legal and policy structures undergirding the ecosystem included: the UK's data protection law, the UK GDPR [118] and Data Protection Act (DPA) 2018 [117]; Freedom of Information requests (FOIs) submitted under the Freedom of Information Act 2000 [49, 115]; guidelines from the Information Commissioner's Office (ICO) [48]; and specific data sharing agreements (DSAs) between parties (see [50]; e.g., [55]).

Together, the evidence indicated that MSHT data sharing relationships formed a large, heterogenous network governed by a sizeable but hard-to-determine number of rules. It was internally fragmented into smaller clusters based on sectors and groups of actors that performed similar roles. The ecosystem is best understood as a decentralised data supply network—the networked, non-linear equivalent of a data supply chain [18]—structured hierarchically into a small set of core actors and many peripheral sub-networks. This structure is consistent with the findings of other studies on data sharing ecosystems (e.g. [29, 30]). It seems reflective of the diverse array of sectors and actors that tend to be involved in human rights initiatives, as well as the power differentials that often lie between them.

4.2 Goals and intended purposes for data sharing

It is helpful to understand the aims behind MSHT data ecosystem's creation. Though components of the ecosystem existed beforehand, the UK Modern Slavery Act 2015 was a foundational piece of legislation, establishing many core mechanisms of MSHT data exchange (e.g. Modern Slavery Statements; Home Office data supply contracts). The Home Office stated the Act was intended to "give law enforcement the tools to fight modern slavery, ensure perpetrators can receive suitably severe punishments for these appalling crimes and enhance support and protection for victims" [116]. Equivalent language exists in the UK Government's guidance for the NRM: the system exists to help "identif[y] and refe[r] potential victims of modern slavery and ensur[e] they receive the appropriate support" [43].

Such statements indicate three primary aims behind the data sharing infrastructure: (1) to enhance the identification and prosecution of cases of MSHT; (2) to support victims and communities affected by MSHT; and (3) to track the rates and distribution of MSHT across the UK. The Government's statements convey the moral gravity of MSHT, emphasising the vulnerability of "potential victims", and present data (and data sharing) as a means to meet policy aims.

Many participants echoed the moralised and victim-centred aspects of official discourse. For P4, it was "morally [...] right that we share because there are people at risk". P10, a law enforcement officer, said people working to tackle MSHT "owe[d] it" to "victims" of MSHT to share and use the data available to the fullest extent. Similarly, P2, a private sector consultant, saw data sharing as a way to prevent "repeated victimisation": by circulating detailed data about a case, practitioners would remove the need for victims to recount their stories multiple times. P3, an independent private sector consultant, believed that without such a "joined up" approach, there was a risk people would "fall through the gaps". One civil servant (P15) claimed the "information" needed was "there, but there [was] an accessibility problem". Meanwhile P7, from an NGO, saw data sharing as critical for understanding people's journey through the exploitation cycle and justice system, as no one organisation held the data. P7 believed data sharing could provide this overview, improve transparency, and enable better interventions. They said the field "still d[idn't] know how much modern slavery exists, where, or why"; without data sharing, the field was "stabbing in the dark operationally [and] at a strategic level".

Overall, participants articulated moral and ethical imperatives to data sharing to help prevent injustice, enable accountability and transparency, and ensure fairer outcomes for those harmed by MSHT. These positive intentions are significant insofar as they were in tension with participants' concerns about how data sharing occurred in practice.

4.3 Legal issues: misconceptions, differing interpretations, limited knowledge

The law was perceived as particularly salient for data sharing, both as a source of risk and a means to reduce it. Legal frameworks—particularly data protection laws—were presented as both enabling *and* preventing data sharing, even when participants perceived such sharing as beneficial to victims, service delivery and improving decision-making. P15, who worked in the public sector, typified this sentiment by depicting the legal landscape as akin to a minefield: uncertain, dangerous, and requiring careful navigation. P15 claimed the "vast majority" of barriers to data sharing related to legal concerns. Ensuring legal compliance was described as a "genuine barrier" to sharing because it consumed time and resources. P17, a government employee, explained legal practices constrained sharing even within the government themselves, and considered the situation to be unfit for the department's needs. In the non-profit sector, P8 said, stipulations in contracts could create "constrictions

around what [organisations could] share". Such comments were broadly representative of how participants tended to perceive and present legal issues as obstacles preventing sharing.

However, most participants also acknowledged that UK data protection law was not well understood by those with whom they interacted. For example, P7, a prominent figure in the non-profit sector, told us that "the majority" of people in his field were "not experts" in data protection. Participants expressed uncertainty about which legal frameworks applied to them, especially regarding who held responsibility for data and when. The UK Information Commissioner's Office (ICO) provides precise guidance on how to share data whilst complying with the law, writing that "data protection law is an enabler for fair and proportionate data sharing". In fact, many of the legal issues raised, particularly around data protection and data sharing, seemed to derive not restrictions or limits of the law – but rather from a lack of understanding of the law and provisions for data sharing. These perceptions may have manifested due to administrative constraints or concerns, or how particular laws and guidance were being operationalised within organisations. Overall, it appears actors' and participants perceptions about the law had led them to withold information and data from one another in the name of legal compliance, feeding an impression that the ecosystem was opaque as a whole.

Meanwhile, victims and affected communities were in a precarious position when it came to the legal protection of their data rights. These communities faced systemic "challenges in accessing legal advice" due to a lack of legal aid funding, limited awareness of their rights, and constrained practical access to aid [27]. Furthermore, it appeared that the opacity of the data supply chain had increased concerns about data's provenance, lineage, and potential misuse (see [18]). We suggest the complexity of the MSHT data ecosystem's legal governance may make respecting data rights worse. The intricacy of ecosystem's legislation, guidance, policy, and contracts would likely compound barriers to accessing legal redress, making it difficult for victims to exercise their data rights. Because decision-making processes about whether to forward on case data were opaque, it appeared extremely difficult to pinpoint responsibility in the circumstance that third party data usage had put people at risk. Such a situation would make it very hard for people to withdraw consent for sharing and retake control of their data. Further, due to policy objectives and exemptions in data protection law, data could be shared in ways that could leave victims in precarious positions and limited their data (and other) rights. As a consequence, the human rights of those contributing to the ecosystem may be undermined.

4.4 Technical and infrastructural issues: data standardisation and interpretation, system interoperability

Participants expressed concerns regarding technical or infrastructural issues centred on three areas: (1) resources, limitations and uses of data infrastructures and systems; (2) difficulties in establishing interoperability between systems; and (3) the standardisation and understanding of the data generating processes.

According to one NGO worker, many MSHT data systems and tools had developed haphazardly. Rather than scrapping outdated systems and creating new ones, managers opted to add functionality to existing systems (i.e., 'function creep') and increase their scope ('scope creep') beyond their original intent [64, 65, 99]. These paths seemed easier and cheaper in the short term; but over time, in this participant's account, some databases' "foundations" became "crappy". Additionally, it was expressed that smaller organisations could lack the resources or capabilities to fully utilise the systems and data they already had access to. By way of illustration, P3 spoke about one NGO that held large amounts of text data but did not "have the tools to mine [it]".

Multiple participants complained that data systems across the ecosystem had come to lack interoperability or technical standardisation, leading to data duplication, fragmentation, and poorly utilised resources. Participants spoke of a lack of agreement regarding categories and typologies. A civil servant, P15, shared that, even within government, organisations did not "always work to common definitions". This was said could contribute to misunderstandings, incompatibilities in datasets, conflicts between would-be collaborators, and ineffective partnerships. P15 claimed the result was a "goldmine" of data "just sitting" in disconnected databases, unused. The feasibility of establishing interoperability was also expressed because "people want[ed] data or the system to do things which can be at odds" (P3). It was "a headache".

Concerns about a lack of understanding in the ecosystem's data generating process in some hubs such as the NRM, resulting in biased interpretations. One workshop attendee illustrated the issue by claiming data on Romanian victims may have been overrepresented, as significant resources and expertise had been directed specifically at tracking Romanian cases. The hidden nature of MSHT may then be compounded by a disproportionate picture of different typologies, rates and source country of victims, skewing interventions and policies, reinforcing bias, and leading to downstream misuse. We note here that recent immigrants and other communities most affected by MSHT are already more surveilled and policed compared to the general population [86], which could lead to further over-representation of their information in datasets on MSHT.

4.5 Operational and Procedural Issues: Informal and insecure data handling practices

Participants also expressed concerns that best practices when handling data were not being followed. Disaggregated data on cases of MSHT and other human rights abuses may incorporate highly sensitive information, such as victims personal details and facts about ongoing criminal investigations. Under both UK data protection law and the principle of the right to privacy (UDHR Article 12 [119]; also [46, 121]), handling MSHT case data usually necessitates strict safeguards for privacy and security, although legal exemptions (e.g. for security or law enforcement reasons) and policy objectives could mean such information was more readily shared. While aggregate or anonymised MSHT data may not have been as sensitive, the nature of the subject matter meant a level of caution was still needed to protect victims.

We heard accusations that actors in the ecosystem were not following good data protection, privacy, and security standards. The non-profit and law enforcement sectors were raised specifically as

sectors where this was prevalent. P3 claimed the "handling, management, and usage of case data to support survivors" was "immature" in the non-profit sector, leading to "ad hoc spreadsheets and thrown together systems". As a result, P7, from an NGO, responded stating that they made data protection and security a priority; however, this was very difficult as there needs to be "sufficient funding" to ensure this, as well as "sufficient safeguards and understanding" around the correct ways to "aggregate and anonymise" the data. Another consultant expressed concern about the lack of "safeguards" involved in such practices: "absolutely no way, I'm not sharing anything in an Excel spreadsheet" (P1). Meanwhile a public sector worker (P19) suggested that sharing within law enforcement could "be quite informal". These claims painted an overall image where a significant volume of potentially sensitive data was being exchanged in informal and, at worst, insecure ways. They imply a lack of standardisation, clarity, or adherence to best practices across certain sectors of the ecosystem. Given the nature of this data, the consequences of a data breach due to substandard data handling could be devastating.

4.6 Downstream risks from sharing: data reuse and misuse

It appears concerns about legal matters, data protection, inaccurate data, and the behaviour of other parties had contributed to a pervasive atmosphere of risk. This perception was directed primarily at parties who were downstream in the data supply chain: there was a common perception that sharing data was risky because of the ways it could be (mis)used once it had been passed on. The most prominent risk came from data reuse – where data is gathered and shared for one purpose but then repurposed without the awareness and/or consent of the person who provided the data.

Participants from frontline agencies argued that downstream sharing was neither transparent nor accountable – and, therefore, was a source of risk for data subjects. They suggested the further away a data subject's data travelled from them, the less clear it became on how it was being used and or how to prevent misuses (see e.g. [18, 105]). These issues of data provenance and lineage were echoed primarily by NGOs—often the data stewards and gateway for many victims of MSHT reporting—who purported a lack of control. P1 expressed concern that such opacity and the risk of data repurposing could have a chilling effect on the victim engagement: "If someone shares data and somebody else acts on it in a way that's detrimental, a person may not share data again".

In 2018, two NGOs lodged an official complaint which alleged "police share the data of victims and witnesses of [modern slavery] crimes with the Home Office for immigration enforcement purposes" [73]. His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS)—the government body responsible for police accountability—found evidence supporting that the information passed to immigration officials may be "enabling offenders and abusers" who "use police involvement as a threat to their victims". "Victims are denied justice, while offenders go unpunished and remain a threat to the public" [38]. Whilst the HMICFRS' report called for a "firewall" between the government's MSHT data systems and its immigration infrastructure [38], the Home Office declined to make these changes [41].

We also heard concerns about the potential for supposedly anonymised data to be de-anonymised once it was shared with another party. While the majority of organisations represented in our study were said to anonymise the data they shared, this was not a guaranteed way to protect privacy and security. As P9 put it, "you can put lots of individually anonymous data together and if somebody has sufficient local knowledge, they might be able to put the pieces together and identify somebody." P9's comment is consistent with research on re-identification via data linkage from multiple anonymised or synthetic datasets. Many studies have shown how an actor may triangulate multiple datasets to re-identify individuals [1, 58, 85, 97]. In the case of MSHT, the ability to re-identify would be held disproportionately by the most central actors in the ecosystem (e.g., government departments, police forces, and prominent NGOs), as well as organised crime networks.

4.7 Distrust and suspicion

The cumulative consequence of the concerns presented was an atmosphere of distrust. At least three participants from three sectors said powerful organisations and technical systems could be a "black hole" to outsiders: actors sucking in data whilst offering no transparency or value in return. These actors or agencies could leverage their central positions in the ecosystem to hoard data for their own uses, whilst denying the opportunity for accountability, reciprocity, or fairness. The Home Office was the most frequent subject of such accusations. P15 claimed this problem was most severe for victims and other more marginal communities, resulting in "the level of reporting from individuals [was] very low".

Suspicion appeared particularly acute across sectoral divides. Participants often appeared to assume negative intentions in those from outside their sector. Members of the public sector, for example, articulated hesitancy to provide information to journalists and NGOs, whom they deemed as "having a particular agenda" in their data requests (P13). This "agenda" was implied to be hostile towards the participant's department – or, at least, to undermine their public policy aims. "You're not going to give a journalist [a] free range of data". Another civil servant alleged that NGOs would sometimes "exaggerate the threat" the government posed to survivors of MSHT so they could "demonstrate their value" (P19). Consultants in the non-profit sector made similar remarks about law enforcement and immigration agencies: when discussing the Border Force, P1 argued the agency's "goals and targets ma[de] exploitation more likely." Comments like these indicate the degree to which actors across the ecosystem lacked trust in one another's motives, capabilities, and actions. We suggest they expose a critical issue: the ecosystem posed fundamental challenges for fairness, accountability, and transparency.

5 DISCUSSION

We now draw on our results to examine the wider significance of the issues in the MSHT data ecosystem in relation to FAccT principles, and the additional factors that may lead to further rights violations when data is shared within human rights contexts. These include barriers preventing victims from accessing legal remedies, privacy violations, and data misuses that lead to serious individual and policy harms. We argue our case exemplifies tensions for fairness,

transparency and accountability which might arise in other similar data sharing environments.

5.1 Transparency

The UK MSHT data ecosystem has significant transparency issues. Opacity was prevalent in many areas: which actors participated in data sharing; what was shared; the specific paths data could take through the ecosystem; how it was processed; what it was used for; if and how it was repurposed or re-shared; and more. Participants expressed frequent frustration about their lack of knowledge about data held by other actors, many of whom they were only connected to via intermediaries. The issue was epitomised by the figure of the "black hole": an actor or system into which data seemed to simply disappear. This metaphor recalls Cobbe et al.'s concept of the "accountability horizon" in data supply chains, defined as "the point beyond which an actor cannot 'see'" within the chain of data exchanges [18]. The situation is ironic considering one of the aims of the Modern Slavery Act 2015 is to *promote* transparency. Opacity about the ecosystem's activities had contributed to widespread distrust and, in turn, may have had a chilling effect on data sharing, thereby potentially limiting insights into MSHT itself. We contend this scenario highlights a fundamental challenge for transparency in data ecosystems: as sharing networks scale, it may be increasingly difficult to identify all third parties who receive data downstream, receive transparency disclosures, or establish trust. This problem is liable to grow in proportion to the length and complexity of an ecosystem's data supply chains.

Transparency over the practices of sharing data—a kind of *operational* or *procedural transparency* [3, 13, 107]—is vital for embedding trust and accountability within human rights data sharing ecosystems. We take operational transparency to encompass disclosures about what kinds of data have been collected, where it has travelled, if it has been duplicated, and how it is used. Nonetheless, operational transparency is not appropriate as a blanket approach. Indeed, disaggregated case data relating to ongoing criminal investigations was exempt from requests under the UK's Freedom of Information Act [51, 115]. This illustrates the importance of managing competing interests and forms of public good when transparency requirements are designed. Moreover, to avoid creating the illusion of transparency [22, 36], disclosures need to be accessible and manageable for their recipients [87]. Given the ecosystem's size, there is a risk victims and advocates could be overwhelmed by disclosures – ironically *reducing* transparency.

More generally, transparency is a contextual good which must be balanced with other factors including rights to privacy and security from harm. There are compelling arguments for why sensitive personal data about people involved in and/or affected by crimes or human rights violations should not be made public (see [11]), including the possibility of re-targeting by abusers or vigilantes, particularly as this data may be combined with other data, risking re-identification. Further, there are circumstances where people may be simultaneously considered as 'victims' *and* criminal 'perpetrators' within cycles of victimisation [25, 98] due to illegal activities they were forced to commit (including illegal migration). Any disclosure of their details could therefore risk their re-criminalisation or otherwise create further legal jeopardy. Finally, as discussed above, there is a danger that overly general calls for insights into MSHT through data without good governance practices will enable an expansion of mass data collection which aggravates surveillance creep.

5.2 Accountability

Without adequate transparency around data sharing activities, it becomes harder to hold people and organisations to account for failures or mistreatment [18]. For instance, whilst the sharing of information on victims of MSHT between police and immigration enforcement was legal (and expected), it may have led to vulnerable people being denied access to safeguarding services or being deported to circumstances of further harm. These situations threaten victims' rights to effective remedies and non-refoulement.

Oversight and accountability mechanisms are vital for ensuring that the systems used to gather and share MSHT data do not undergo further function creep. Efforts to tackle modern slavery could drift towards datafied surveillance ('dataveillance'; [15, 123]) and what Birchall terms 'shareveillance': "a state in which we are always already sharing" [7]. Thanks to the ubiquity, automaticity—and often invisibility—of data sharing, Birchall argues, would-be surveillants benefit immensely as they combine data received from nebulous sources.

Accountability mechanisms could help counterbalance the disparities in power and resources observed across the data ecosystem. The forms accountability takes between an NGO and a government department within a contract to provide data processing services, for instance, will be substantively different when compared to the NGO's relationship with affected communities and responsible for stewarding their data. This is made more difficult through the opacity of the data supply chain. The most vulnerable and powerless, such as victims of MSHT, must be able to access accountability mechanisms — particularly as it relates to data.

5.3 Fairness

Issues with transparency and accountability in data sharing may combine to produce a problematic environment for establishing fairness. Unfairness may manifest in multiple ways: unequal distributions of power and resources; the differential (mis)treatment of people by the ecosystem's processes and outcomes; in imbalances in who could generate, gather, control, process, or use data; and via inequities in how data was handled, exchanged, or ultimately used. In such a complex, moralised environment, fairness—whether process versus outcome, or individual versus group—is unlikely to be applied uniformly. It could appear a sharing situation emerges as simultaneously fair and unfair depending on the definition and context. Questions of fairness to whom, for what purpose, and at what scale must be asked.

For MSHT, the collection and sharing of data could misrepresent the nature and distribution of cases, negatively affecting decision-making. This can have discriminatory effects on victims and other vulnerable communities. Unrepresentative data poses a serious threat when datasets are layered, triangulated, and used in wider systems, and problems may arise, for example, should reporting and case data be used to train machine learning systems. If used to guide interventions like predictive policing systems, this may reinforce

unfair and discriminatory outcomes for marginalised communities [76, 96]. Flawed interpretation of the data may have political consequences: MSHT in the UK has been a point of national political contention in recent years, with government ministers alleging that claims for safeguarding are often fraudulent attempts to avoid being deported for immigration offences [33, 93, 108]. Such arguments can stem from (mis-)interpretations of statistics about MSHT derived from the MSHT data ecosystem. Allegations of widespread fraud in the system have been challenged vigorously and are not supported by the government's own data [47].

Questions of distributional fairness should also be posed at meso (i.e., organisational) and macro (i.e., societal) scales. On an organisational level, participants from NGOs expressed frustration at what they perceived to be opaque and unfair relationships between civil society groups and government bodies. At a societal scale, data gathering intended to help tackle MSHT may encourage shareveillance and segue into dataveillance.

5.4 Similarities to other data sharing contexts

MHST illustrates how using data to address human rights issues risks contributing to additional human rights violations, particularly when dealing with sensitive data and tensions with other policy objectives. The challenges we identified in the MSHT data ecosystem may also appear in comparable environments, such as humanitarian, public health and public safety settings. We suggest there are three features which make such replication likely: (1) risks of individual and group level harms (e.g. discrimination, retargeting or victimisation); (2) the complex data supply chains that cross sectors and borders; and (3) situations where legal and policy instruments limit access to data protection rights. These issues are likely to be exacerbated when the primary sources and subjects of the data being handled are victims of human rights violations. Such people can be highly vulnerable if their data is misused, if they lack oversight over their data, or if mechanisms for remedy are opaque and inaccessible.

For example, MSHT data sharing echoes examples of data protection incidents in humanitarian settings. In 2021, Human Rights Watch reported that the United Nations High Commission for Refugees (UNHCR)—which is mandated to aid refugees, forcibly displaced communities, and stateless people—shared sensitive personal data on refugees from Myanmar's Rohingya ethnic minority who sought refuge in Bangladesh with the Bangladeshi government. In turn, Bangladesh passed it to the government of Myanmar – the very state that people were seeking refuge from [45]. These cases share several characteristics: they involve actors handling sensitive personal data on potential victims of rights violations; they occur in complex environments where many organisations operate from many sectors; and they centre on the role of state actors, which may exercise sovereign power to request data and/or withhold it.

Moreover, our case study illustrates how issues with FAccT principles can emerge as data ecosystems increase in size, order, and complexity. Take transparency: as actors and relationships grow in a given ecosystem, it becomes harder to accurately describe the ecosystem as a whole. Any actor seeking an accurate overview of the ecosystem will therefore require an increasing amount of information. If the ecosystem grows in a decentralised manner, it is likely it will become more laborious to identify data holders and trace data flows [92]. Moreover, it is plausible powerful actors could leverage their position to control information flows to their benefit by constricting transparency [14]. These issues of scale and complexity have similar implications for accountability. As a data sharing network grows in size and complexity, whether the overall ecosystem or any of its constituent relationships is 'fair' or responsible becomes increasingly difficult to ascertain. Consequently, diverse and complex data ecosystems are likely to feature a multitude of moral/ethical constituencies with competing interests and perspectives, thereby exacerbating fairness challenges.

Key takeaways
Lack of operational transparency about data sharing operations risks undermining data subjects' rights
Complexity and scale of data ecosystem makes transparency more difficult to establish
Transparency must be balanced against privacy and other rights
Few effective mechanisms for accountability or for the most marginalised to seek redress
Danger of drift towards surveillance/shareveillance
Many interacting parties and goals mean it may be difficult to decide on a 'one-size-fits-all' approach to fairness
Risk of data sharing contributing to further discrimination and harms against vulnerable communities (e.g. survivors)
These issues are likely to be repeated in other cases of human rights data sharing

Table 3: Summary of key takeaways

6 CONCLUSION

Well-intentioned attempts to share data within human rights initiatives can enable harms against the very people they seek to protect. Efforts to challenge MSHT in the UK provide an instructive example of how this can occur. In the span of just under two decades, a complex ecosystem of data providers and users had emerged. The system's stated aims were to better identify cases, increase prosecutions of perpetrators, improve support for victims, and enhance the country's overall understanding of MSHT. Yet issues ranging from confusion about the law to allegedly insecure data practices appeared to have undermined such goals. As a consequence, vulnerable people interacting with the ecosystem—victims of MSHT and their communities—may have been exposed to further harm.

Our case demonstrates how a lack of fairness, accountability, and transparency in data sharing can constitute a human rights issue in their own right. Inadequate transparency over data sharing may impede effective remedies, social rights, protections, and access to public services. Such issues are especially acute as data travels further away from the control of its original holder or provider.

If actors and/or systems downstream are not trustworthy, gaps in accountability or transparency also raise concerns regarding privacy and cyber-security vulnerabilities.

Ensuring that data sharing is genuinely beneficial demands an awareness of why negative human rights consequences can emerge and how they can be mitigated. This is especially true if the reason for sharing data is to *promoteand respect* human rights. All those involved in data sharing—whether as system designers, data providers, or recipients—must be cognisant of the how these practices may put human rights at risk. Yet, the contextual nuances of specific data sharing relationships and mechanisms within human rights data ecosystems may pose a fundamental challenge to 'one-size-fits-all' approach to fairness, accountability, and transparency in technology. We therefore advocate for more scrutiny of the role played by (un)fairness, (un)accountability, and (non-)transparency in data sharing for human rights – within human rights contexts and beyond.

RESEARCHER POSITIONALITY STATEMENT

We are a diverse, multi-disciplinary research team that hold multiple identities. Most of us were educated in the Global North. We acknowledge that our educational histories, professional backgrounds, and positionality as researchers based at prominent UK research institutions confer us a high degree of privilege compared to those most impacted by the subject of our work – namely, victims of MSHT and other affected communities.

We did not engage directly with people with lived experience of MSHT. Our study focused on the practices and perspectives of diverse actors in the MSHT data sharing ecosystem: the data stewards and receivers of highly sensitive data regarding victims of MSHT. We also did not ask participants to share victims of MSHT's views. Whilst many of the participants are from frontline agencies engaging directly with victims of MSHT, further study is needed to document how those with lived experiences perceive data sharing practices. Our knowledge of the experiences of those facing rights violations is from our professional work, rather than our personal lived experiences.

Moreover, our positions as academics and researchers conferred us privileged access to speak to prominent figures across the MSHT data sharing ecosystem, which most people (i.e. victims of MSHT) interacting with the ecosystem would lack. By applying a rigorous, standardised qualitative analysis methodology, we have endeavoured to ensure our analysis is not weighted unfairly towards any one set of participants.

ACKNOWLEDGMENTS

We thank the participants for contributing their time and expertise. We are grateful to Sunny Dillon, Alys McAlpine, Holli Sargeant, Jovan Powar, Mark Briers, Eirini Malliaraki, Andrew Wallis, the Open Data Institute, and the Modern Slavery Data Group for their contributions during prior stages of this research project. We thank the Chair and reviewers for their helpful suggestions on improving this manuscript. And thanks to Ruoyun Hui, Emma Kallina, Yesim Kakalic, and Harry Bowles for feedback throughout the manuscript journey.

This work was funded by the Modern Slavery and Human Rights Policy and Evidence Centre/AHRC and The Alan Turing Institute. Funds were also received through Wave 1 of The UKRI Strategic Priorities Fund under the EPSRC Grant EP/T001569/1 and EPSRC Grant EP/W006022/1.

REFERENCES

[1] Dalal Al-Azizy, David Millard, Iraklis Symeonidis, Kieron O'Hara, and Nigel Shadbolt. 2016. A literature survey and classifications on data deanonymisation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9572 (2016), 36–51. https://doi.org/10.1007/978-3-319-31811-0{_}3/COVER

[2] Mike Ananny and Kate Crawford. 2018. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society* 20, 3 (3 2018), 973–989. https://doi.org/10.1177/1461444816676645

[3] Gloria Andrada, Robert W. Clowes, and Paul R. Smart. 2023. Varieties of transparency: exploring agency within AI systems. *AI and Society* 38, 4 (8 2023), 1321–1331. https://doi.org/10.1007/S00146-021-01326-6/TABLES/1

[4] Kevin Bales. 2005. *Understanding global slavery: a reader.* University of California Press, Oakland, CA. https://www.ucpress.edu/book/9780520245075/understanding-global-slavery

[5] Michael J Belotto. 2018. Data Analysis Methods for Qualitative Research: Managing the Challenges of Coding, Interrater Reliability, and Thematic Analysis. *The Qualitative Report* 23, 11 (2018), 2622–2633.

[6] Clare Birchall. 2011. Introduction to 'Secrecy and Transparency'. *Theory, Culture & Society* 28, 7-8 (12 2011), 7–25. https://doi.org/10.1177/0263276411427744

[7] Clare Birchall. 2016. Shareveillance: Subjectivity between open and closed data. *Big Data & Society* 3, 2 (11 2016). https://doi.org/10.1177/2053951716663965

[8] Michael Boniface, Laura Carmichael, Wendy Hall, Brian Pickering, Sophie Stalla-Bourdillon, and Steve Taylor. 2022. The Social Data Foundation model: Facilitating health and social care transformation through datatrust services. *Data & Policy* 4 (2022). https://doi.org/10.1017/dap.2022.1

[9] Mark Bovens. 2007. Analysing and Assessing Accountability: A Conceptual Framework1. *European Law Journal* 13, 4 (7 2007), 447–468. https://doi.org/10.1111/J.1468-0386.2007.00378.X

[10] Geoffrey C Bowker and Susan Leigh Star. 1999. *Sorting things out: classification and its consequences.* The MIT Press, Cambridge, MA.

[11] danah boyd. 2010. "Transparency Is Not Enough.". *Gov2.0 Expo* (2010). http://www.danah.org/papers/talks/2010/Gov2Expo.html

[12] Svend Brinkmann. 2017. The Interview. In *The SAGE Handbook of Qualitative Research* (5 ed.), Norman K. Denzin and Yvonna S. Lincoln (Eds.). SAGE Publications, Thousand Oaks, CA.

[13] Ryan A. Buell. 2019. Operational Transparency: Make Your Processes Visible to Customers and Your Customers Visible to Employees. *Harvard Business School* 4 (2019), 102–113. https://www.hbs.edu/faculty/Pages/item.aspx?num=55804

[14] Manuel Castells. 2011. A Network Theory of Power. *International Journal of Communication* 5 (2011), 773–787. http://ijoc.org.

[15] Roger Clarke. 1988. Information technology and dataveillance. *Commun. ACM* 31, 5 (5 1988), 498–512. https://doi.org/10.1145/42411.42413

[16] Victoria Clarke and Virginia Braun. 2022. *Thematic analysis: A practical guide.* SAGE Publications Ltd, London. https://uk.sagepub.com/en-gb/eur/thematic-analysis/book248481#description

[17] Jennifer Cobbe, Michelle Seng Ah Lee, and Jatinder Singh. 2021. Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems. *FAccT 2021 - Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (1 2021), 598–609. https://doi.org/10.1145/3442188.3445921

[18] Jennifer Cobbe, Michael Veale, and Jatinder Singh. 2023. Understanding accountability in algorithmic supply chains. *2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (4 2023). https://doi.org/10.1145/3593013.3594073

[19] CPS. 2022. Modern Slavery, Human Trafficking and Smuggling. https://www.cps.gov.uk/legal-guidance/modern-slavery-human-trafficking-and-smuggling

[20] Sylvie Delacroix and Neil D Lawrence. 2019. Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law* (10 2019). https://doi.org/10.1093/idpl/ipz014

[21] ECPAT. 2023. National Referral Mechanism. https://www.ecpat.org.uk/national-referral-mechanism

[22] Lilian Edwards and Michael Veale. 2017. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *SSRN Electronic Journal* (5 2017). https://doi.org/10.2139/SSRN.2972855

[23] European Commission. 2024. Support Centre for Data Sharing. https://futurium.ec.europa.eu/en/support-centre-data-sharing/pages/about

[24] Marcel Fassnacht, Carina Benz, Daniel Heinz, Jannis Leimstoll, and Gerhard Satzger. 2023. Barriers to Data Sharing among Private Sector Organizations.

In *Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS)*. 1663–1672. https://hdl.handle.net/10125/103084

[25] David Gadd and Rose Broad. 2024. When Victims of Modern Slavery Became Offenders: The Unravelling of the UK's Modern Slavery Agenda. *Journal of Human Trafficking* (4 2024). https://doi.org/10.1080/23322705.2024.2303254

[26] Alison Galloway. 2005. Non-Probability Sampling. *Encyclopedia of Social Measurement* (1 2005), 859–864. https://doi.org/10.1016/B0-12-369398-5/00382-0

[27] Jean-Pierre Gauci, Noemi Magugliani, and John Trajer. 2023. *Impacts of a lack of legal advice on adults with lived experience of modern slavery*. Technical Report. Modern Slavery & Human Rights Policy & Evidence Centre (MSPEC), London. https://www.unseenuk.org/wp-content/uploads/2023/01/Legal-advice-Research-Summary.pdf

[28] Theodora Gazi. 2020. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Journal of International Humanitarian Action* 5, 1 (7 2020), 1–7. https://doi.org/10.1186/S41018-020-00078-0

[29] J. Gelhaar, F. Becker, and T. Groß. 2022. Characterization of Relationships in Data Ecosystems. In *Proceedings of the Conference on Production Systems and Logistics: CPSL*, D. Herberger and M. Hübner (Eds.). publish-Ing., Hannover. https://doi.org/10.15488/12159

[30] Joshua Gelhaar, Tobias Groß, and Boris Otto. 2021. A Taxonomy for Data Ecosystems. *Proceedings of the Annual Hawaii International Conference on System Sciences* 2020-January (1 2021), 6113–6122. https://doi.org/10.24251/HICSS.2021.739

[31] Joshua Gelhaar, Tan Gürpinar, Michael Henke, and Boris Otto. 2021. Towards a taxonomy of incentive mechanisms for data sharing in data ecosystems. *PACIS 2021 Proceedings* (7 2021). https://aisel.aisnet.org/pacis2021/121

[32] Joshua Gelhaar and Boris Otto. 2020. Challenges in the Emergence of Data Ecosystems. In *PACIS 2020 Proceedings*. https://aisel.aisnet.org/pacis2020/175

[33] Melanie Gower. 2023. *Modern slavery cases in the immigration system*. Technical Report. UK Parliament, London. https://commonslibrary.parliament.uk/research-briefings/cbp-9744/

[34] Farrah Stone Graham, Susan T. Gooden, and Kasey J. Martin. 2016. Navigating the Transparency–Privacy Paradox in Public Sector Data Sharing. *The American Review of Public Administration* 46, 5 (9 2016), 569–591. https://doi.org/10.1177/0275074014561116

[35] Monika Halkort. 2019. Decolonizing data relations: On the moral economy of data sharing in Palestinian refugee camps. *Canadian Journal of Communication* 44, 3 (2019), 317–329. https://doi.org/10.22230/cjc.2019v44n3a3457

[36] David Heald. 2006. Varieties of Transparency. In *Transparency: the Key to Better Governance*, Christopher Hood and David Heald (Eds.). Oxford University Press, Oxford, Chapter 2. https://global.oup.com/academic/product/transparency-9780197263839?cc=us&lang=en&#

[37] Daniel Heinz, Carina Benz, Marcel Fassnacht, and Gerhard Satzger. 2022. Past, Present and Future of Data Ecosystems Research: A Systematic Literature Review. In *PACIS 2022 Proceedings*. https://aisel.aisnet.org/pacis2022/46

[38] HMICFRS, College of Policing, and Independent Office for Police Conduct. 2018. *Safe to share? Report on Liberty and Southall Black Sisters' super-complaint on policing and immigration status*. Technical Report. HMICFRS, London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945314/safe-to-share-liberty-southall-black-sisters-super-complaint-policing-immigration-status.pdf

[39] Home Office. 2019. *Independent review of the Modern Slavery Act 2015: final report*. Technical Report. Home Office, London. https://www.gov.uk/government/publications/independent-review-of-the-modern-slavery-act-final-report

[40] Home Office. 2021. Publish an annual modern slavery statement. https://www.gov.uk/guidance/publish-an-annual-modern-slavery-statement

[41] Home Office. 2021. Review of data sharing: migrant victims and witnesses of crime. https://www.gov.uk/government/publications/review-of-data-sharing-migrant-victims-and-witnesses-of-crime/review-of-data-sharing-migrant-victims-and-witnesses-of-crime-accessible-version

[42] Home Office. 2023. About us. https://www.gov.uk/government/organisations/home-office/about

[43] Home Office. 2023. National referral mechanism guidance: adult (England and Wales). https://www.gov.uk/government/publications/human-trafficking-victims-referral-and-assessment-forms/guidance-on-the-national-referral-mechanism-for-potential-adult-victims-of-modern-slavery-england-and-wales

[44] Home Office, Karen Bradley, and Theresa May. 2015. Historic law to end Modern Slavery passed. https://www.gov.uk/government/news/historic-law-to-end-modern-slavery-passed

[45] Human Rights Watch. 2021. UN Shared Rohingya Data Without Informed Consent. https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

[46] Kristian P. Humble. 2021. International law, surveillance and the protection of privacy. *The International Journal of Human Rights* 25, 1 (2021), 1–25. https://doi.org/10.1080/13642987.2020.1763315

[47] Ed Humpherson. 2022. Ed Humpherson to Jennifer Rubin: use of National Referral Mechanism statistics. https://osr.statisticsauthority.gov.uk/correspondence/ed-humpherson-to-jennifer-rubin-use-of-national-referral-mechanism-statistics/

[48] ICO. 2021. *Data sharing code of practice*. Technical Report. Information Commissioner's Office (ICO), London. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

[49] ICO. 2023. What is the Freedom of Information Act? https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/guide-to-freedom-of-information/what-is-the-foi-act/

[50] ICO. 2024. Data sharing agreements. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements

[51] ICO. 2024. When can we refuse a request for information? https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/guide-to-freedom-of-information/refusing-a-request

[52] ILO. 2022. Modern slavery: 50 million people worldwide in modern slavery. https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_855019/lang--en/index.htm

[53] ILO. 2023. ILO Contributions to achieve Target 8.7 (The 2030 development agenda). https://www.ilo.org/global/topics/sdg-2030/goal-8/target-8-7/lang--en/index.htm

[54] ILO. 2023. What is forced labour, modern slavery and human trafficking. https://www.ilo.org/global/topics/forced-labour/definition/lang--en/index.htm

[55] Independent Anti-Slavery Commissioner and Home Office. 2020. Data Sharing Protocol between HO and the Independent Anti-Slavery Commissioner Purpose. https://www.antislaverycommissioner.co.uk/media/1420/data-sharing-agreement-for-iasc-and-home-office.pdf

[56] Marvin Jagals and Erik Karger. 2021. INTER-ORGANIZATIONAL DATA GOVERNANCE: A LITERATURE REVIEW. In *ECIS 2021 Research Papers*. https://aisel.aisnet.org/ecis2021_rp/57

[57] Lena J. Jaspersen and Christian Stein. 2019. Beyond the Matrix: Visual Methods for Qualitative Network Research. *British Journal of Management* 30, 3 (7 2019), 748–763. https://doi.org/10.1111/1467-8551.12339

[58] Shouling Ji, Weiqing Li, Mudhakar Srivatsa, and Raheem Beyah. 2016. Structural Data De-Anonymization: Theory and Practice. *IEEE/ACM Transactions on Networking* 24, 6 (12 2016), 3523–3536. https://doi.org/10.1109/TNET.2016.2536479

[59] Scott D. Kahn and Anne Koralova. 2022. A journey toward an open data culture through transformation of shared data into a data resource. *Data & Policy* 4 (2022). https://doi.org/10.1017/dap.2022.22

[60] George Kamberelis, Greg Dimitriadis, and Alyson Welker. 2017. Focus Group Research and/in Figured Worlds. In *The SAGE Handbook of Qualitative Research* (5 ed.), Norman K. Denzin and Yvonna S. Lincoln (Eds.). SAGE Publications, Thousand Oaks, CA.

[61] Unni Karunakara. 2014. Data Sharing in a Humanitarian Organization: The Experience of Médecins Sans Frontières. In *Issues in Open Research Data*, Samuel A. Moore (Ed.). Ubiquity Press, London, 59–76. https://doi.org/10.5334/BAN.D

[62] Maximilian Kasy and Rediet Abebe. 2021. Fairness, equality, and power in algorithmic decision-making. *FAccT 2021 - Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* 11 (3 2021), 576–586. https://doi.org/10.1145/3442188.3445919

[63] Emma Knight and Alex Gekkar. 2020. Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures. *Surveillance & Society* 18, 2 (2020), 231–243.

[64] Bakhtawar Komal, Uzair Iqbal Janjua, Fozia Anwar, Tahir Mustafa Madni, Muhammad Faisal Cheema, Muhammad Noman Malik, and Ahmad Raza Shahid. 2020. The Impact of Scope Creep on Project Success: An Empirical Investigation. *IEEE Access* 8 (2020), 125755–125775. https://doi.org/10.1109/ACCESS.2020.3007098

[65] Bert-Jaap Koops. 2021. The concept of function creep. *Law, Innovation and Technology* 13, 1 (1 2021), 29–56. https://doi.org/10.1080/17579961.2021.1898299

[66] Christopher Kuner and Massimo Marelli. 2017. *Handbook on Data Protection in Humanitarian Action*. Technical Report. International Committee of the Red Cross, Geneva. https://rm.coe.int/handbook-data-protection-and-humanitarian-action-low/168076662a

[67] Jacqueline Kuzio, Mohammad Ahmadi, Kyoung-Cheol Kim, Michael R. Migaud, Yi-Fan Wang, and Justin Bullock. 2022. Building better global data governance. *Data & Policy* 4 (2022), e25. https://doi.org/10.1017/DAP.2022.17

[68] Todd Landman. 2020. Measuring modern slavery: Law, human rights, and new forms of data. *Human Rights Quarterly* 42, 2 (5 2020), 303–331. https://doi.org/10.1353/hrq.2020.0019

[69] Bruno Latour. 2005. *Reassembling the social: an introduction to actor-network-theory*. Oxford University Press.

[70] Benjamin Laufer, Thomas Gilbert, and Helen Nissenbaum. 2023. Optimization's Neglected Normative Commitments. In *FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. Association for Computing Machinery, 50–63. https://doi.org/10.1145/3593013.3593976

[71] Rosa Lavelle-Hill, Gavin Smith, Anjali Mazumder, Todd Landman, and James Goulding. 2021. Machine learning methods for "wicked" problems: exploring the complex drivers of modern slavery. *Humanities and Social Sciences Communications* 8, 1 (12 2021). https://doi.org/10.1057/s41599-021-00938-z

[72] Michelle Seng Ah Lee, Luciano Floridi, and Jatinder Singh. 2021. Formalising trade-offs beyond algorithmic fairness: lessons from ethical philosophy and welfare economics. *AI and Ethics* 1, 4 (6 2021), 529–544. https://doi.org/10.1007/S43681-021-00067-Y

[73] Liberty and Southall Black Sisters. 2018. Super-complaint prepared by Liberty and Southall Black Sisters. https://www.libertyhumanrights.org.uk/issue/liberty-and-southall-black-sisters-super-complaint-on-data-sharing-between-the-police-and-home-office-regarding-victims-and-witnesses-to-crime/

[74] David Lyon. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society* 1, 2 (2014). https://doi.org/10.1177/2053951714541861

[75] Donald A MacKenzie and Judy Wajcman. 1999. General Introduction. In *The social shaping of technology* (2nd ed ed.). Open University Press, 1–49.

[76] Vidushi Marda and Shivangi Narayan. 2020. Data in New Delhi's predictive policing system. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. ACM, New York, NY, USA, 317–324. https://doi.org/10.1145/3351095.3372865

[77] Bovens Mark. 2010. Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. *West European Politics* 33, 5 (2010), 946–967. https://doi.org/10.1080/01402382.2010.486119

[78] Natasha McCarthy and Franck Fourniol. 2020. The role of technology in governance: The example of Privacy Enhancing Technologies. *Data & Policy* 2 (2020). https://doi.org/10.1017/dap.2020.8

[79] Michelle McLeod and Maurice McNaughton. 2016. View of Mapping an emergent Open Data ecosystem. *The Journal of Community Informatics* 12, 2 (2016), 26–46. https://openjournals.uwaterloo.ca/index.php/JoCI/article/view/3220/4223

[80] Ella McPherson. 2015. *ICTs and Human Rights Practice: A Report Prepared for the UN Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions*. Technical Report. www.cghr.polis.cam.ac.uk

[81] Sally Engle Merry. 2016. *The seductions of quantification: measuring human rights, gender violence, and sex trafficking*. The University of Chicago Press. 249 pages.

[82] Sally Engle Merry. 2017. Counting the Uncountable: Constructing Trafficking through Measurement. In *Revisiting the Law and Governance of Trafficking, Forced Labor and Modern Slavery*. Cambridge University Press, 273–304. https://doi.org/10.1017/9781316675809.010

[83] Eric T. Meyer, Jon Crowcroft, Zeynep Engin, and Anne Alexander. 2017. Data for Public Policy. *Policy & Internet* 9, 1 (3 2017), 4–6. https://doi.org/10.1002/poi3.147

[84] David L. Morgan. 1996. Focus Groups. *Annual Review of Sociology* 22, 1 (8 1996), 129–152. https://doi.org/10.1146/annurev.soc.22.1.129

[85] Arvind Narayanan and Vitaly Shmatikov. 2008. Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset). *arXiv* (2008).

[86] Kaelynn Narita. 2023. An infrastructural approach to the digital Hostile Environment. *Journal of Global Ethics* (2023). https://doi.org/10.1080/17449626.2023.2272773

[87] Chris Norval, Kristin Cornelius, Jennifer Cobbe, and Jatinder Singh. 2022. Disclosure by Design: Designing information disclosures to support meaningful transparency and accountability. *ACM International Conference Proceeding Series* 22 (6 2022), 679–690. https://doi.org/10.1145/3531146.3533133

[88] ODI. 2022. *Mapping data ecosystems: Tools for documenting and mapping data ecosystems*. Technical Report. Open Data Institute (ODI), London. http://theodi.org/wp-content/uploads/2022/04/2022_ODI_Mapping-data-ecosystems-2022-update.pdf

[89] Marcelo Oliveira, Glória de Fátima Barros Lima, and Bernadette Farias Lóscio. 2019. Investigations into Data Ecosystems: a systematic mapping study. *Knowledge and Information Systems* 61, 2 (11 2019), 589–630. https://doi.org/10.1007/S10115-018-1323-6/METRICS

[90] Marcelo Oliveira and Bernadette Farias Lóscio. 2018. What is a data ecosystem?. In *ACM International Conference Proceeding Series*. Association for Computing Machinery. https://doi.org/10.1145/3209281.3209335

[91] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball Sampling. In *SAGE Research Methods Foundations*, Paul Atkinson, Sara Delamont, Alexandru Cernat, Joseph W. Sakshaug, and Richard A. Williams (Eds.). SAGE Publications, Thousand Oaks, CA. https://doi.org/10.4135/9781526421036831710

[92] J. Powar and J. Hancock. 2023. The limits to modelling dataflow networks: a conceptual synthesis. In *International Conference on AI and the Digital Economy (CADE 2023)*. Institution of Engineering and Technology, Venice, 134–143. https://doi.org/10.1049/icp.2023.2597

[93] Ben Quinn. 2023. UK illegal migration bill will have profound consequences, warns UN body. https://www.theguardian.com/uk-news/2023/jul/18/uk-migration-bill-to-become-law-as-government-sees-off-lords-challenge

[94] Tim Rapley. 2014. Sampling Strategies in Qualitative Research. In *The SAGE Handbook of Qualitative Data Analysis*, Uwe Flick (Ed.). SAGE Publications, London, Chapter 4. https://doi.org/10.4135/9781446282243

[95] Joanna Redden. 2018. Democratic governance in an age of datafication: Lessons from mapping government discourses and practices. *Big Data and Society* 5, 2 (7 2018). https://doi.org/10.1177/2053951718809145

[96] Rashida Richardson, Jason M Schultz, and Kate Crawford. 2019. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online* 192 (2019). https://ssrn.com/abstract=3333423

[97] Felix Ritchie and Jim Smith. 2019. Confidentiality and linked data. *arXiv* (7 2019). https://arxiv.org/abs/1907.06465v1

[98] Silvia Rodríguez-López. 2020. Telling Victims from Criminals: Human Trafficking for the Purposes of Criminal Exploitation. In *The Palgrave International Handbook of Human Trafficking*, J. Winterdyk and J. Jones (Eds.). Vol. 1. Palgrave Macmillan, Cham, 303–318. https://doi.org/10.1007/978-3-319-63058-8{_}17

[99] Samiaji Sarosa and Arthur Tatnall. 2015. Failure to Launch: Scope Creep and Other Causes of Failure from an Actor-Network Theory Perspective. *International Journal of Actor-Network Theory and Technological Innovation* 7, 4 (10 2015), 1–13. https://doi.org/10.4018/ijantti.2015100101

[100] Emrys Schoemaker, Dina Baslan, Bryan Pon, and Nicola Dell. 2020. Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development* 17, § (2020), 13–36. https://doi.org/10.1080/02681102.2020.1785826

[101] Clive Seale. 2012. Sampling. In *Researching Society and Culture*, Clive Seale (Ed.). SAGE Publications, Thousand Oaks, CA., Chapter 9. https://uk.sagepub.com/en-gb/eur/node/53906/print

[102] Andrew D. Selbst, Danah Boyd, Sorelle A. Friedler, Suresh Venkatasubramanian, and Janet Vertesi. 2019. Fairness and abstraction in sociotechnical systems. *FAT* 2019 - Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency* (1 2019), 59–68. https://doi.org/10.1145/3287560.3287598

[103] James A. Shaw, Nayha Sethi, and Christine K. Cassel. 2020. Social license for the use of big data in the COVID-19 era. *npj Digital Medicine* 3, 1 (10 2020), 128. https://doi.org/10.1038/s41746-020-00342-y

[104] Jatinder Singh and Jennifer Cobbe. 2019. The Security Implications of Data Subject Rights. *IEEE Security & Privacy* 17, 06 (11 2019), 21–30. https://doi.org/10.1109/MSEC.2019.2914614

[105] Jatinder Singh, Jennifer Cobbe, and Chris Norval. 2019. Decision Provenance: Harnessing Data Flow for Accountable Systems. *IEEE Access* 7 (2019), 6562–6574. https://doi.org/10.1109/ACCESS.2018.2887201

[106] Cynthia Stohl, Michael Stohl, and Paul M. Leonardi. 2016. Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age. *International Journal of Communication* 10, 0 (1 2016), 15. https://ijoc.org/index.php/ijoc/article/view/4466

[107] Paul Sturges. 2007. What is this absence called transparency? *The International Review of Information Ethics* 7 (9 2007), 221–228. https://doi.org/10.29173/irie25

[108] Rishi Sunak. 2023. PM's remarks on illegal migration: 7 December 2023. https://www.gov.uk/government/speeches/pms-remarks-on-illegal-migration-7-december-2023

[109] Oisín Tansey. 2007. Process tracing and elite interviewing: A case for non-probability sampling. In *PS - Political Science and Politics*, Vol. 40. 765–772. https://doi.org/10.1017/S1049096507071211

[110] Renata Tesch. 2013. *Qualitative research: Analysis types and software tools*. Taylor and Francis. 1–331 pages. https://doi.org/10.4324/9781315067339/QUALITATIVE-RESEARCH-ANALYSIS-TYPES-SOFTWARE-RENATA-TESCH

[111] Fran Tonkiss. 2012. Discourse Analysis. In *Researching Society and Culture*, Clive Seale (Ed.). SAGE Publications, Thousand Oaks, CA., Chapter 23.

[112] Traffik Analysis Hub. 2023. How it Works. https://www.traffikanalysis.org/how-it-works

[113] Matteo Turilli and Luciano Floridi. 2009. The ethics of information transparency. *Ethics and Information Technology* 11, 2 (3 2009), 105–112. https://doi.org/10.1007/S10676-009-9187-9/METRICS

[114] Barbara Ubaldi, Charlotte Van Ooijen, and Benjamin Welby. 2019. A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance. (5 2019). https://doi.org/10.1787/19934351

[115] UK Parliament. 2000. Freedom of Information Act 2000. https://www.legislation.gov.uk/ukpga/2000/36/contents

[116] UK Parliament. 2015. Modern Slavery Act 2015. https://www.legislation.gov.uk/ukpga/2015

[117] UK Parliament. 2018. Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/

[118] UK Parliament (Retained EU Regulation). 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [United Kingdom General Data Protection Regulation]. https://www.legislation.gov.uk/eur/2016/679

[119] UN General Assembly. 1948. Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights
[120] UN ODC. 2023. Sustainable Development Goals. https://www.unodc.org/roseap/en/sustainable-development-goals.html
[121] UN OHCHR. 1966. International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[122] UN OHCHR. 2015. Modern slavery may be hidden in supply chains, but it can be rooted out – UN rights expert. https://www.ohchr.org/en/press-releases/2015/11/modern-slavery-may-be-hidden-supply-chains-it-can-be-rooted-out-un-rights
[123] Jose Van Dijck. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12, 2 (5 2014), 197–208. https://doi.org/10.24908/ss.v12i2.4776
[124] François van Schalkwyk, Michelle Willmers, and Maurice McNaughton. 2016. Viscous Open Data: The Roles of Intermediaries in an Open Data Ecosystem. *Information Technology for Development* 22, sup1 (8 2016), 68–83. https://doi.org/10.1080/02681102.2015.1081868
[125] Stefaan Verhulst, Zeynep Engin, and Jon Crowcroft. 2019. Data & Policy: A new venue to study and explore policy–data interaction. *Data & Policy* 1 (2019). https://doi.org/10.1017/dap.2019.2
[126] Stefaan Verhulst and David Sangokoya. 2015. Data Collaboratives: Exchanging Data to Improve People's Lives. https://sverhulst.medium.com/data-collaboratives-exchanging-data-to-improve-people-s-lives-d0fcfc1bdd9a
[127] Stefaan Verhulst and Andrew Young. 2019. The Potential and Practice of Data Collaboratives for Migration. In *Guide to Mobile Data Analytics in Refugee Scenarios*. Springer International Publishing, Cham, 465–476. https://doi.org/10.1007/978-3-030-12554-7{_}24
[128] Stefaan Verhulst and Andrew Young. 2022. Identifying and addressing data asymmetries so as to enable (better) science. *Frontiers in Big Data* 5 (7 2022). https://doi.org/10.3389/fdata.2022.888384
[129] Walk Free. 2022. Global Estimates of Modern Slavery 2022. https://www.walkfree.org/reports/global-estimates-of-modern-slavery-2022/
[130] Michael Williams and Tami Moser. 2019. The Art of Coding and Thematic Exploration in Qualitative Research. *International Management Review* 15, 1 (2019).
[131] Dan Wu, Stefaan Verhulst, Alex Pentland, Thiago Avila, Kelsey Finch, and Abhishek Gupta. 2021. How data governance technologies can democratize data sharing for community well-being. *Data & Policy* 3 (7 2021). https://doi.org/10.1017/DAP.2021.13
[132] Meg Young, Luke Rodriguez, Emily Keller, Feiyang Sun, Boyang Sa, Jan Whittington, and Bill Howe. 2019. Beyond open vs. Closed: Balancing individual privacy and public accountability in data sharing. *FAT* 2019 - Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency* (1 2019), 191–200. https://doi.org/10.1145/3287560.3287577
[133] Andrej Zwitter and Oskar J. Gstrein. 2020. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action* 5, 1 (5 2020), 1–7. https://doi.org/10.1186/S41018-020-00072-6