Personal and Ubiquitous Computing
https://doi.org/10.1007/s00779-021-01655-9

ORIGINAL ARTICLE

The cardboard box study: understanding collaborative data management in the connected home

Damla Kilic[1] · Andy Crabtree[1] · Glenn McGarry[1] · Murray Goulden[2]

Received: 30 October 2020 / Accepted: 15 September 2021

Abstract
The home is a site marked by the increasing collection and use of personal data, whether online or from connected devices. This trend is accompanied by new data protection regulation and the development of privacy enhancing technologies (PETs) that seek to enable individual control over the processing of personal data. However, a great deal of the data generated within the connected home is interpersonal in nature and cannot therefore be attributed to an individual. The cardboard box study adapts the technology probe approach to explore with potential end users the salience of a PET called the Databox and to understand the challenge of collaborative rather than individual data management in the home. The cardboard box study was designed as an ideation card game and conducted with 22 households distributed around the UK, providing us with 38 participants. Demographically, our participants were of varying ages and had a variety of occupational backgrounds and differing household situations. The study makes it perspicuous that privacy is not a ubiquitous concern *within the home* as a great deal of data is shared by default of people living together; that when privacy is occasioned it performs a distinct social function that is concerned with *human security* and the safety and integrity of people rather than devices and data; and that current 'interdependent privacy' solutions that seek to support collaborative data management are *not well aligned* with the ways access control is negotiated and managed within the home.

Keywords Connected home · Internet of Things · Databox · Personal data · Interdependent privacy · Collaborative data management

1 Introduction

Personal data has and continues to receive a great deal of attention. In technological quarters, it is often referred to as the oil of the digital economy, or some similar analogy is invoked to denote personal data as resource that is valuable to innovation and economic growth. The turn to data-driven innovation has been accompanied by widespread societal concern—witness the Facebook and Cambridge Analytica scandal for prime example (though this is by no means the only one)—and has been accompanied by new data protection legislation. The EU, for example, implemented the General Data Protection Regulation (GDPR) in 2018, and the USA and Japan have considered upgrades to their legislation with varying degrees of success [2, 47]. What is common across both legal and technological sectors is the focus on the individual. Personal data is seen and treated as something that either belongs to a user (natural person or data subject in legal terms) or is generated by them in the course of their interactions with digital applications and services, a point underscored by GDPR [24]:

> 'personal data' means any information relating to **an** identified or identifiable natural person ('data subject'); **an** identifiable natural person is **one** who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic,

✉ Damla Kilic
damla.kilic@nottingham.ac.uk

Murray Goulden
murray.goulden@nottingham.ac.uk

[1] School of Computer Science, University of Nottingham, Jubilee Campus, Nottingham NG8 1BB, UK

[2] School of Sociology and Social Policy, University of Nottingham, Nottingham NG8 1BB, UK

Published online: 08 October 2021

> mental, economic, cultural or social identity of **that** natural person. (Article 4, our emphasis)

The upshot is that many and varied privacy enhancing technology (PET) initiatives that seek to protect personal data—e.g. Mydex [46], OpenPDS [16], HAT [70], MyData [54], Databox [44] and Solid [63]—invariably focus on the individual in society, not the *social group*.

Laudable as such endeavours are they nevertheless overlook the fact that a great deal of the data generated within the connected home [31] is interpersonal in nature [28] and cannot therefore be attributed to an individual [17]. Take smart meters or indeed an increasing range of connected domestic appliances (TVs, washing machines, kettles, toasters, heating systems, lights, etc.). Unless one lives alone, and not simply in a legal sense of sole occupier but in the sense of never hosting others, the domestic Internet of Things generates unprecedented amounts of data that is essentially born social [19]. Of course, individuals may have their own connected devices, but as the digital is increasingly embedded within the very fabric of domestic life—in physical structures, fixtures, fittings and the mobilia of the home [58] from appliances to fast moving consumer goods [8]—then an increasing amount of the data generated in the connected home of the future will be tied to multi-party interactions. It is not hard to appreciate then that connecting a myriad mundane thing to the Internet, including an increasing array of consumables wrapped up in intelligent packaging [75], will reach beyond the individual in many millions and indeed billions of cases worldwide.

Why does this matter? GDPR exempts data processing for ‘purely personal or household activity’ (Article 2 & Recital 18), which means household members can process data generated by their co-inhabitants as they wish, and data born social stands outside legal protection even in the most advanced regulatory regimes. While significant efforts are being made to empower individual data management, there is a significant gap in our understanding of the increasing collection and use of personal data in *social* contexts generally and the home in particular and the concomitant challenge of enabling collaborative rather than individual data management in the connected home. We thus designed and deployed the ‘cardboard box’, a proxy for a PET called the Databox [14] with the aim of understanding how people reason about data within the connected home and the challenges this might raise for collaborative data management, *where the management of data involves or implicates more than one party*. The Databox is intended to sit at the edge of the network in the home [45] and act as a gateway to an individual’s personal data, enabling users to install apps that process their data locally to deliver personalised services. That it is *intended* to do so explains the need for a proxy—the Databox was not in deployable state at the time of the study. However, we saw no reason why we could not probe the Databox concept with householders cum potential end users, along with the challenges bound up in collaborative data management to inform ongoing development of the platform.

For the study, the cardboard box in question was used alongside a set of ideation cards [39] in card sorting exercise, in order to explore participants’ reasoning concerning the appropriate management of different forms of domestic data that were potentially interpersonal in nature. In Section 2, we consider relevant literature in the privacy study field. Section 3 explains our methodology via an unpacking of both the cardboard box, the associated ideation cards and the data collection and analysis. Sections 4, 5 and 6 cover findings, discussion and conclusions, respectively.

The results and primary contributions of this study reshape our understanding of privacy within the home, where it is often assumed (if it is considered at all) that inhabits have an abiding concern to withhold information from those they live with. The presumption in part underpins the development of PETs, and while our study does find that people have occasional need for privacy in their everyday lives, it is an occasioned matter driven by an abiding concern with *human security* and the need to protect others from online harms and ensure their integrity as social actors, much more than it is to withhold information about one’s digital activities from co-inhabitants. It is not then data privacy that matters most *within* the home, as much is already accessible. Rather it is the *negotiated* nature of data access and use that underpins and articulates the collaborative management of data between household members. The value of data in this context lies less in the preservation of personal secrets and more in its *exchange*, at times deliberate and at others serendipitous, in coordinating the mundane activities of everyday life. In short, what is at stake is not simply the privacy of individuals, but the *social and moral ordering of the group* [9]. In this respect, we find that existing approaches to collaborative data management furnished by efforts to engineer ‘interdependent privacy’ [34] do not resonate with the ways in which access control is socially managed and negotiated within the home. We conclude with a discussion of the implications of these findings.

2 Background

The dynamic and contested character of data access in the home undermines the predominant concept of privacy in social and technical studies, namely the ‘privacy as control’ thesis attributed to legal scholar Alan Westin [71]. This thesis construes of privacy as the ability for an *individual* to control, edit and delete information about oneself and decide when, how and to what extent information is communicated with others. Sandra Petronio’s communicative theory of privacy management [53], predicated on the dialectical tension and interplay *between* individuals *and the group*, would appear to be much more apposite. However, this thesis, which shifts the focus from the individual to the individual-as-a-member-of-a-group, is reminiscent of early debate in the field of computer-supported cooperative work (CSCW), which found such a conception deeply problematic [30]. At the nub of the debate is the recognition that individuals are not merely situated in groups but are 'mutually dependent' upon one another and thus 'meshed together' in social units [62]. Understanding and unpacking mutual dependence and the ways in which social units are meshed together became CSCW's unique and distinctive problem, resolved through the explication of 'work practice', i.e. the empirical elaboration of *social* practices that *organise* what individuals do synchronously or asynchronously, whether they are co-located or distributed [6]. However, efforts to recognise the socially organised nature of privacy, and to build it into the analytic apparatus of social studies and technology development alike, turn on the inadequate conceptualisation of the individual-as-the-member-of-a-group.

Thus, and for example, Irwin Altman's [1] 'boundary management' thesis, famously championed by Palen and Dourish [51] in a systems design context, construes of privacy as a process of 'dynamic boundary regulation' in which selective access to the self is governed by the individual-in-interaction. Altman's thesis underpins Petronio's [53], which seeks to elaborate how boundaries are regulated through rule development, particularly of co-ownership and guardianship, and how breakdowns are managed. The notion of rules as key to social organisation also chimes with Helen Nissenbaum's [48] influential concept of 'contextual integrity', where privacy is seen to be governed by context-specific norms and values that regulate the flow of information. Rules, norms and values provide for laymen and analysts alike a generic, common-sense framework organising the actions of the individual-as-a-member-of-the-group (see the work of the eminent sociologist Talcott Parsons [52] for prime example). However, in the social sciences, they have long been understood to be a problematic means of accounting for social organisation [21]. Simply put, there is a 'praxiological gap' between rules, norms and values *and* their enactment in everyday life. As Rawls [23] puts it with respect to rules, for example, they cannot tell you how to follow them, that would entail an infinite regress, and as vom Lehn [69] explains, norms and values do not, in practice, provide a generic framework for action but are instead occasioned and ad hoc resources invoked, made relevant and used locally by members to organise action in situ.

The relevance of this sociological argument to the development of privacy enhancing technologies lies in understanding how technological solutions do, or do not, align with it. Of particular note are efforts to engineer solutions supporting 'interdependent privacy' [34]. The concept pulls together various ideas that recognise the social nature of personal data. It includes 'collective privacy' [64], 'multi-party privacy' [66], 'networked privacy' [4], 'multiple-subject privacy' [25], 'peer privacy' [7] and 'group privacy' [57]. These various concepts of privacy have subtly different meanings but coalesce around two key thematics. The first one is *the impact of others* on one's privacy where, for example, data affect not only the individual who shares the data but those implicated in or related to it [4], including the disclosure of an individual's private information by peers [7], or the actions of persons surrounding an individual (friends, family, strangers in the public space, etc.) affect the individual's privacy [57]. The second one is the *collaborative management* of personal data, where the members of a group collectively manage data [64], more than one party controls the visibility of data [66], and no single person has the right to control how the data is shared [25]. Interdependent privacy recognises that a great deal of data is both *social by default*—emails, phone calls, social media posts and photos are often cited to demonstrate the point—and that the data is at the outset *enmeshed in social relationships* (friendship, kinship and broader social networks). To use the nomenclature of the UK Information Commissioner's Office, personal data is often 'mixed', i.e. *inextricably linked* to other data subjects [35].

The recognition that personal data is often mixed, and is thus *meshed together* with multiple parties, has led to the development of interdependent privacy mechanisms to enable group-level privacy management. These largely focus on online social networks (OSN), but there appears to have been some work around mobile phones [27] and shared PETs [26]. There is also a predominant focus on *collaborative access control*. Wishart et al. [72] thus exploit *privacy policies* to allow the owner of content to nominate co-owners who can change the scope of a policy to reflect their own interests. González-Manzano et al. [26] developed a PET for managing co-owned data that similarly allows a data owner to assign co-ownership to data and for each party to specify access control policies; ownership trumps co-ownership where conflicts arise. Hu et al. [33] developed a multi-party access control model that *aggregates* privacy policies from different categories of user to decide whether to deny or grant access and uses a *voting* mechanism to resolve privacy conflicts. Mehregan and Fong [43] extend the relationship-based access control (ReBAC) model to support interactive policy negotiation, obliging co-owners to collaboratively specify a *policy negotiation protocol* regulating access to data. Ilia et al. [36] exploit privacy policies alongside facial recognition to regulate the *visibility of photos*, blurring the faces of users who have restricted access. Li et al. [41] *encrypt the faces in photos* so that they are only visible if a viewer is given a key, and a similar approach is adopted by Olteanu et al. [50].

A further body of work coalesces around the *detection and resolution of conflicts*. In addition to those methods of conflict resolution outlined above, Hu et al. [32] have developed an algorithmic model that exploits *automated voting strategies* to resolve conflicts. Automated approaches also exploit the ReBAC model to detect and resolve conflicts in privacy policies based on *measures* of the relationship strength or intimacy that holds between two users, derived from their online activity and interactions, which triggers an automated agent-based, one-step negotiation protocol [65]. Agent-based negotiation strategies are further extended by Kekülluoğlu et al. [40] and exploit a point-based system to measure reciprocity as a resource for conflict resolution. The turn to automation and AI sees the use of facial recognition to automatically detect people in photos that have been shared on OSNs [74] and to obfuscate them [42]. Zhong et al. [76] use a convolutional neural net to automatically detect potential privacy conflicts in photographs.

The purpose of this whistle stop tour around the interdependent privacy literature is to understand the broad ways in which computing is being used to support the collaborative management of mixed data. What we see is that support is largely focussed on collaborative access control, which revolves around the specification of privacy policies, and to a lesser extent on detecting and resolving conflicts, particularly through the use of machine learning and AI. While interdependent privacy is to be commended for recognising the inherently social nature of a great deal of data in the networked world, these solutions are nonetheless problematic in a domestic context. Interdependent privacy solutions developed for online social networks, and which are largely limited to photos at the current moment in time, are not well-suited to the home. For example, it would be absurd for the members of a family to assign co-ownership, specify individual privacy policies, and redact individual images in family photos, while this could potentially be done automatically, that would be to miss the point, as this is not what we do because they are *family* photos.

The kind of solutions currently offered by interdependent privacy is a consequence of seeing people as individual-members-of-a-group whose privacy needs protection, which might work well in OSNs but not a domestic context, where no matter how it is composed (e.g. traditional middle-class nuclear family, LGBTQ, single parent, ethnic minority, religious, secular), people are members of a discrete *social unit*. While the relationships, expectations and responsibilities are different, the same applies to shared *households*. The members of these social units are not simply individuals-in-a-group; the group has *facticity* of its own that members orient to and use to define their relationships and the expectations and responsibilities that hold between them, be it parenting, cooking, doing the washing up, paying the bills, etc. Furthermore, members of the unit know, and are expected to know, private, often intimate and even highly sensitive things about one another, and this knowledge is, indeed, key to what makes them a family and to a lesser degree a household. Thus, a great deal of what passes for data in the home, even personal data that may clearly be attributed to an individual (data of birth, driving licence, passport, bills, medical information, political affiliation, sexuality, etc.), are *shared by default of our living together*, a point underscored by much of our data.

3 Methods

The study took the form of a game-like activity played in participant's homes at a date and time of their choosing. Participants were first informed of the purpose of the game and consented in writing to allow us to study their playing of it before being introduced to the gameplay procedures described below. Data captured during the study consisted of audio recordings of the participants and researchers' talk, and photographs of the cards placed in the red and blue boxes after the game had been played (as per Fig. 1). The game sessions lasted between 50 min and 2 h. The audio data was subsequently transcribed and anonymised and yielded 547 pages and 170,000 words of data.

3.1 Participants

Ethics approval for the cardboard box study (application reference CS-2018-R5) was obtained in accordance with the University of Nottingham's research procedures [68], and data collection was subsequently undertaken over a 3-month period between September and December 2018. We recruited 22 households distributed around the UK providing us with 38 participants via our social networks (no incentives or rewards were offered or received). Household composition varied and included families with children, couples, housemates and people who lived alone. Where more than one member of the household participated in the activity described below, they did so together. We anticipated that the discussion of digital data and privacy may similarly implicate and affect children, and so where children were interested and parents or guardians deemed it appropriate, we thought it relevant and indeed necessary not to exclude them from our studies. Therefore, children under the age of 16 were involved in the studies, albeit as part of a household group, and not individually. Demographically, our participants were of varying ages and had a variety of occupational backgrounds and differing household situations, as can be seen in Table 1. Our sample was nearly gender-balanced: 55% of participants identified as female and 45% as male. Most of the participants (87%) were between 20 and 59 years old. Twenty-six of our participants were British by birth and upbringing, and 12 were not.

In discussing the participating cohort, it is important to acknowledge the implications of the study's ethnomethodologically informed understanding of what the object of study in design-focused research is, and what this means for notions of generalisability. Our research interest lies

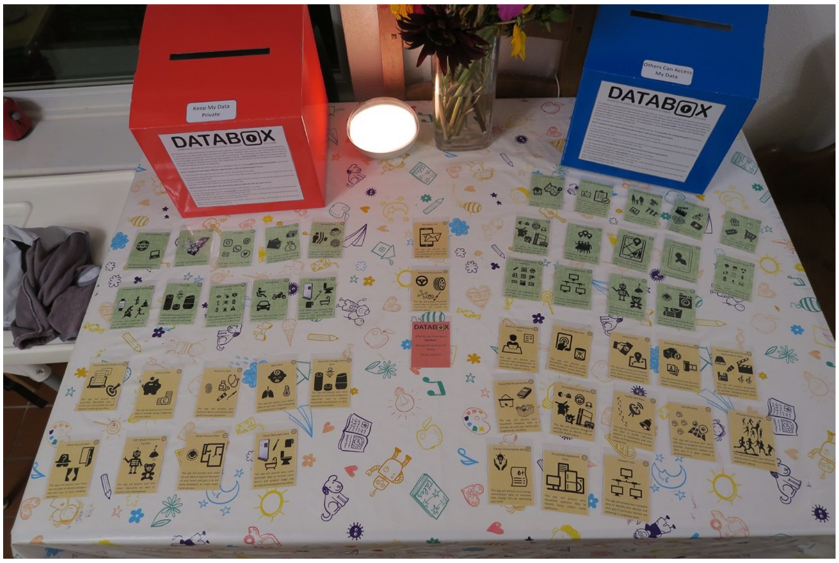


Fig. 1 The Databox proxy

in members' mundane reasoning [55] about everyday encounters, enabled by what Sacks [60] calls 'the machinery of interaction', the *mechanisms* by which we *order* everyday shared experiences. We do this not with the intention of exhaustively documenting our settings—we are not anthropologists—but to generate technology-agnostic design insights applicable to the culture studied [12].

The question of applicability brings us to generalisability. Our claims of generalisability hinge not upon quantified, positivistic reasoning where scale is central, but rather on a recognition that culture itself provides for such generalisability in order that society is able to operate as a shared coherent reality. That is to say, beneath the specific local enactments of any interaction, the ordered reasoning discovered in any one setting does not belong to that setting, but the culture it is a part of, and is recognisable to members of that culture. As our interest is in commonly recognisable reasoning, we do not seek to further subdivide our sample by any defined variables.

The culture in question here might be broadly glossed as 'British', though our participants who were not British by birth or upbringing did not—at the level of mundane reasoning we address here—exhibit notably different repertoires.

We do not claim a generalisability beyond this culture, but we do highlight that in an increasingly interconnected world, profound cultural differences *at the level of mundane reasoning* should not be assumed to begin at national boundaries. Here we invoke a test of recognisability—if our findings are recognisable to the reader, as our participants' reasoning was recognisable to us, then there are solid grounds for declaring the findings applicable to the reader's own context [11, 12]. The limits of this generalizability we return to in Section 5.2.

3.2 Designing and deploying the Databox proxy

The Databox proxy (Fig. 1) consists of two cardboard boxes, two decks of ideation cards and a set of guidelines explaining what the boxes signify and what participants are supposed to do with the cards—rules of the game as it were—which were affixed to the boxes. While the Databox is a single unit, two cardboard boxes were required to clearly reflect its functionality and allow participants to reason about the decisions they would have to make. Thus, one box (a red box on the left of Fig. 1) was labelled Keep My Data Private and the other (a blue box) was labelled Others Can Access My Data. The first (green) deck of ideation cards (running across the middle of Fig. 1) presented different types of data that might be found in the current and future connected home; the second (yellow) deck is data processing requests that might be made by third-party apps. The rules instructed participants that if they wanted to keep their data private, they should place the cards from deck one in the red box. However, if they wished to share the data with someone they knew, either a family member, friend or some other personal acquaintance, then they should place the cards from deck one in the blue box. This broad set of relationship categories purposefully covered a wide gamut of possibilities, in recognition of the fact that these categories are porous and their implications across different households vary. While the distinction between household member and non-household member might be sharp in some cases, such as might be found in the nuclear family of white middle classes, in others, such as white working class and some ethnic minority communities, non-household members might play a much more prominent role in domestic life. By keeping this wording broad, we sought to allow for such variation, which could then

Table 1 Participants in the cardboard box study

Participants		Age	Gender	By birth	Occupation	Household info
G1	G1M	Mid 50s	M	British	Sales (construction)	Single (primary care for elderly parents, one with dementia, who he lives with)
G2	G2M	Early 30s	M	British	University researcher	Married (no children)
	G2F	Early 30s	F	British	Researcher for public body	Married (no children)
G3	G3F	Early 70s	F	British	Retired (former goods driver)	Married (two adult children not resident, three grandchildren)
	G3M	Early 70s	M	British	Retired (former clerical)	Married (two adult children not resident, three grandchildren)
G4	G4F	Early 50s	F	British	Philatelist	Married (two adult children not resident, five grandchildren under 10 years old)
G5	G5M	Early 30s	M	British	Firefighter	Married (two children, 7 and 13 years old)
G6	G6M	Early 50s	M	British	Graphic designer	Single (one child, 17 years old)
G7	G7F	Late 50s	F	British	Physiotherapy assistant practitioner	Married (two children, one resident, one adult)
	G7M	Late 60s	M	British	Training manager	Married (two children, one resident, one adult)
	G7T	Mid 10s	F	British	Student and part-time sales associate	Single (lives with parents)
G8	G8F	Early 40s	F	British	Medical secretary	Married (one child, living together)
	G8M	Early 40s	M	British	Technical programme manager	Married (one child, living together)
G9	G9F	Late 20s	F	British	Researcher (mental health)	Single (lives with her partner)
	G9M	Early 30s	M	British	Service coordinator within IT	Single (lives with his partner)
G10	G10F	Late 30s	F	Non-British	Care support worker	Married (three children living together)
G11	G11F	Early 30s	F	Non-British	Academician as a civil engineer	Married (no children)
	G11M	Early 30s	M	Non-British	Geospatial engineer	Married (no children)
G12	G12F1	Late 20s	F	Non-British	PhD student (architecture)	Married (no children)
	G12F2	Early 20s	F	Non-British	Master student (business)	Single
G13	G13M	Late 20s	M	Non-British	PhD student (computer science)	Single
G14	G14F1	Early 20s	F	Non-British	Dentist	Married (one child, 17 months old)
	G14M	Late 20s	M	Non-British	University lecturer	Married (one child, 17 months old)
	F14F2	Late 20s	F	Non-British	Intern as economist	Single
G15	G15M	Late 30s	M	Non-British	IT engineer	Married (one child, 8 years old)
	G15F	Late 30s	F	Non-British	University researcher	Married (one child, 8 years old)
	G15C	Under 10s	F	Non-British	Student	Single
G16	G16F	Early 40s	F	British	Secondary school teacher	Married (two children, 3 and 8 years old)
G17	G17M	Late 30s	M	British	University researcher	Married (two children, 10 and 12 years old)
	G17F	Late 30s	F	British	Teaching assistant	Married (two children, 10 and 12 years old)
G18	G18M	Early 50s	M	British	University researcher	Married (three children—one living at home)
	G18F	Early 50s	F	British	Social worker	Married (three children—one living at home)
G19	G19F	Late 30s	F	British	Supermarket manager	Single (living alone)
G20	G20M	Early 50s	M	British	Mechanic	Married (two children—one living at home)
	G20F	Early 50s	F	British	Customer services—car garage	Married (two children—one living at home)

Table 1 (continued)

Participants		Age	Gender	By birth	Occupation	Household info
G21	G21M	Early 30s	M	British	Supervisor—baggage handler	Married (two children, 1 and 5 years old)
	G21F	Early 30s	F	British	Court clerk	Married (two children, 1 and 5 years old)
G22	G22M	Late 20s	M	British	Computer systems management	Single (lives with his partner

be picked up in the analysis of what was said—which as discussed below was of greater importance than card placement.

For the second deck, which does not feature in our analysis here due to space constraints, participants were instructed to put third-party apps they viewed as making unacceptable use of their data in the red box and those they could see some *value* in, in the blue box. If participants could not decide which box to place a card in, then it was placed in between the boxes and returned to afterwards for further deliberation. A final (red) card asked participants what they thought about the Databox concept and whether or not they could see a use for such a device in their everyday lives.

Working through the decks was no mere card sorting exercise. Indeed, we were not especially interested in what cards ended up in which box, but rather in the *mundane reasoning* [55] that provided for their placement. We therefore asked participants to articulate their decision-making, whether to the researcher or other family members or both, to give voice to taken for granted issues of privacy and personal data use, current and prospective, in their homes. In our interactions with participants, we referred to the activity as a 'game' to cultivate a tone of playfulness, which we were keen to harness to open up an engaging dialogue between family members and/or flatmates around personal and potentially sensitive topics. The designation also recognised that the assignation of cards was a collaborative, rule-bound and goal-directed activity, which we felt would aid in developing and sustaining a shared orientation. The rules of the game were purposefully lightweight. They did not, for example, seek to impose any particular turn-taking in the sessions where multiple family members were taking part to ensure parity of contribution. Questions were directed to the group, and individuals were free to contribute as much or as little as they wished.

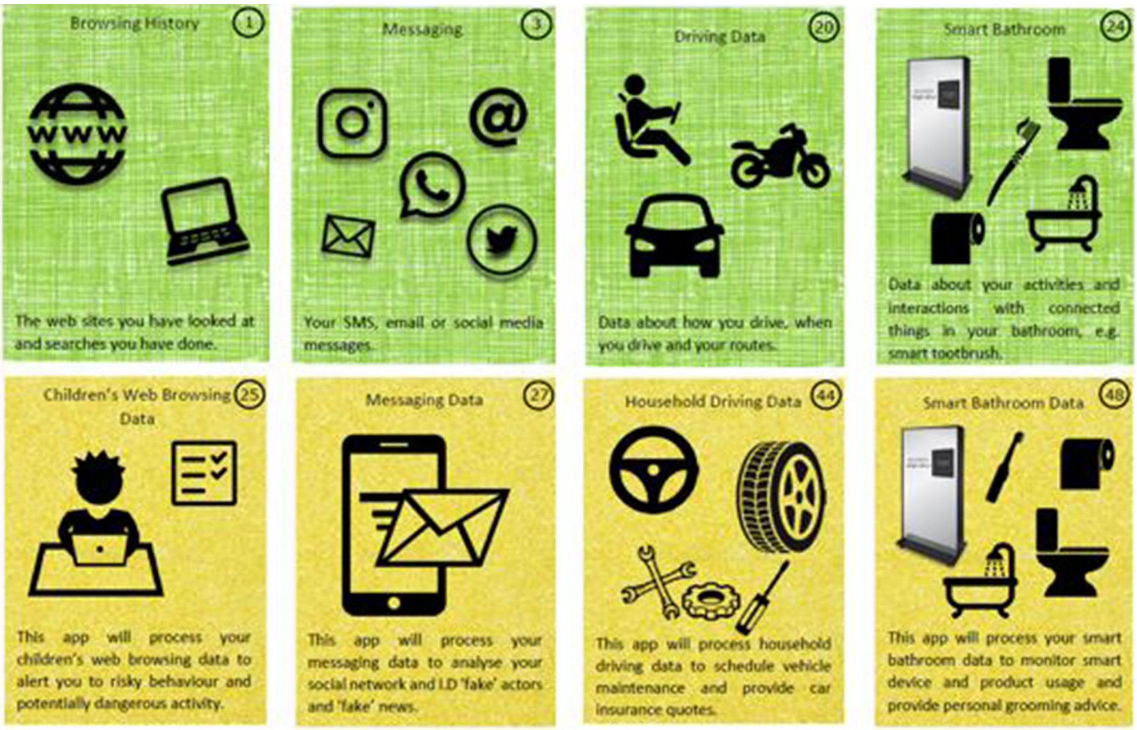
Insofar as the game was played in household groups, then the articulation was often collaborative, occasionally contested and arrived at through mutual elaboration. There were of course also occasions when group members held different and competing views, which led to some cards not being placed in either the red (keep private) or blue (others can access) boxes and the same applied to cards that were seen to be about irrelevant data.

3.3 Designing the ideation cards

We are not the first to make use of ideation cards in design. We use the term as a generic descriptor for the use of cards as a structuring device for research activities, not in the sense of the activities we used them for being ideational. In their survey of card-based design tools, Wölfel and Merritt [73] note that card-based approaches 'have been used widely by designers' to articulate the design process, make specific design proposals concrete and enable communication between designers and users. A broad range of card-based approaches are available to designers (Wölfel and Merritt identify eighteen), and an increasing array of online tools support their use. We designed our own cards from scratch, creating two different decks of 24 cards each, the first deck representing different types of data that can currently and will foreseeably be found in the connected home and the second deck representing third-party data processing apps that would exploit the data represented in the first deck. The decks were colour-coded to distinguish between them (as noted above, data types were green, apps yellow), and they were printed on paper and inserted in transparent sleeves. Both decks of cards were designed in a portrait format, with typical playing-card size dimensions (8 × 6 cm). Each card consists of four parts: the name of the ideation card, the card number, icons illustrating the data types or data processing and an explanation of each card (Fig.2); the back of the cards does not contain any content.

The first step in designing card content involved specifying data types that can currently and foreseeably be found in the connected home. We thus considered common data types currently found in our own homes and of people we know—e.g. web browsing histories, social media, photos and videos, online services such as banking and shopping, location data from our phones, black boxes for monitoring driving in cars, Alexa and Siri. We then turned to the Internet to identify IoT devices and products for the home and the data they generate, including the Internet of Useless Things [38], the Internet of Shit [37] and Postscapes [56], which allowed us to identify a broad range of connected devices that would generate data about everyday activities across the home. We also took research that we knew of into account, such as the Predictive Shopping List [20], the Living Room of the Future [59] and the Connected Shower [15]. We categorised devices and data into different types, online, wearable, environmental, smart products and appliances, vehicles, etc., as a means of collating the results of our survey (we use the term loosely) and parsing the rather large collection of discrete data sources finding their way into the connected home.

Having identified different types of domestic data, we set about formulating card content. This was an iterative process that consisted of narrowing down the range of potential options to a manageable proportion that could be addressed by participants in a reasonable time frame. We ended up with twenty-four data type cards falling under two main categories that we thought easy explainable to participants: online data and connected devices. The deck thus consisted of eleven online data cards and thirteen connected device data cards spanning a broad range of everyday activities from surfing the web to the apps used on mobile phones to biometric data, activity tracking, voice logs, home security devices, etc. (see [39] for full details). We then designed the second deck of data processing cards, each one matched to a corresponding data type card (see Fig. 2). The cards were then piloted on handful of colleagues to check their legibility, and minor amendments were made to text and images as needed prior to engaging participants with the Databox proxy.



The web sites you have looked at and searches you have done.

Your SMS, email or social media messages.

Data about how you drive, when you drive and your routes.

Data about your activities and interactions with connected things in your bathroom, e.g. smart tootbrush.

This app will process your children's web browsing data to alert you to risky behaviour and potentially dangerous activity.

This app will process your messaging data to analyse your social network and I.D 'fake' actors and 'fake' news.

This app will process household driving data to schedule vehicle maintenance and provide car insurance quotes.

This app will process your smart bathroom data to monitor smart device and product usage and provide personal grooming advice.

Fig. 2 The ideation cards (see [39] for all cards)

3.4 Data analysis

Analysis of the data involved obtaining a gross overview of participant reaction by quantifying the responses to each card in terms of how many participants wanted to share or keep the data private (see Fig. 3, for example). We then drilled down into the transcripts to understand the reasoning that accounted for participants' overall response to each card. Analysis here was initially done by the whole team and focused on identifying the discrete issues that occupied the participants' talk. We worked through a transcript for each card as a team, attending to explicit or implicit characterisations of the issue, and then members of the research team worked through the other transcripts individually, searching for other instances of the same issue or alternate issues. These were then collated, which allowed us to identify a spectrum of issues ranging from the positive to the negative accounting for the overall response to each card.

Our approach towards understanding the discrete response patterns emerging from the cardboard box study might be construed of as thematic analysis [5], but we would characterise it as the documentary method of interpretation.

> The method consists of treating an actual appearance [e.g., an utterance or sequence of talk] as 'the document of', as 'pointing to', as 'standing on behalf of' a presupposed underlying pattern. Not only is the underlying pattern derived from its individual documentary evidences … the individual documentary evidences, in their turn, are interpreted on the basis of 'what is known' about the underlying pattern. Each is used to elaborate the other. The method is recognisable for the everyday necessities of recognising what a person is 'talking about' … [21]

Ours is a common-sense method of interpretation used by professional analysts and lay persons alike, though 'rarely' acknowledged as sociologist Harold Garfinkel (ibid.) points out. It underpins thematic analysis as well as a broad range of analytic methods in the social sciences and HCI. It is indispensable to the practical job of making decisions about what persons are talking about (amongst many other sociological phenomenon) and determining when the same is the same, thereby enabling us to identify discrete patterns in our data. The decision-making and determination turn on being a 'member' [22] or competent speaker of a natural language subject to the 'hearer's maxim' [61]. As speakers of a natural language known in common and shared with our participants, we employed the hearer's maxim to identify the issues that occupied our participants' reasoning as manifest in their verbal consideration of each ideation card and thereby mapped out the spectrum of issues providing for the discrete response patterns represented in the pie charts. The mapping (i.e. the spectrum of issues accompanying each ideation card) is available online [39]. It should be seen and treated as an initial characterisation or sketch, rather than an exhaustive description, subject to revision, elaboration and refinement (e.g. as done in the course of writing up specific results for this paper) through continued use of and adherence to the hearer's maxim.

4 Findings

Participant response to the Databox proposition was generally positive. Overall, 75% of participants could see a place for such a device in their everyday lives for a variety reasons ranging from its perceived ability to enable agency, consent and control over data sharing, allowing people to be more

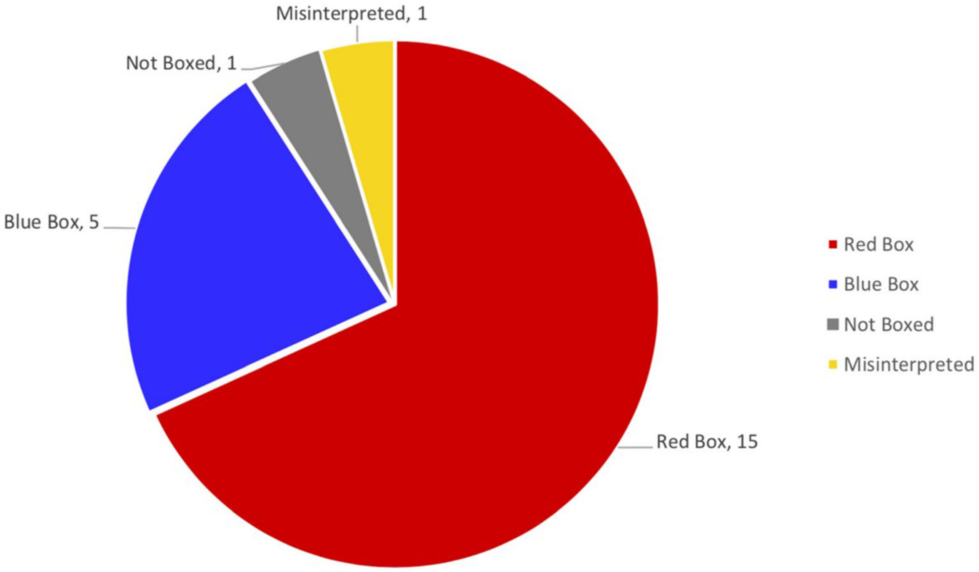


Fig. 3 Responses to card number 24

aware and informed about data use by third parties, minimising data distribution, reducing the risk of exposure to ‘unsavoury characters’, safeguarding household members and increasing privacy, choice and utility. Nevertheless, some participants entertained reservations about security and the potential for ‘hacking’, seeing the Databox as a potential ‘honey pot’ for thieves either online or physically. The perceived risks of ‘putting all your eggs in one basket’ largely underpinned 25% of participants rejecting the Databox proposition, though there was a minor view that ‘we already have enough tech to manage in everyday life’. Participants were also generally receptive to the idea of apps that process their personal data in return for some personalised service but showed a marked resistance to third-party apps that sought to process data regarding personal finance, location, social media and messages, data generated by smart vacuums and toys, voice logs, smart bathroom and personally identifiable data including biometric data (again see [39] for the specific app propositions with respect to these data). Resistance to the uses of such data was not necessarily due to concerns about the data itself but the appropriateness of the app propositions. For example, the proposed use of GPS data to alert family members when another was running late was seen as running contrary to social expectations and persons doing one another ‘the courtesy’ of contacting those who need to know such information.

We would like to say more about participants’ response to the Databox and specific app propositions, but we are cognisant of the constraints of space and the focus of this paper on collaborative data management in the connected home. We must then set aside these aspects of the study here and attend to the first deck of cards, which sought explore the interpersonal nature of data sharing. When asked to consider different types of personal data that can currently and will foreseeably be found in the connected home, we thus asked participants if they wished to share the data represented on cards one to twenty-four with someone they knew, either a family member, friend or some other personal acquaintance, and to articulate their reasoning for doing, or not doing, so.

Overall responses to deck one can be seen in Fig. 4. It can be seen at a glance, perhaps surprisingly for those wedded to the presumption of privacy, that the majority of cards were treated as referencing types of data that others can access. These include cards 1 (browsing history), 2 (apps used), 4 (location data showing places visited), 5 (personally identifiable data), 6 (personal videos and photos), 7 (films and music), 9 (shopping data), 11 (gaming data), 12 (location data for family monitoring), 13 (location data for monitoring pets), 14 (data about your baby’s breathing and temperature), 15 (physical activity data), 16 (data about environmental conditions in the home), 18 (data from household security devices), 19 (data about your household appliances), 21 (data about devices connected to your home network), 22 (smart toy data) and 23 (data about your cleaning practices and routines). Nevertheless, cards 1, 9, 12, 17 (voice logs from Alexa, etc.), 20 (driving data) and 22 were closely contested, and cards 3 (SMS, email or social media messages), 8 (financial data), 10 (biometric data) and 24 (smart bathroom data) were strongly viewed as referencing data that should be kept private.

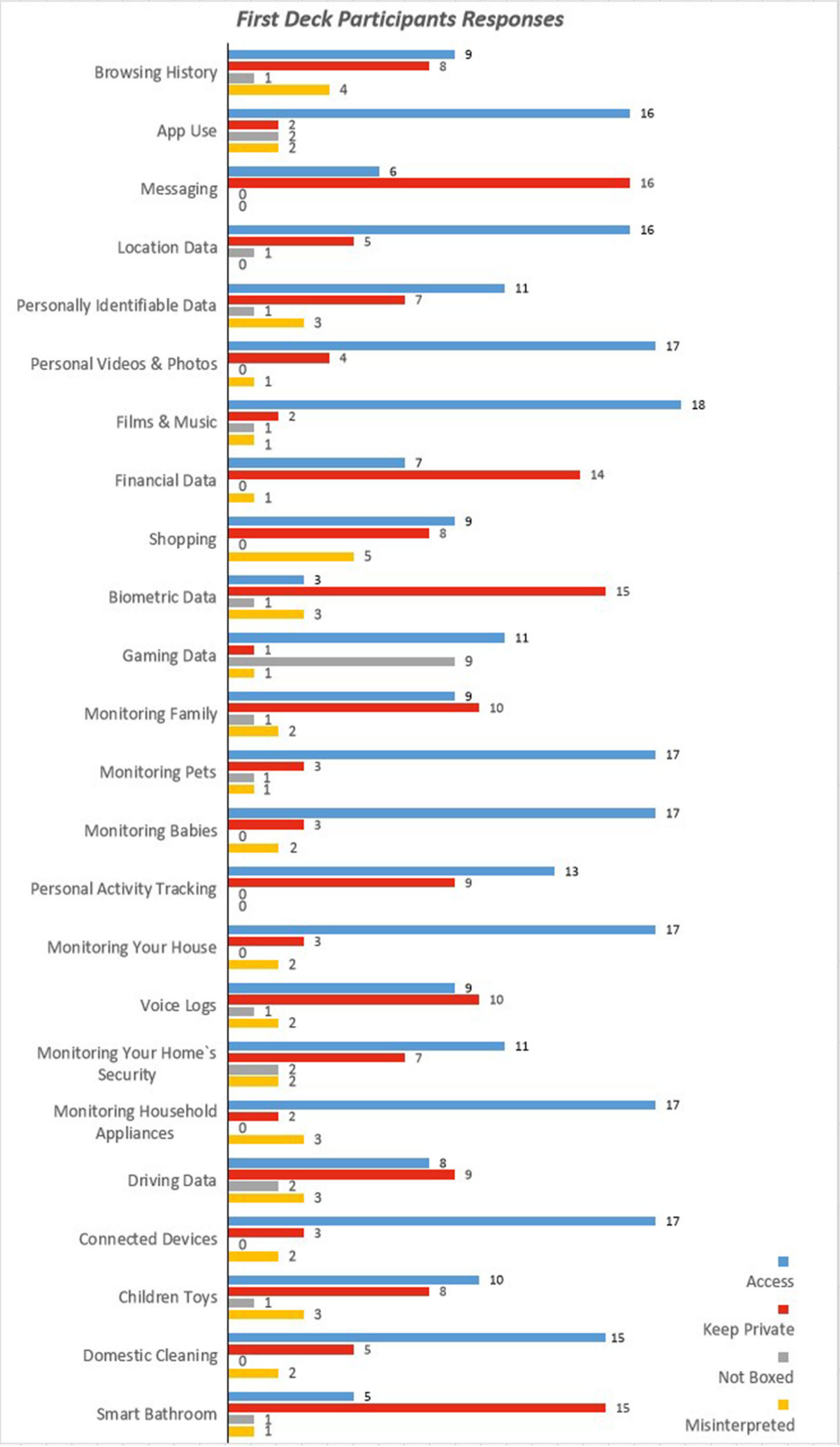
Figure 4 also makes it perspicuous that some minority of participants misinterpreted most of the cards. The purpose of this deck of cards was to provoke mundane reasoning about *interpersonal* data sharing *in a domestic context*. However, accessing or sharing ‘data’ is rarely occasioned as a topic for discussion in its own right in the ordinary run of domestic life, and it can, as the frequent but largely low level of misinterpreted responses indicate, be a difficult proposition to parse. Participants had no difficulty in understanding that external actors generally wanted to access their data, but accessing one another’s data occasionally eluded them when considering specific data types, which led to cards being misinterpreted and participants therefore reasoned about data sharing in terms of third-party access, rather than sharing data with someone they knew. Thus browsing history—well recognised as a target for external actors—was misunderstood by four participants, while messaging was not misunderstood by any. The latter, we would suggest, is less often subject to discussions of third-party monitoring (indeed increasingly such apps encrypt conversations) but is readily analogous to overhearing a house member’s phone conversation, or reading their diary. As such it was easily parsable as a matter of interpersonal concern.

That people do not usually talk about accessing or sharing ‘data’, and occasionally misinterpreted the purpose of this deck of cards, does not mean that they had nothing to say about interpersonal data sharing in a domestic context. On the contrary, as Fig. 4 indicates and invites us to inspect a rich array of reasoning underpinned participants responses to deck one and its towards unpacking this that we now turn. We should note, however, that just as we do not have sufficient space to elaborate participants’ response to the Databox and specific app propositions, then so we are constrained as to what we can say about deck one cards. It is not possible to treat each card separately. Instead, we examine the different *orders* of mundane reasoning that account for the overall response patterns surfaced in Fig. 4 to elaborate key issues involved in arriving at decisions to keep data private within the home, to allow others access and to contest access. It is with the former that we begin.

4.1 Keeping data private

Several discrete orders of mundane reasoning were invoked by participants in accounting for their decisions to keep data private within the home. These include the need to keep data

Fig. 4 Overall responses to deck one



private to avoid harms, manage accountability, preserve autonomy, exercise choice, maintain control and address underlying concerns about the Databox proposition and data sharing in general. We italicise text to indicate direct quotations from our participants below, and the specific cards that occasioned their comments are reference in brackets.

4.1.1 Avoiding harm

While Fig. 4 makes it perspicuous that participants were willing to let others access a great deal of their data, there were occasions when they deemed it necessary to keep data private within the home. Participants did not want to give others *limitless and uncontrolled access* to their data (C6, C10), it would be *a step too far*(C24) as *nobody needs to know* (C1, C15, C16), and it *should not be anybody's interest* (C2). As one participant put it with respect to location data (C4), for example:

> G5 / M: I just do not wish people to know where I am 24/7 … why you would want anybody to know where you are walking!

Not only did the prospect of unfettered access make participants *feel uncomfortable* (C8, C10, C12, C14, C15, C18); some data were seen as highly *personal*, containing *lots of private information* (C6, C8, C9, C15) and even *dangerous things*(C10) that others might *use against them* (C20). Unfettered access posed *a threat to personal security*, potentially enabling others to *pretend to be them when they are not*(C10) or opening them up to other forms of attack such as *burglary* (C4). It was also the case that decisions to keep data private were accounted for by participants in terms of the perceived need to protect the privacy of the other people they lived with and who were in their care. Unfettered access would then be *risky for children's safety* (C6)*, as there are too many dodgy people* (C22), and participants felt the demonstrable need to *show respect* to family members in the round (C12). It is clear then that participants' reasoning around privacy decisions was shot through with moral considerations of the potential *harms to people* occasioned by unfettered access to data in an interpersonal context. Thus, decisions to keep data private were not 'simply' made on the tautological grounds that the data is nobody else's business, but generally accounted for and warranted in terms of avoiding perceptible harms to both the individuals doing the decision-making and the other's they lived with who may affected by their decisions.

4.1.2 Accountability

This general concern with what might be called 'human security' and avoiding harm coalesced specifically around the issue of accountability. Privacy decisions thus hinged on the perceived potential for data to be used by others to *hold participants to account*, as the following extract, which arose in the course of a couple considering the use of Netflix and determining what to do with film and music data, illustrates (C7):

> G8 / M: I watched a program once about hookers and we had an argument about that didn't we? (Both laugh). It was a Louie Theroux kind of thing. And that felt kind of, you know, it popped up and we had an argument about that and I thought, "Well hang on a minute."
> G8 / F: Well, it was a bit letchy wasn't it?
> G8 / Interviewer: So, would you prefer not to share this?
> G8 / F: From me?
> G8 / M: Yeah.
> G8 / F: Oh my god (laughs).
> G8 / M: I think I am allowed to watch what I want to watch. I think everyone's allowed to have a letch. Yeah.

Participants sought to avoid enabling others to *have a moan* (i.e. to complain) at them in general (C2) but were particularly concerned at the prospect of being held to account by *particular individuals*, often their partners, with respect to *specific activities* including what they watch on TV (C7), their finances (C8), gaming (C11), exercise (C15), unguarded speech captured by voice logging (C17), use of the central heating (C19), domestic cleaning (C23) and bathroom and product usage (C24). Privacy decisions were driven by consideration of the *granularity* of data, e.g. seeing that £100 had been spent was not the same as seeing that £100 had been spent *on sweeties*, which was seen to undermine strategic ambiguity or more prosaically *the option of telling white lies* (C20). While accountability has its virtues (see Section 4.2.4), it is not always welcome for social as well as personal reasons. Privacy decisions were thus made to avoid disrupting the intimate interpersonal arrangements participants have already put in place to manage their accountabilities, *saying* rather than showing data (which is *not so friendly*) for example (C8), and to otherwise avoid *spoiling* social events (birthdays, Christmas, surprise parties, etc.) where *secrecy* is a necessary ingredient of their success (C1).

4.1.3 Identity/impression management and autonomy

The potential for data to be used by others to hold participants to account drove a particular concern with accountability that centred on identity/impression management and the importance of data privacy to personal autonomy. Participants did not want others to *get a clear picture about them*, and they especially did not want them to be able to apprehend *sensitive issues* (C1), including personal interests, bodily functions, sexual fetishes, political views, personality traits and future plans. It is notable that privacy decisions were not accounted for here tautologically either, but in terms of the need to manage what others might make of their data. Participants recognised the potential for their data to be *misconstrued* by others whether by accident or design and that it enabled others to make *assumptions* about them (C17). They wished to avoid giving others the *wrong impression* about themselves (C1) and *damaging their relationships* to boot (C17). Participants therefore sought to manage their identity and other people's impression of them, even those they lived with, in the face of the constant *creeping intrusion* of data into *every nook and cranny* of their lives (C23). As one participant put it with respect to the smart bathroom (C24):

> G6 / M: It is like smart watches and Fitbits and all the rest of it. There is going to be metrics for every part of your daily life, like how many times you have chewed your sandwich, because obviously there is a healthy number of chews, there has got to be; seventy-two, I think. But it is this thing that everything has got to be measured. For what reason I do not know. Dickens wrote to this up in the 19th century with Thomas Gradgrind who wanted to measure everything. Yeah, it was a problem then. It was this kind of hard empiricism that everything should be measured and quantified. Whether you know the value of these things is another matter.

Participants thus decided to keep data private to protect their identity and manage other people's impression of them in a bid to preserve their *autonomy*, which was seen to be increasingly threatened if not eroded by *this hard empiricism*. This again applied to others as much as the individual, with participants treating *children as sacred*(C22) and eschewing unfettered data access on the basis that it *compromises the foundations of liberty*(C8) and undermines personal *choice*.

4.1.4 Choice and control

It is becoming visible that privacy decisions were accounted for in terms of interconnected orders of mundane reason that put human security at the centre of participant's decision-making and sought to avoid potential harms through the management of interpersonal accountabilities, including identity and impression management, in order to preserve personal autonomy in the face of an unprecedented and apparently relentless degree of data harvesting that is seen to be destabilising the very foundations of liberty and thus undermining personal choice. That data might be personal and even sensitive means that participants expected to be able to exercise choice over access and to control who their data could or would be disclosed to (C3). As one participant put it with respect to family monitoring (C12):

> G22 / M: I cannot think of a situation in which I ever would share that data and it would have to be through me. It is not like they could just – I would not give people access to a repository of that if that's how you are looking at it?
> G22 / Interviewer: Yeah?
> G22 / M: Because – if it is other people's data then it is their data not my data, so I do not get to choose.

Participants did not want to expose a repository of their data to others in general, but rather wanted to *design* the disclosure of data for *specific recipients*(C3) or *relevant people* (C12). 'Recipient design' was seen as key to controlling data disclosure, even with intimate *partners* (C3), and even then, participants might want to keep *parts* of the data private (C15). The desire is to control who gets to see what was accounted for in terms of the need to manage the potential *consequences* of disclosure, such as it being *misconstrued* (C3). Recipient design was also seen as key to *respecting* and *protecting* the privacy of other parties implicated in the data (C3). Participants saw themselves as having a *duty of trust* not to share data that implicated others *unless* there was real need (C3). Participants also felt obliged to protect data due to potential legal liability (C3).

4.1.5 Rejecting the premise

It was a notable feature of participants' responses that while answering the questions we had asked them – i.e., in which box would they place this or that card and why? – that their answers were frequently qualified in ways that drew the underlying assumption of data collection and sharing into question. For example, with reference to accessing home security data (C18), including data from video cameras, one participant rejected the premise entirely:

> G16 / F: God it is like bloody big brother! I would not even video who is in my house in the first place.

She was not alone in throwing the fundamental presumption underlying the Databox, and data harvesting and use more generally, into question. Our participants offered a range of reasons and reasoning as to why the presumption was inappropriate. Participants simply could not understand the *point and purpose* (C14, C19, C22, C23) of allowing others to access data or think of a *reason* for allowing others to access data (C21, C22), and access most definitely requires *specific* reasons (C4). Similarly, they did not see why anyone would *need* to see the data (C13, C22) or see any *benefit* in letting others see the data (C9). Participants not only saw *no need* to share data (C23) but could not see why others would *want* to access it either. Not only would the data be utterly *uninteresting*(C3) and *not* something that others would want to know (C7), enabling access would be *over the top*, *grim*, *creepy* and *annoying* (C12, C24). It was the case too that the underlying proposition was simply seen as *redundant*, that others can already access data, so the question is neither here nor there (C20) or *practically irrelevant*, having nothing do with participant's everyday lives (C15). Participants also rejected the underlying presumption as they could see *no occasion* to share data (C4). This reflects a common feature of participants' decision-making, which turned throughout the game on formulating practical uses case making specific questions relevant to their everyday lives (either retrospectively or prospectively). Failure to do so saw the underlying presumption being rejected, whether or not cards were placed in the red (keep private) or blue (access) box (see Section 4.2.6).

4.2 Deciding that others can access data

Several discrete orders of mundane reasoning were also invoked by participants in accounting for their decisions to *allow others to access their data*. Participants reasoned about and accounted for access decisions in terms of having nothing to hide; that they already share data or would find it useful to do so; and because of the virtues of accountability. Nonetheless, access decisions were subject to choose and control, and, just as with privacy decisions, we found that participants also had occasion to question the Databox proposition and notion of data sharing in general.

4.2.1 Nothing to hide

Access decisions were accounted for in terms of participants having *nothing to hide* (C9, C11) and variations on this theme: that there was *nothing untoward* in the data (C1), *nothing personal or private* about it (C2, C16), nothing *dodgy* that *warrants hiding* (C1), *no secret*(C7) and just *harmless information*(C13) that participants *would not mind* or *would not be bothered* about sharing with others (C1, C11, C16, C20). As one participant put it when asked about allowing others to access her driving data (C20), for example:

> G9 / Interviewer: You would be worried about him judging your driving or your family judging your driving?
> G9 / F: I just do not think anyone would be bothered. So, I would not really mind.

The data was often seen as trivial, *just crap* (C2)—*sudoku scores*, *music*, *lights on*, *lights off*, etc.—and participants had *no issues* with sharing (C2, C19) as the data was seen to be of little consequence. Indeed, the data was seen as something that others could *not do anything with*(C2) and posed *no existential threat* (C7, C21). Participants were also sensitive to the social context in which they and the data reside, and that data do not belong to a single person *unless you live alone* (C18). There is then *no reason not to share* data (C19), and *no permission* is required by participants to share it *between us* (C22). *Trust*(C23) occasionally accounted for the potential availability of data to friends, but access decisions stood more firmly on the perceived harmlessness of the data and what is effectively shared ownership or at least shared rights and privileges. It was also the case that participants found it *too much effort* to keep data private (C24), that one would really have to have *something to hide*(C21) and *good reason* to hide it (C8) to want to go to the trouble of doing that.

4.2.2 We already share data

It soon became apparent that while focusing our questions on ideation cards, we were not dealing with purely hypothetical situations. Participants *already share* data with one another in the course of their everyday lives, and the social context in which they reside was often invoked to account for access decisions. Indeed, it became apparent that domestic life consists for many participants of a shared and mutually visible ecology of activities, practices, devices and data. Thus, access decisions were accounted for in terms of *living together*(C23) and *already sharing information*(C24) that *anyone can see* (C20, C21), where anyone means *everybody here* including *family and friends* (C5, C6). Participants *shared devices* (C1), used *family share* (C2), *synced data* across devices (C3), used *common* devices (C6), *joint accounts*(C8) and *shared* data sources (C9). For example (C1):

> G21 / F: The iPad, its open to anyone isn't it? Because we both have the log in
> G21 / M: Oh, and family
> G21 / F: And the laptop
> Interviewer: So, it is a shared device. What about your personal machines?
> G21 / F: We both have access to each other's. It is not intentionally shared; it just is shared.

Whether to *share messages* from others (C3), *monitor one another's whereabouts*, *coordinate people and events*, *enhance personal safety* (C4), *track and find each other* (C12), *calculate* each other's share of the energy bill (C19), etc., sharing data with others was for participants accountably something *you usually do, don`t you?* (C4). It is also usual for data to extend beyond the immediate confines of the home to other social actors, the *dog walker* (C18), *work colleagues* (C15), *local community groups* (C16), etc., reflecting participants' broader interests, engagement and relationships with others. Access decisions were thus predicated on the relevance of data to oneself-and-others. While there is some element of choice in this (C6), e.g. the particular messages or photos one shares, participants nevertheless saw the sociality of domestic life as largely prohibiting data being treated as wholly private (C1, C3, C4, C7, C8, C21). Rather data was seen as already shared by default of living with others, something that sits within a lively social context and is of intersubjective relevance and utility.

4.2.3 It could be useful

Access decisions predicated on the intersubjective relevance and utility of data extended beyond what participants already do with data to considerations of what might usefully be done with it. This is then a distinctive order of reasoning concerned not with extant data sharing practices but potential data sharing practices. Of particular note was the potential participants saw in exploiting data to *monitor* family members (C11, C12, C13, C14, C19, C22) in the course of carrying out their parental responsibilities. Participants thus envisaged using the data to *log the games* their children played (C11), to *see where* their kids and the pets are (C12, C13), to *prioritise children's health and well-being* (C14), to see how their child is *learning and progressing* and otherwise *curtail non-beneficial play* (C22). As one couple put it in considering household appliance data, for example (C19):

> G15 / F: I do not mind share it within our family. I do not know, probably the fridge would be aware [child's name] opens the fridge two times, three times, five times or more per day, I do not know
> G15 / M: You can make statistic of it. You can be aware of what choices she picking up from the fridge. You can understand and analyse as well. You can see which brands she loves or not. You can do many things with these. I think again this is also very useful thing to share.

Access decisions were shot through with prospective as well as retrospective accounts of data sharing in everyday life. Accompanying the shared by default, inherently social, intersubjectively relevant and useful grounds upon which data is already shared, prospective accountability surfaces the foreseeable potential of data to *help not hinder*(C14) participants in exercising the responsibilities they have for those they live with as complementary grounds for arriving at access decisions.

4.2.4 The virtues of accountability

Access decisions were also taken on the basis that definite virtues were seen to accompany the accountability created in sharing data with others. While data could be used to hold people to account for the things they have (or have not) done, this was not always a bad thing, nor is it limited to people but includes devices, products and appliances (C21, C23, C24). Participants thus found that data is *like having a witness*(C17) and that access would enable household members to *check* up on and *see* what is *going on* in the home (C21, C23, C24). The ability to check and see was in turn seen to *enhance safety* (C4, C19, C21) and to empower household members as the following consideration of household monitoring (C16) illustrates:

> G14 / F1: It is like I have this app, yeah, but they do not have and I cannot
> Interviewer: This is no just kind of app. You can think smart devices in your home, for example, for lights
> G14 / F2: We can share because do you remember? One day I forgot to close gas. We should share and they should know.
> G14 / M: What she says if we could track it in the device that she forgot to switch the gas off. I think it is good to share because we are living in a house that and we all care about this house. Yeah, and we all need to know what conditions are in the house.

Accountability allows *others to look at issues* (C19), including external parties where data was seen a key to rendering landlords accountable for dangerous appliances and providing *evidence* and *proof* of their failings (C16). Access decisions thus turned upon the perceived virtues of accountability and empowering others to inspect what is going on in the home as a necessary precursor to intervention.

4.2.5 Choice and control

Those participants' attributed virtues to accountability do not mean that they were happy to allow unfettered access to their data. Participants recognised the *occasional* need for privacy, whether to avoid rendering oneself accountable for things they do *not* want to be accountable for (C4) and feeling concomitantly *uncomfortable* or *embarrassed* (C10), breaching *secrecy* (C17), spoiling *surprises* (C9, C12, C19) or simply to avoid others taking data *out of context* (C1, C15). Access is thus dependent on *who* is looking at the data (C2) and is accompanied by the practical need to *constrain* access based on the *type* of data in question and the *potential recipients* (C3), as one participant highlights in considering smart toys (C22), for example:

> G16 /F: In principle [yes], but there is a big difference between sharing with your partner or the father of your children and sharing with even the next step out of family or close friends. There is a massive difference between that.

Access is also dependent on *context* (C6, C18), on not only who is accessing what but why and to what end. While being prepared to allow *different people* to access *different data*(C7) in principle, doing so has to be *appropriate* to both recipient *and* sharer (C6). It also has to be done in a *controlled way* (C6, C12, C15) for *selective people* (C4, C6, C11, C12, C13, C14, C15, C16, C18, C19, C22) at *selective times* (C4, C12) on a *limited basis*(C5) for a *specific purpose* (C5, C14) and involves *only* so much data as is necessary (C19). Just as participants decided to keep data private because they wished to exercise control over its disclosure through 'recipient design', then so too access decisions turn on the same proviso.

4.2.6 Rejecting the premise

Access decisions were clearly rooted in the social fabric of participants' everyday lives, and while they were evidently willing to share data with other people they knew, this did not mean they accepted the Databox proposition without question. Participants placed value on *speaking to people*(C3) and so were unconvinced by the practical day-to-day relevance of the Databox proposition. Others did not think the people they knew would be *impressed* by their data (C7) or *really care* about it (C23), that it was essentially uninteresting, though some worried that it might *make others feel bad*(C9) and *breed hypochondriacs* (C14). Some participants felt that in the absence of actually being asked to share data with others, they could not really make an *informed decision* (C21), but by far and away the most common reason for doubting the proposition lay in the question, why? *Why would they want to know* (C23)? *Why, for what purpose* (C1)? It is not simply that participants *need a reason*(C2) to share data that is under their personal control but that whatever the reason it *would be weird* (C3, C16)*, they would be weird*(C24) and they might think *you are a bit weird* too (C1):

> G9 / M: I would share it with you.
> G9 / F: Yeah. But why though? Like, it is not a resounding "No, I wouldn't let you look through my search history." I would not mind it. It is not like anything there is a cause for concern. But it is just kind of like, a bit awkward. You might feel like you have to justify stuff you are looking at or they might just think you are a bit weird.

The evident willingness of participants to allow other people they know to access their data, indeed the default inevitability of access in many cases along with the retrospective and prospective intersubjective utilities and virtues that accountably attach to it, should be tempered then by the *weirdness* of technical mechanisms that seek to support interpersonal data sharing. This is not to dismiss technological efforts—75% of participants could see a place for the Databox in their everyday lives—but it is to highlight their anthropological *strangeness* at this point in time.

4.3 Contesting access

Before moving on to consider what our findings might mean for the design of technological mechanisms supporting interpersonal data sharing and collaborative data management in the home, it also important to recognise the contested character of our findings. There is a sense in which every ideation card presented was contested, insofar as no type of data was wholly agreed upon as private or accessible by our participants. Furthermore, some cards were not boxed at all. We focus here briefly on the reasoned grounds upon which this outcome stood (we say briefly as not many cards were treated this way). Card 11 (gaming data) was the most contested card—9 participants did not box it—but this was on the mundane grounds that it was simply *irrelevant*, they did not play digital games and so this data was not a feature of their everyday lives. Two participants simply could not decide how to respond to a couple of cards (C2, C18), being *50-50* as to whether or not it would be a good idea to share data or not. A couple of participants agreed to disagree, seeing the others' *logic* but not concurring with it (C4, C7). And one participant begged the question as to *why* you would store the data in the first place (C5)? Lack of relevance notwithstanding, then lack of agreement was the most common grounds upon which access decisions were challenged and contested, though the reasons offered were not all of apiece. One participant sought to avoid being accountable for their behaviour and so not would agree to let their partner access the data (C20). Another had nothing to hide, but their partner did not want the data anyway (C24). However, access was a more contentious topic *outside* of immediate partner or spouse relationships. Thus, housemates contested access on the basis of the data being *personal* and *lacking trust* in recipients (C1, C10), and children and teenagers, while happy to access their parents' data, did *not* wish to reciprocate (C12, C17).

> G15 / C: Alexa and Siri? I like using Siri.
> G15 / F: But if I am hearing what you are telling to them, do you mind if I hear those conversations between you and Siri?
> G15 / C: No!
> G15 / M Why not?
> G15 / C: This is my data.
> G15 / F: This is too much personal?
> G15 / M: You have to explain us why? We want to know it.
> G15 / C: No. No. No.
> Interviewer: I guess you are using them for personal purposes?
> G15 / C: Yes. This is private.

The contested character of our findings reveals an underlying *dynamic* to domestic life that is also consequential to collaborative data management and its support. Simply put, people will disagree, they will not always want to be accountable to one another, they will have occasion to lack trust, and they will not necessarily want to reciprocate. The nature of our relationships, the kinds of people we live with, their ages and stages of life, all shape and drive this dynamic and it is towards understandings the implications it holds for design that we now turn.

5 Discussion

It could be argued that the cardboard box study speaks to the data privacy literature by asking people to decide whether or not to keep data private.For the vast bulk of the time, data privacy is simply not an issue in domestic life. As the participants in our study make perspicuous, people already share data with one another as a matter of course by virtue of their living in a shared ecology of activities, practices and devices. Amongst themselves there is little that warrants hiding; indeed hiding data from other co-inhabitants is often seen to involve too much effort given that much of it is 'crap' that poses 'no existential threat', though we note members of shared households are sometimes more circumspect. Furthermore, members find that a great deal of data shared by default of living together *is* socially useful, enabling them to know what others are doing and to respond appropriately. The brute fact is that the *sociality* of domestic life often prohibits data being treated as wholly private. Rather data is seen and treated as something that is already shared by default of living with others and is of intersubjective relevance and utility.

This is not to say there is no need for privacy in the connected home. Our study makes it perspicuous that privacy is occasionally invoked to negate the potential for data to render members accountable to the cohort for everything they do (what they eat, watch on TV, how much energy they use, the cleaning they do, or time they spend playing games, etc.). The what of the matter is neither here nor there, as what people might be held accountable for changes from home to home, cohort to cohort, but there is clearly strong need to be able to control one's accountability in the connected home of the present and the future. As our study makes visible, controlling accountability is key to a person's identity and impression management [29], particularly where sensitive issues (such as personality traits, bodily functions, sexual fetishes and political views) are concerned. In short, our participants sought to control the accountabilities created by data to avoid giving others the 'wrong impression' about themselves, which might in turn 'be damaging' to their relationships.

The potential for data to damage people and their relationships lies at the heart of our participants' concern with data privacy. Privacy then plays a *social function*. It is not an end in itself, not merely a matter of being able to withhold information, but a means to an end: relationship maintenance. The social function of privacy is to avert perceptible risks to *human security* and thus avoid harms to members of the social unit created, in this case, by the increased potential for accountability that accompanies the increased amounts of data in the connected home. While the ability to hold people (and devices) to account clearly has its virtues, unchecked it creates real and tangible threats to members' interpersonal relationships. The home is a key site for 'intimate personal violence' [e.g. 49], and the digital already is implicated in domestic harms, enabling gas lighting and domestic abuse [e.g. 3, 18]. Our participants saw occasional need then to control access to data in order to avoid rendering themselves uncomfortable, subject to embarrassment or other serious consequence including effects that might impact their liberty and autonomy. At the same time, however, participants recognised the intersubjective nature of data: that it like them resides in a social context inhabited by other people and is located in a mutually visible ecology of activities, practices and devices that accords by default of living together *shared* rights and privileges over data access and disclosure. Data is thus a 'relational object' [10], i.e. an object that is inextricably embedded in a nexus of social relationships and relational concerns that organise access, and the shared rights and privileges that control it include the right to *contest* privacy decisions and *disagree* with them.

There is a strong sense then in which privacy decisions are *negotiated*, not in the sense understood by the interdependent privacy literature as to do with conflict resolution, but with the disclosure (or not) of data. As Tolmie and Crabtree [67] elaborate, the negotiation is done through 'the 'calculus of accountability', which governs the practical politics of sharing in everyday life. The calculus seeks to balance the management of cohorts, identities, and the visibility of the digital self in the networked world with considerations of just who it is persons might be accountable to and in what ways. Our study like theirs finds that data is disclosed on the basis of 'recipient design', i.e. through the interactional crafting of data access and disclosure in specific places, at specific times, in specific ways, for specific people to mitigate perceived risks or threats. Recipient design is a pronounced feature of the cardboard box study, driving both privacy and access decisions. Our study extends our understanding of the recipient design of data disclosure, not only highlighting the moral duty of trust that informs the calculus with respect to mixed data, and the need to enable persons to allow different people to access different data, at selective times, on a limited basis, for a specific purpose, and only with so much data as is necessary, but also raising the critical question of who gets to decide these matters and *how*?

Recipient design is not only concerned with the interactional tailoring of information, including its non-disclosure. As our study makes perspicuous, it also trades on and presupposes that the parties to interaction have the *rights* and *privileges* to do so. In environments where data is shared by default of living together, collaborative data management mechanisms are needed that allow household members to *make* that determination and specify who amongst them *can* take decisions to disclose data or withhold access. This is a non-trivial requirement, for as insofar as data is distributed across members, then rights and privileges are also be distributed and tied to the different types and subsets of data. Add to this the dynamics of family life -of parenting and being parented, of growing up, and growing old, etc.-, it becomes clear that mechanisms not only need to be capable of handling the specifics of data sharing on any occasion (the just who, just what, just when, for just how long, etc.) but also the fluid set of relationships that are implicated in its use. What on one day in one situation only requires one parents to say so, for example, may on and in another require both, and in the future their children's as well, or instead.

5.1 Moving beyond interdependent privacy

Any suggestion, then, that interdependent privacy might hold the keys to collaborative data management in the home would, at this point in time, be rather tenuous for we are not dealing here with individuals-in-a-group but persons *meshed together* in a social unit, who share data by default of living together and who have shared but differentially distributed rights and privileges over data access and disclosure. Furthermore, those rights and privileges are shaped by the fluid dynamics of everyday life in an environment where privacy decisions are always occasioned and subject to the calculus of accountability and negotiation through recipient design on a case-by-case basis. The mechanisms proposed by interdependent privacy assume that privacy decisions allowing persons to avoid harm can be *prefigured*, a matter of collaboratively specifying preferences and policies beforehand or engaging in conflict resolution *after the fact*. However, the priorities of everyday life (getting the kids up, dressed, fed, to school on time and all that other stuff we *have* to do) seem to us to mitigate against families expending effort on encoding data and attaching policies to its use. Furthermore, there is no possibility of members specifying privacy policies in advance other than in the most gross or general of terms, for not only do all rules imply infinite regress and beg the question of when and how they should be applied, they are also 'merely advisory to action' [77] and so their practical relevance to actual concrete situations has to be determined within the unfolding flow of everyday life. Manually voting or delegating conflict resolution to automated strategies based on measures or indeed the *metrication* of intimacy or reciprocity is unlikely to settle disagreements either; on the contrary, they may well exacerbate them.

It might be argued that we are a little harsh in our treatment of interdependent privacy. However, our study, amongst many others, underscores the fact that people have preferences for data sharing, that these implicate others, that negotiations take place between them, that conflicts arise and are resolved. Nonetheless, efforts to support collaborative data management in the home have a very long way to go. As Tolmie and Crabtree [67] put it:

> Digital systems derail the case-by-case interactional crafting and shaping which is at the core of the practical politics of sharing, and instead oblige people to engage in generic rather than situated practices of action and reasoning to manage the sharing of personal data in the digital world.

If interdependent privacy is to enable collaborative data management in the home, it will need to change its analytic focus and move beyond an individual-in-the-group conception of privacy to see privacy as a function within a social unit that enables its members to avoid the potential harms created by accountability in an increasingly connected world [28]. It will need to move beyond photos as test cases for its approaches. It will need to develop support mechanisms to enable the differential distribution of rights and privileges within the dynamic and fluid context of everyday life in the home. And it will need to support the calculus of accountability and enable recipient design not as a precursor to data access and disclosure but as something that can be crafted on a case-by-case as members deem circumstance and occasion dictate. Current access control and negotiation mechanisms do not offer this level of collaborative support.

5.2 Limitations

The results reported herein should be considered in light of some limitations. Of the 22 households in our study, it was not possible to always include all members, for various practical reasons—disinterest in taking part, unavailability and additionally in the case of children it might simply be that their age rendered it impossible. This did mean though that we inevitably missed some in-groupdynamics—for example, while a 7-years-old might be too young to meaningfully participate in a 90-min group interview, they would nevertheless have some role to play in regard to data generated by them in the home. While our cohort did cut across age, family role, occupation, class and ethnicity, it could certainly be argued that additional diversity amongst our participants would have expanded the study's claims of generalisability. We recognise that even at the level of mundane reasoning considered here, profoundly different cultures and living arrangements might produce different findings. Similarly, a greater involvement of children might have surfaced different interactions—though the practical challenges of further involving children would likely require a study specifically formulated for this purpose.

Conducting the game as a shared enactment amongst members was a deliberate choice to surface typical everyday household engagements. Inevitably, this also means that disparities between members—whether in terms of authority, agency, expertise or other—might impact on their engagement with the game. From the standpoint of individualistic theorisations of privacy, this could be considered a weakness, though from the authors' perspective it is simply a reflection of the asymmetries which are, rightly or wrongly, to be found in any group. In regard to participants' capacity to be honest in front of one another—one could easily imagine for example a teen being unwilling to share particularly contentious information in front of their parents that they *might* otherwise share under the guise of anonymity with an interviewer—this is certainly a possibility, though we did encourage all participants at the start of the game to focus on general principles rather than specific examples should they have any concerns. Again, this is a case where a specifically tailored research design would be productive.

Finally, as noted in Section 4, many cards were misinterpreted by a minority of participants. In part we believe this reflects the fact that questions of privacy are commonly framed as being a matter of threats from unknown third parties, to the detriment of questions of interpersonal privacy. The presence of deck two, which *did* probe such questions, may have contributed to the confusion. Regardless, the instructions given to participants should have been clearer so that some responses did not have to be disregarded from the analysis.

6 Conclusion

The home is a site marked by the increasing collection and use of personal data, whether online or from connected devices. This trend is accompanied by new data protection regulation and technological efforts to develop privacy enhancing technologies (PETs). However, both focus on the individual despite the fact that a great deal of the data generated within the connected home is interpersonal in nature [28] and cannot therefore be attributed to an individual. There is a significant gap in our understanding of the increasing collection and use of personal data in *social* contexts generally and the home in particular and the concomitant challenge of enabling collaborative data management in the connected home. In a bid to address the challenge, we designed and deployed the 'cardboard box', a proxy for a PET called the Databox that adapts the technology probe approach to provoke mundane reason about the interpersonal nature of data in the home. The study reveals that:

- A great deal of data in the current and prospective connected home is *shared by default of persons living together* in a mutually visible ecology of activities, practices and devices.
- Privacy is an occasioned (not ubiquitous) feature of everyday life in the home that plays a *social function* concerned to ensure *human security* and protect people from the harms created by increased accountability created by data.
- Collaborative mechanisms are required to enable the case-by-case negotiation of privacy decisions, including the *differential distribution of rights and privileges* in a dynamic and fluid context.

These original findings build on and extend previous work [13, 28, 67] and are of relevance to technological efforts to support the collaborative management of data. However, as we show in this paper, current technological solutions designed under the auspices of 'interdependent privacy' [34] are predicated on inadequate conceptualisations of users as individuals-in-a-group rather than members of a social unit whose data is necessarily meshed together with others. This leads to collaborative access control and conflict resolution (negotiation) mechanisms that are ill-suited to deployment in the home. Not only are household members unlikely to invest time and effort in pre-specifying privacy policies to regulate the use of shared data by others in the home, the practical relevance of such rule-based solutions will always be subject to evaluation on actual occasions of data access and disclosure. Furthermore, both manual and automated negotiation mechanisms fail to support the negotiated character of data sharing as understood by household members, which is concerned with the recipient design of data access and disclosure rather than conflict resolution, and medicated solutions to conflict are only likely to pour oil on troubled waters.

Current technical mechanisms offered by interdependent privacy do not provide adequate support for collaborative data management in the connected home, and while participants in our study saw some promise in the Databox, we would sound a note of caution. Technological solutions are unlikely to sit comfortably in an environment where its inhabitants increasingly perceive themselves to be *threatened* by increasing volumes of data. While household members are clearly cognisant of the potential for harm, solutions that help them manage human security by enabling or curtailing access to data are currently seen as 'a bit awkward'. It is not that people do not get the point of technological solutions but rather that they are seen to be part of an 'annoying' problem, a 'hard empiricism creeping into every nook and cranny' of domestic life, where 'everything is measured and quantified'. Access control solutions thus seem 'over the top' and 'unfriendly' in an environment where a great deal of data is born social and otherwise shared by default of living together and stand in sharp contrast to 'speaking to people'. There is promise then, but it is tempered by human frustration at the predicament that makes technological solutions necessary, and this may well generate some resistance to adoption in the short term. Nonetheless, there is clear and evident need to support collaborative data management and enable people to negotiate interpersonal data access in the home. The potential for harm is otherwise too great.

Funding This work was supported by the Engineering and Physical Sciences Research Council (grant numbers EP/M001636/1, EP/N028260/2, EP/R03351X/1). Murray Goulden is also supported by a Nottingham Research Fellowship (NRF) Award.

Data availability The data set drawn on by this paper is publicly available: https://drive.google.com/open?id=1TKEBPN9HNa6WMmnrAVAb3gZ00Na4qT0e.

References

1. Altman I (1975) The environment and social behaviour: privacy, personal space, territory and crowding. Brooks Cole, Monterey
2. Bischoff P (2018). What is the consumer privacy bill of rights? Comparitech, 27 November 2018. https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights. Accessed 6 December 2019
3. Bowles N (2018). Thermostats, locks and lights: digital tools of domestic abuse. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. Accessed 6 December 2019
4. Boyd D (2012). Networked privacy. Surveillance & Society, vol. 10, no. 3&4, December 2012, https://doi.org/10.24908/ss.v10i3/4.4529
5. Braun V, Clarke V (2008) Using thematic analysis in psychology. Qualitative research in psychology, vol. 3 (2), pp. 77–101
6. Button G, Harper R (1995) The relevance of 'work-practice' for design. Computer Supported Cooperative Work: The Journal of Collaborative Computing, vol. 4, December 1995, pp.263–280
7. Chen J, Ping J W, Xu YC, Tan B (2015). Information privacy concern about peer disclosure in online social networks. IEEE Transactions on Engineering Management, vol. 62, issue 3 August 2015, pp. 311–324
8. Cognizant (2015). The rise of the smart product economy. https://www.cognizant.com/InsightsWhitepapers/the-rise-of-the-smart-product-economy-codex1249.pdf. Accessed 6 December 2019
9. Crabtree A, Mortier R, Rodden T, Tolmie P (2012) Unremarkable networking: the home network as a part of everyday life. In DIS '12. Proceedings of the Designing Interactive Systems Conference, Newcastle, UK, 11-15 June, 2012. New York: ACM Press, pp. 554-563
10. Crabtree A, Mortier R (2015). Human data interaction: historical lessons from social studies and CSCW. In ECSCW '15. Proceedings of the 14th European Conference on Computer Supported Cooperative Work, Oslo, Norway, 19-23 September, 2015. Switzerland: Springer International Publishing, pp. 1-20
11. Crabtree, A. and Tolmie, P., 2016. A day in the life of things in the home. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*,
12. Crabtree A., Tolmie P., Rouncefield M. (2013) "How many bloody examples do you want?" Fieldwork and generalisation. In: Bertelsen O., Ciolfi L., Grasso M., Papadopoulos G. (eds) ECSCW 2013*: Proceedings of the 13th European Conference on Computer Supported Cooperative Work*, 21-25 September 2013, Paphos, Cyprus. Springer, London. https://doi.org/10.1007/978-1-4471-5346-7_1
13. Crabtree A, Tolmie P, Knight W (2017). Repacking privacy for a networked world. Computer Supported Cooperative Work: The Journal of Collaborative Computing and Work Practices, vol. 26 (4), May 2017, pp. 453–488
14. Crabtree A et al (2018). Building accountability into the internet of things: the IoT Databox model. Journal of Reliable Intelligent Environments, vol.4, no.1, January 2018, pp. 39–55
15. Crabtree, A, Hyland L, Colley J, Flintham M, Fischer J, Kwon H (2019). Probing IoT-based consumer services: 'insights' from the connected shower, personal and ubiquitous computing, Online First. DOI 0.1007/s00779-019-01303-3
16. de Montjoye Y, Wang S, Pentland A (2012). On the trusted use of large-scale personal data. Bulletin of the IEEE Technical Committee on Data Engineering, vol.35, no.4, March 2012, pp. 5–8
17. Flintham M, Goulden M, Price D, Urquhart L (2019). Domesticating data: socio-legal perspectives on smart homes and good data design. Theory on Demand, vol. 29, pp. 343–360
18. Freed D, Palmer J, Minchala D, Levy K, Ristenpart T, Dell N (2018). "A stalker's paradise" – how intimate partner abusers exploit technology. In CHI '18. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Canada, 21-26 April, 2018. New York: ACM Press, paper no. 667
19. FTC Staff Report (2015) Internet of things: privacy and security in a connected world. Federal Trade Commission, January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Accessed 6 December 2019
20. Fuentes C, Porcheron M, Fischer JE, Costanza E, Malik O, Ramchurn SD 2019. Tracking the consumption of home essentials. In CHI '19. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Glasgow, Scotland, 4-9 May, 2019. New York: ACM Press, paper no. 639
21. Garfinkel H (1967). Studies in ethnomethodology. Englewood Cliffs, New Jersey: Prentice Hall
22. Garfinkel H, Sacks H (1970) On formal structures of practical action. In: McKinney JD, Teryakian EA (eds) Theoretical sociology: sociology: perspectives and development. Appleton-Century Crofts, New York, pp 337–366
23. Garfinkel H (2002) Ethnomethodology's program: working out Durkheim's aphorism. Rowman & Littlefield Publishers, Lanham, Maryland
24. General Data Protection Regulation (2016) Official Journal of the European Union, vol.59, pp. 1–88
25. Gnesi S, Matteucci I, Moiso C, Mori P, Petrocchi M, Vescovi M (2014). My data, your data, our data: managing privacy preferences in multiple subjects personal data. In APF 2014. Proceedings of the Annual Privacy Forum, Athens Greece, 20–21 May 2014. Cham: Springer, pp. 154–171
26. González-Manzano L, González-Tablas A, Fuentes J, Ribagorda A (2014). cooped: co-owned personal data management. Computers & Security, vol 47, November 2014, pp. 41–65

27. Guo Y, Zhang L, Chen X (2014). Collaborative privacy management: mobile privacy beyond your own devices. In SPME '14. Proceedings of the ACM MobiCom Workshop on Security and Privacy in Mobile Environments, Maui, Hawaii, 7-11 September 2014. New York: ACM Press, pp. 25-30
28. Goulden M, Tolmie P, Lodge T, Mortier R, Pietilainen A, Teixeira R (2017). Living with interpersonal data: observability and accountability in the age of pervasive ICT. New Media and Society, vol. 20 (4), April 2018, pp. 1580–1599
29. Goffman I (1956) The presentation of self in everyday life. University of Edinburgh, Edinburgh
30. Greif I (1988) Computer supported cooperative work: a book of readings. Morgan Kaufmann Publishers, San Mateo
31. Harper R (ed.) (2011). The connected home: the future of domestic life. London, Springer-Verlag.
32. Hu H, Ahn G (2011). Multiparty authorization framework for data sharing in online social networks. In DBSec 2011. Proceedings of the IFIP Annual Conference on Data Applications Security and Privacy, Richmond (VA), USA, 11–13 July 2011. Heidelberg: Springer, pp. 29–43
33. Hu H, Ahn G, Jorgensen J (2013). Multiparty access control for online social networks: model and mechanisms. IEEE Transactions on Knowledge and Data Engineering, vol. 25, issue 7, July 2013, pp. 1614–1627
34. Humbert M, Trubert B, Huguenin K (2019). A survey on interdependent privacy. ACM Computing Surveys, vol.52 (6), October 2019, article 122
35. ICO (2019). Personal data of both the requester and others. https://ico.org.uk/media/1209/personal-data-of-both-the-requester-and-others-foi-eir.pdf. Accessed 6 May 2020
36. Ilia P, Carminati B, Ferrari E, Fragopoulou P, Ioannidis S (2017). SAMPAC: socially-aware collaborative multi-party access control. In CODASPY '17. Proceedings of the 7th ACM Conference on Data and Application Security, Scottsdale (AZ), USA, 22-24 March 2017. New York: ACM Press, pp. 71-82
37. Internet of Shit (2019). https://internetofshit.net. Accessed 24 September 2019
38. Internet of Useless Things (2019). https://iout.rehabagency.ai. Accessed 24 September 2019
39. Kilic D (2019). The cardboard box study. https://drive.google.com/open?id=1TKEBPN9HNa6WMmnrAVAb3gZ00Na4qT0e. Accessed 12 December 2019
40. Kekülлüoğlu D, Kökciyan N, Yolum P (2016). Strategies for privacy negotiation in online social networks. In PrAISe '16. Proceedings of the 1st International Workshop on AI for Privacy and Security, The Hague, Holland, 29-30 August 2016. New York: ACM Press, pp. 1-8
41. Li F, Yu J, Zhang L, Sun Z, Lv M (2017a). A privacy-preserving method for photo sharing in instant message systems. In ICCSP '17. Proceedings of the International Conference on Cryptography, Security and Privacy, Wuhan, China, 17–19 March 2017. New York: ACM Press, pp. 38–43
42. Li Y, Vishwamitra N, Knijnenburg B, Hu H, Caine K (2017b). Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos. Proceedings of the ACM on Human-Computer Interaction, vol.1, December 2017, article 67
43. Mehregan P, Fong P (2016). Policy negotiation for co-owned resources in relationship-based access control. In SACMAT '16. Proceedings of the 21st ACM Symposium on Access Control Models and Technologies, Shanghai, China, 5-8 June 2016. New York: ACM Press, pp. 125-136
44. Mortier R et al (2016). Personal data management with the databox: what's inside the box? In CAN '16. Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking, Irvine, California, 12 December 2016. New York: ACM Press, pp. 49–54
45. Miller P (2018) What is edge computing? The Verge, 7 May, 2018. https://www.theverge.com/circuitbreaker/2018/5/7/17327584/edge-computing-cloud-google-microsoft-apple-amazon. Accessed 6 December 2019
46. Mydex (2007). https://mydex.org/about-mydex. Accessed 6 December 2019
47. Nishi M (2018). Data protection in Japan to align with GDPR. Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, 24 September 2018. https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr. Accessed 6 December 2019
48. Nissenbaum H (2004). Privacy as contextual integrity. Washington Law Review, vol. 79, no. 30, February 2004, pp. 101–139
49. Office for National Statistics (2016). Violent crime and sexual offences - intimate personal violence and serious sexual assault. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/compendium/focusonviolentcrimeandsexualoffences/2015-02-12/chapter4violentcrimeandsexualoffencesintimatepersonalviolenceandserioussexualassault. Accessed 6 December 2019
50. Olteanu A, Huguenin K, Dacosta I, Hubaux J (2018). Consensual and privacy-preserving sharing of multi-subject and interdependent data. In NDSS. Proceedings of the Symposium on Network and Distributed Systems Security, San Diego (CA), USA, 18-21 February 2018. https://www.ndss-symposium.org/wp-content/uploads/2018/07/ndss2018_06B-1_Olteanu_paper.pdf. Accessed 7 May 2020
51. Palen L, Dourish P (2003). Unpacking 'privacy' for a networked world. In CHI '03. Proceedings of the CHI Conference on Human Factors in Computing Systems, 23-27 February 2003. New York: ACM Press, pp. 129-136
52. Parsons T (1968) The structure of social action. New York: Free Press
53. Petronio S (2010) Communication privacy management theory: what do we know about family privacy regulation? Journal of Family Theory & Review 2(3) September 2010:175–196
54. Poikola A, Kuikkaniemi K, Honko H (2015). MyData - a nordic model for human-centered personal data management and processing. http://urn.fi/URN:ISBN:978-952-243-455-5. Accessed 1 August 2019
55. Pollner M (1987) Mundane reason: reality in everyday and sociological discourse. Cambridge University Press, Cambridge
56. Postscapes (2019) IoT devices and products. https://www.postscapes.com/internet-of-things-award/winners. Accessed 6 December 2019
57. Radaelli L, Sapiezynski P, Houssiau P, Shmueli E, de Montjoye Y(2018). Quantifying surveillance in the networked age: node-based intrusions and group privacy. arXiv, March 2018. https://arxiv.org/abs/1803.09007. Accessed 6 May 2020
58. Rodden T, Benford S (2003). The evolution of buildings and implications for the design of ubiquitous domestic environments. In CHI '03. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Fort Lauderdale, Florida, 5-10 April 2003. New York: ACM Press, pp. 9-16
59. Sailaja N, Colley J, Crabtree A, Gradinar A, Coulton P, Forrester I, Kerlin L, Stenton P (2019) The living room of the future. In TVX '19. Proceedings of the ACM International Conference on Interactive Experiences for Television and Online Video, Salford, England, 5-7 June, 2019. New York: ACM Press, pp. 95-107
60. Sacks, H. (1984) "Notes on methodology", Structures of social action: studies in conversation analysis (eds. Maxwell, J.M. and Heritage, J.), pp. 21-27, Cambridge University Press
61. Sacks H (1992). The baby cried. The mommy picked it up. In G. Jefferson (ed): Lectures on conversation. Oxford: Blackwell, Volume I, Lecture 1, spring 1966, pp. 236-242

62. Schmidt K, Bannon L (1992) Taking CSCW seriously: supporting articulation work. Computer Supported Cooperative Work: An International Journal, vol. 1 (1), March 1992, pp. 7–40
63. Solid (2018). https://solid.mit.edu. Accessed 1 August 2019
64. Squicciarini A, Shehab M, Paci F (2009). Collective privacy management in social networks. In WWW '09. Proceedings of the 18th International Conference on World Wide Web, Madrid, Spain, 20–24 April 2009. New York: ACM Press, pp. 521–530
65. Such J, Rovatsos M (2016). Privacy policy negotiation in social media. ACM Transactions on Autonomous and Adaptive Systems, vol. 11, no. 1, February 2016, article no.4
66. Thomas K, Grier C, Nicol D (2010). unFriendly: multi-party privacy risks in social networks. In PETS 2010. Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Berlin, Germany, 21–23 July 2010. Heidelberg: Springer, pp. 236–252
67. Tolmie P, Crabtree A (2017) The practical politics of sharing personal data. Personal and Ubiquitous Computing, vol. 22 (2), August 2017, pp. 293–315
68. UoN (2019) Integrity and ethics. https://www.nottingham.ac.uk/research/ethics-and-integrity. Accessed 6 December 2019
69. vom Lehn D (2019). from garfinkel's 'experiments in miniature' to the ethnomethodological analysis of interaction. Human Studies, vol. 42, February 2019, pp. 305–326
70. Ward P (2015). Hub of all things (HAT). In J. Richards (ed.) Digital leaders. Swindon, Wiltshire, British Computer Society, pp. 58–59
71. Westin A (1967) Privacy and freedom. Atheneum, New York
72. Wishart R, Corapi D, Marinovic S, Sloman M (2010). Collaborative privacy policy authoring in a social networking context. In POLICY 2010. Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks, Fairfax (VA), USA, 21–23 July 2010. New Jersey: IEEE, pp. 1–8
73. Wölfel C, Merritt T (2013) Method card design dimensions: a survey of card-based design tools. In P. Kotze, G. Marsden, G. Lindgaard, J. Wesson and M. Winckler (eds.): INTERACT 2013. Proceedings of the 14th IFIP TC 13 International Conference on Human-Computer Interaction, Cape Town, South Africa, 2–6 September, 2013. Heidelberg: Springer-Verlag pp.479–486
74. Xu K, Guo Y, Guo L, Fang Y, Li X (2017). My privacy my decision: control of photo sharing on online social networks. IEEE Transactions on Dependable and Secure Computing, vol. 14, issue 2 March 2017, pp. 199–210
75. Yousefi H, Su H, Imani S, Alkhaldi K, Filipe C, Didar T (2019) Intelligent food packaging: a review of smart sensing technologies for monitoring food quality. ACS Sensors 4(4):808–821
76. Zhong H, Squicciarini A, Miller D (2018). Toward automated multiparty privacy conflict detection. In CIKM '18. Proceedings of the 27th International conference on Information and Knowledge Management, Torino, Italy, 22–26 October 2018. New York: ACM Press, pp. 1811-1814
77. Zimmerman D (1970). The practicalities of rule use. Pp.221-238. in Douglas, J.D. (ed.): Understanding everyday life: toward the reconstruction of sociological knowledge. Chicago: Aldine Publishing Company, 221–238

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.