[Published in New Media & Society, Online First version available at http://journals.sagepub.com/doi/full/10.1177/1461444817700154**]**

Living with Interpersonal Data: Observability and Accountability in the Age of Pervasive ICT

Goulden, M.; Tolmie, P; Mortier, R; Lodge, T.; Pietilainen, A-K.; Teixeira, R.

Abstract

The Internet of Things, alongside existing mobile digital technologies, herald a world in which pervasive sensing constantly captures data about us. Simultaneous with this technology programme are moves by policymakers to shore up the digital economy, through the legislating of new models of data management. These moves seek to give individuals control and oversight of their personal data. Within shared settings the consequences of these changes are the large-scale generation of *interpersonal data*, generated by and acting on the group rather than individual. We consider how such systems create new forms of observability and hence accountability amongst members of the home, and draw on the work of Simmel (1906) and Goffman (1971) to explore how these demands are managed. Such management mitigates the more extreme possibilities for domestic monitoring posited by these systems, yet without careful design there remains a considerable danger of unanticipated negative consequences.

Introduction

The *observability* of members' actions within the home changes over time as the practices they enact change. One catalyst is new technological and material affordances. As observability changes, so do the ways in which observability is *managed*. Two generations ago, a child in a western society might commonly evade observation by parents by escaping the home to play with friends outside. One generation ago, changes to technology contributed to new opportunities to escape observation behind closed bedroom doors. These changes included increasingly personalised entertainment devices, and supportive changes to the material fabric of the home, such as the transition to central heating extending thermal comfort beyond the sitting room. In changing the availability and possibilities of domestic space, technological and material developments have played an important role in *when* and *how* the activities of others in the setting can be seen.

In this article we argue that two interlinked developments are generating new forms of observability to fellow members of settings, in the form of what we term *interpersonal data*, in which the 'data subject' is the group. The first of these developments is that of pervasively-sensed environments – specifically in the form of ever-more sophisticated mobile ICTs and the Internet of Things (IoT). Digital technologies are no longer imprisoned within discrete devices, but increasingly embedded within everything that surrounds us, as an unseen forest of networked sensors, processors and actuators. The promise is of a world in which new service offerings become possible while existing services execute more efficiently. Within the home this project is packaged up as the 'smart home', and this forms the backdrop to our work.

The second development concerns emerging models of data management. By rendering ever broader swathes of the material world amenable to remote monitoring and (automated) control, the practices enmeshed in these objects become themselves open to reimagining and redirecting. In the IoT vision, what makes this omnipotence feasible is the algorithm, which will orchestrate the great majority of the work of processing the data flowing into the network. The logic of this project – directing information, and so agency, from the outer edges of the network towards the core – is one of centralisation. The algorithms may run locally, but the agency invested in them originates elsewhere, in the efforts of the software engineers who designed them. Certainly this is the case with today's initial endeavours, where companies like Google and Facebook hoover up the data their technologies detect of our activities, and leave us with little or no sense of what was taken, to what end.

This logic sits uncomfortably with the ethos of decentralised, non-hierarchical networks of agents which is often attached to digital culture (Gere, 2008). Legislators are seeking to ameliorate this tension between centre and edge, not least because of the fear that it could lead to the widespread public rejection of smart projects, and the digital economy predicated upon them (Crabtree et al., 2016). Key to these efforts is ensuring that some form of local oversight is enacted, "*to put users in control of their own data*" (European Commission, 2012, pp. 1–2). It is envisaged that this oversight will take the form of tools which grant users access to their data. Third party service providers will only be able to run operations on this data with the express permission of the user:

> *To enforce transparency and user control, device manufacturers should provide tools to locally read, edit and modify the data before they are transferred to any data controller [...] Device manufacturers should enable local controlling and processing entities allowing users to have a clear picture of data collected by their devices and facilitating local storage and processing without having to transmit the data to the device manufacturer.* (Article 29 Data Protection Working Party, 2014, p. 22)

An important aspect of this new data management model is that, for the first time, users will be encouraged, and enabled, to engage with the data captured from their activities. For self-ownership to be meaningful, some understanding of what is owned is required. There is also a second promise offered by this engagement, and that is for users to provide additional contextual information to the algorithms running smart home services. The occasional visits of an elderly relative might necessitate higher temperatures within the house for the period. Without the input of local expertise it is highly questionable whether automation can identify and respond appropriately to such mundane occurrences (*Redacted*, 2016).

The pervasive sensing offered by smart and mobile ICTs, in combination with the new data management models which seek to bolster their adoption, create the conditions for the large-scale creation of interpersonal data. We classify interpersonal data as that which is *generated by and observable to* the members of a group or setting. This observability may be direct through visualisation of the data, or indirect through experience of a service which is operating on that data. A prosaic example would be the browser history on a laptop or tablet shared amongst members of the family. A more novel illustration is that of the *Tado* smart thermometer, which continually tracks the

location of members of the house using the GPS on their smartphones, activating the heating only when they approach the home. In this latter example, the data begins as personal data on one member's phone, but becomes interpersonal data in its co-option by smart home technology. As these examples suggest, the observability of this data may, indeed often will, be highly mundane. At other times, as we discuss below, it can be potentially highly volatile.

By its very nature, interpersonal data creates new forms of observability between members. This observation in turn prompts new demands for accountability as the previously unseen is surfaced. Via a study of such accounting, we consider how these new forms of observability are managed by members of domestic settings, and so what the implications of these developments might be. The work reported here draws primarily on one study within an EU-funded research project to create a data management tool, or *Personal Information Hub*, of the kind advocated by legislators. The study involved the collection of data from participants' digital devices, followed by exercises in which their data was made visible to both themselves and others (family members and/or the researcher). Our interest was in how people managed this exposure through their accounts. Material from a parallel study (reported in *Redacted*, 2016), in which data from sensors placed throughout the home was collected and presented back to three families, is also drawn upon.

Privacy, Surveillance and Accountability in the Home

Privacy-focused treatments of digital data have to date focused overwhelmingly on issues of *personal* data – particularly on the meeting points between individual and outside parties (e.g. Norberg et al., 2007; Wessels, 2012), and indeed it is such a frame that can be seen in the problem and prescription described by policy makers above. By contrast, our interest lies in understanding the implications of access to such data within intimate relationships (boyd, 2014; Mäkinen, 2016). In this context it is necessary to recognise our setting as a smart *home*, rather than *house* (Richardson, 2009), in which technologies and data can only be understood as enmeshed in the practices and moral orders of a dynamic setting (Hargreaves et al., 2013; Shove, 2003), where membership, roles, relations, and routines are both durable and regularly reconfigured. Key dimensions of this space include generational (e.g. McLean, 2011) and gender roles (e.g. Oudshoorn et al., 2004).

In this space our focus falls on the ways in which observability, and in turn accountability, are shifted by the technologies sketched above. What we will show is that technologies of accountability do not necessarily create new transparency, but do generate new accounting practices to meet the demands raised by these technologies (Neyland, 2007). In understanding this process we draw on the work of both Simmel and Goffman.

On Preserves and Discretion

In our analysis we draw on Goffman's treatment of "territories of the self" (1971) and Simmel's (1906) study of secrecy, and particularly the role of *discretion*. Goffman identifies ownership claims over *preserves* as a key feature of the organisation of social life. Of particular interest here is the "*information preserve*", being "*[t]he set of facts about himself to which an individual expects to control access while in the presence of others*" (p.38-39). Presence need not be understood as necessarily entailing face-to-face

interaction – indeed the sociotechnical systems considered here can be understood as an extension of presence beyond the immediate moment. The maintenance, transgression, and negotiation of these claims is socially organised, which is to say takes place within moral orders – sets of rules shared by members of a group concerning right and wrong conduct. The application of these rules is dependant however on socially determined variability: as suggested above in the discussion of homes, the strength of claims, and the extent of preserves, is patterned by the hierarchies of the setting (p.64). From the individual's perspective, what matters is '*not whether a preserve is exclusively maintained, or shared, or given up entirely, but rather the role the individual is allowed in determining what happens to his claim*' (p.60). We can see then that preserves should be understood not as absolutes, but rather as resources to be managed and contested within situated interactions.

Within the home, preserves are often shared, particularly between partners. To share a preserve is to remove a barrier that would otherwise stand between individuals, and this gives both symbolism and substance to relationships. This sharing is not limitless however, and here we turn to Simmel's (1906) interest in *discretion* as a means by which claims over informational preserves can be respected by other members of the setting.

> *This attitude consists by no means merely in respect for the secret of the other - that is, for his direct volition to conceal from us this or that. It consists rather in restraining ourselves from acquaintance with all of those facts in the conditions of another which he does not positively reveal.* (p.452)

In Simmel's work, this concept is limited in its application, only deployed with reference to a particular form of relationship – that between '*acquaintances'* (*ibid.*), being pairs at some distance from one another. In our own analysis, discretion appears far more universal. To use one example relevant to our study, discretion is in operation when a husband or wife elects not to peruse their partner's emails, despite having the ability to do so by way of the saved account login on the family computer. Of course this is not to claim that all intimate relationships operate in this manner, rather that all such relationships which allow for trust do so. Nevertheless, there are moments when discretion must '*yield to the demands of practical necessity*' (p.455), and one feels – with reference to the local moral order – justified in crossing these boundaries. In the previous example, this moment might come following doubts about the partner's fidelity. In other intimate relationships, particularly ones marked by a gross imbalance of power such as between a parent and a (younger) child, the caveats of practical necessity may be formalised. boyd (2014) describes such a situation in her account of teenagers' use of social media, where a 15-year-old boy called Christopher shares all his passwords with his parents, on the understanding that this access will only be invoked in emergencies which necessitate it (p.73). What constitutes an emergency goes unarticulated, but we might confidently assume it consists of fears that an egregious transgression of the local moral order is underway (which might be realised as fears for the child's safety).

The reason for Simmel's limited application of discretion to simply acquaintances can perhaps be understood by reference to his treatment of observability. He writes:

> *In general, men credit themselves with the right to know everything which, […] through purely psychological observation and reflection, it is possible to ascertain.*

> *In point of fact, however, indiscretion exercised in this way may be quite as violent, and morally quite as unjustifiable, as listening at keyholes and prying into the letters of strangers.* (p.455-456)

The knowledge which may be gained from one's own senses, and reflection upon them, grows exponentially with proximity. Whilst an acquaintance might yield little from such methods which is not revealed *voluntarily*, with intimacy arises the sharing of preserves. As such, what is left for discretion to manage might be considered relatively little. Yet what remains – that which can only be reached through keyholes and letters – carries even greater significance, because it is upon this discretion that trust and respect are based. It is the observability of what remains which is brought into play by the technologies considered in this article. Much of what becomes observable is mundane, unworthy of comment. Some, inevitably, raises questions, particularly so where activity is suggested which appears in breach of the local moral order, and it is those cases we focus upon here.

Methods

This article draws on two parallel studies carried out in the UK in 2014-15.

Analysis: The studies drew on an ethnomethodologically-informed approach in which, through "*articulation work*" (Schmidt & Bannon, 1992), members of a setting render their actions accountable to others in a manner which makes possible the cooperative behaviour required for a home to function. The accountability practices we identify are grossly observable methodological ways of handling the exposure of personal information. They were seen repeatedly throughout our studies and are presented through the specific cases provided in order to make manifest how they are articulated in naturally occurring interaction. The examples provide concrete evidence of a "*machinery of interaction*" (Sacks, 1984) in play which is generalizable to the wider population: "*While locally enacted by them it is not theirs alone but belongs to the culture that they are members of. It is a resource that the culture provides for [everybody wanting to accomplish that kind of activity]*" (Crabtree et al., 2013). In other words "*generalisation works within everyday life and is 'built into' ordinary activities*" (Sharrock & Randall, 2004).

The purpose of the studies as designed was to situate people in such a way that their data was made visible to other parties (including the researcher but primarily to other members of their cohort). At the outset our interest was in how the intelligibility of the data was established through participants' accounts, and the resources they drew on. This work is presented in (*Redacted*, 2016).

During the thematic analysis, carried out using Nvivo, it became clear that in accounting for their data, participants were constantly working the boundaries of their own and their fellow member's information preserves. This led us to develop the notion of interpersonal data with which we frame this article. One consequence of this framing emerging only during the analysis is that we do not capture all aspects of observability. Our data shows how members manage the exposure of data, but little on the work of preventing exposure in the first place.

Study 1: Sixteen participants were recruited, consisting of four individuals (not used in this paper), one mother and teenage son, four couples with children living at home, and one retired couple whose children had left home. Participants were recruited through a recruitment website, and from participation in previous studies. Browsing and location data were collected from their devices (mobile phone, tablet, laptop and/or desktop) over a period of eight weeks, using a combination of internally-developed software and the Moves app detailed below. All the devices monitored were used on a daily basis. Two interviews, focused on those in the house and their activities, and the role of digital technologies in their day-to-day lives, were conducted at the start of the study. At the completion of monitoring, households were given a guided exercise in which the members were collectively presented with a series of visualisations of the data collected from their devices, and tasked with making sense of them.

Study 2: In this previously reported study (*Redacted*, 2016) three families, comprising of a semi-retired couple; a couple with an adult daughter living at home; and a couple with two children aged 10 and 7, were recruited. These families were recruited from amongst members of the broader research project (see Ethics section below). It is important to note that none of these members were involved in the study itself, or indeed from the same institution. They were effectively strangers to the researchers. We add that the research was primarily concerned with the methodological ways in which participants managed this data in interactions with other household members rather than with the researcher. The study used a similar approach to Study 1, with the distinction that the data collected was from sensors placed around the home, capturing temperature, humidity, light levels and motion, and electricity consumption for the property.

Ethics: The sensitivities around some of the data that was captured clearly carried the potential to cause distress for participants. Both studies went through lengthy ethics review prior to approval. The design of the studies addressed these concerns in a number of ways. Firstly, the sharing of *sensitive* data was never the goal of the studies, and considerable efforts were made to avoid it. In both studies, participants were given explicit prior warning of the kinds of data to be captured and made visible to members of the setting. It was assumed that, forewarned, participants would take steps to prevent the capture of anything they wished to hide. To this end, participants of both studies were shown how to disable data capture, and how they could delete data already captured. Purposefully, the research team were not informed of such actions. As avoidance was more difficult in Study 2, given the more distributed data capture, the participants were drawn from within the research team. Finally, specific steps were taken to gather informed consent from all participants, including the creation of a simplified information sheet for children in the families which took part. Based on our interaction with participants we are confident that no distress was caused in these studies.

Observability in the smart home

In the following analysis we consider firstly how existing regimes of observability in the home are structured around both the technologies used and the local moral order. These regimes are challenged in a world of pervasive ICT in which activity traces are captured both by sensors embedded within the home's fabric, and by mobile devices travelling with the member outside it

In this world new data management models mean that such data is easily accessible to members of the setting, and tools are provided to render it legible to them, creating new accountability demands. We shall see how these new forms of observability are managed through the accounting work of those implicated. We highlight the important role of ambiguity, in the relationship between what is digitally sensed and what is personally experienced; in the inner workings of these systems; and in the authorship of the activity observed. The nature of our study of such a world – whereby we task participants with looking through the data captured from their setting – has the effect that discretion is sidestepped as a means of managing observability: the decision of whether or not to look is taken from participants. We shall see though how discretion begins to reassert itself as sensor-derived observability starts to be incorporated into the home's moral order.

Observability and discretion

A notable affordance of contemporary mobile devices is the ability to be unobservable in plain sight. By angling the screen away from those co-present, the focus of one's attention can be hidden. That one is interacting with an electronic device is readily observable, and in certain situations (for example at the family dinner table) this alone may constitute a breach of the moral order. In many more situations however, whilst the activity of *using* the device is acceptable, the *use of* the device may determine otherwise. Aside from the orientation of the device (landscape might suggest watching or playing, portrait reading) and the form of any physical interaction with it, an observer is given little information from the back of the device's housing. The difficulty of observing activity was seen in an interview with parents of two teenagers, a 14-year-old daughter and a 19-year-old son:

James She'll [daughter] go off to bed and you'll go up there and she's probably still watching the same stuff on her tablet.
Anne Yes, but I think she reads on that so sometimes I go in and, sort of, say, stop screening it, but she's reading. You know, she's reading on her-
James -I think she does a quick flick.

James He [son] never did anything that, kind of, aroused, you know, you never walked in on him with something that shouldn't… Whereas other parents, sort of, report this stuff, so he's either very discreet or...

As a parent, James considers encroachment into his children's information preserves justified, if not obligatory given his role as guardian. What is notable here is that in both situations James carries some level of suspicion that his children are breaching the moral order. He suspects his daughter, having been sent to bed, is continuing to watch on her tablet the same programmes she was watching downstairs, but is quickly switching between apps (another observability-avoiding affordance) to dodge detection. Not least due to the experiences of other parents, he recognises that his son may be accessing pornographic material on his devices. In both examples however, the absence of direct observation negates a demand for accountability. Without the "demands of practical necessity" taking precedence with evidence of a clear breach, the "beauty of discretion" (Simmel 1906:455) holds sway. No prerogative is handed to, or obligation placed upon, James to encroach on his children's preserves.

Observability breaching the moral order

The data captured in our studies was understood by participants, first and foremost, as being a record of their or their family's activity (*Redacted*, 2016). Only when this interpretation became problematic were alternative accounts sought. It is the reading of machine activity[1] as *indexical* to human experience which allows for the observation of fellow members of the setting. We use 'indexical' here in the ethnomethodological sense that, whilst the machine activity is understood as mapping to human experience, the specific interpretation of it is tied to the local setting. In the following excerpt we see an exchange between a wife and husband, Carol and Rob, as they look through the browsing logs of a family's laptop, which is shared between themselves and their 10-year-old son, Sam. Carol and Rob's attention lands on the URL of a gambling website run by the betting company *William Hill.*

Rob Now *that* [URLs of gambling website], they are adverts
Carol Right
Rob they're popup adverts when Sam's on something on YouTube or his Roblox or something like that.
Carol Right.
Rob Because they get popups all over the place.
Carol Yes.
Rob So I didn't know… I don't go on William Hill on the laptop
Carol No
Rob I go on my phone. I've got an app
I Yes
Rob I wouldn't go on *any* of those
Carol No, no.
Rob because I've got the app and all I do is my pound accumulator. *They* are popups.

The first thing to note here is that, read as human activity, the logs appear to be rendering observable actions which would otherwise have remained hidden. In this particular case these actions carry potentially serious ramifications. To be engaged in a circumscribed activity, which gambling is in this setting, without the consent of other (adult) members would constitute a breach of the moral order. In the exchange we not only see Rob's attempt to disown the activity in order to absolve himself, but in the supportive interjections offered by both Carol and then by the interviewer, we also see a collective defence of the moral order itself, which is only sustained for as long as members sustain it.

For our analysis, it is notable that there is no "marker" (Goffman 1971:65) attached by the system to this interpersonal data which might identify the agent responsible. As the family's shared laptop, it might be any of the setting's members, and yet in initiating an account, Rob effectively lays down a marker only to then disown it. In doing so he is self-violating (*ibid.*p77) his own information preserve, but only as a defence against the expected encroachment of others. Rob is obligated to do so by the locally-shared knowledge that he does indeed gamble, though only in a ritualised, responsible manner, placing a £1 "accumulator" bet every Saturday morning through the *William Hill* app on his phone. It is this knowledge, held by participants rather than logging systems, which marks the activity as his. This same knowledge exonerates him in the account which follows, which establishes that what is recorded cannot be human

activity, because that takes place on a different device. Recognising Rob's gambling ritual as described, his wife accepted his account as correct. Whilst the data triggers the account, it is the shared information preserve of the couple that both implicates him, and through the trust it engenders, exonerates him.

Managing the breach

In establishing that this activity could not be his, Rob presents an alternative explanation in the form of advertising. In doing so he appears to suspend the reading of human activity into the data, only to then reassert it by claiming that underlying this advertising is Sam's use of certain websites. The exchange above continues:

Rob Yes, so you can see there [gestures to other URLs requested on the device] they're adverts.
I "Traffic manager", yes.
Rob Yes, so they'll be popup adverts. So that's something for us to keep an eye on when Sam is on there.
Carol Hmmmm.
Rob Because yes- so that's interesting.
Carol That's interesting.
Rob That is *really interesting* so… yes, maybe something we… keep an eye on.
I Do you have any Ad Block software or anything like that?
Rob We do… Um, I'm going to have to go through his settings on his account
Carol Yes
Rob and just double check everything - what everything is.
I Yes.
Rob They shouldn't be coming up, so…
I Yes.

Here we see a potential breach of the moral order, prompted by interpersonal data, turned into a reassertion of it through the accounting work of members. What began as a need for Rob to stymie any possible reading of deviance into his behaviour is developed into a *coordinated* demonstration of responsible parenting, by both parents expressing a concern for what their son is exposed to whilst online, and the knowledge of appropriate tools to address the issue. In the context of Sam's safety, and given his age, any concerns about discretion are waived by his parents. The mirrored repetition of "interesting" establishes this as a shared account. The interviewer supports the parents to develop the account further by posing a question which invites them to demonstrate their proficiency at protecting their child online. This switch from breaching to buttressing is made possible by the ambiguous relationship between the data logs and participants' actions. This ambiguity is a resource for those, like Rob, who have the status within the setting to make use of it. This status allows him to encroach on his son's information preserve in a manner which sustains the members' reading of the data as records of human activity. He does so by adopting the role of agent of Sam's authorship, but in such a way that what appeared transgressive is rendered innocent, any moral infractions passed on to the advertising pop ups.

Having provided the observability which triggers the account above, it is notable that the role of the logged data is henceforth limited to referencing the presence of some URLs which are taken to relate to advertising. Again it is local knowledge, in the form of Rob's own observation that the websites used by Sam generate popup adverts, which

provides the basis for the alternative account, and situates it within the setting's moral order.

Sources of ambiguity

The 'black box' nature of these technical systems – complex, opaque and often dependant on proprietary algorithms whose precise workings are commercial secrets, offers a rich seam of uncertainty for accounts to mine. In the following example Rob and Carol discuss location data from the GPS sensor on Rob's phone, captured in the study by an app called Moves.

Moves describes itself as an "*activity diary of your life*". It is a seemingly simple piece of software which generates a record of *locations* the user has *occupied*, as distinct from a more common *route* along which the user has *travelled*, as one might experience using a satnav or Google Maps. The user is presented with a kind of timeline, showing the duration spent at points visited during the day. The precise manner in which the app distinguishes between a *destination* on the one hand, and merely a *pause* at a traffic light or whilst tying a shoelace, is unknown to anyone except the software engineers behind its algorithms. When combined with fallible GPS signals, and other limitations such as device battery life, what does become clear when using the app is the presence of "*seams*" (Chalmers & Maccoll, 2003) in the system – points of breakdown which have the effect of leaving behind them curios in the data. One participant was recorded as spending 30 minutes in the exercise yard of a medium-security prison not far from his house. On another occasion the same participant – a 36-year old male – was recorded as staying overnight in a retirement home nearby. Unsurprisingly, he could not recall either event.

In the case of Rob's timeline (the app on Carol's phone only collected a week of data before ceasing to work), amongst the location data provided by Moves two particular claims prompted extended discussion between the couple. One suggested Rob had spent an evening at a conference centre, the other an entire work day at a hotel – the Mercure – in the centre of town. Below, Carol and Rob together discuss possible explanations for these records (in this particular task no interviewer was present but audio was captured). The exchange begins with Carol questioning the reliability of the technical system producing them.

Carol So some is accurate and some… is
Rob Yeah some is
Carol like random, you know, to you know, 50 metres or something, do you think?
Rob Yeah. I mean, City Conference Centre… 6:56 to 10:04… on the 3rd of December, I just
Carol The only thing that I can think of is that you were at a gig at The Cockpit.
Rob Mmm.
Carol And… because that is up from there, isn't it?
Rob Yeah
Carol Do you know where I mean City Conference Centre?
Rob Yeah. Yeah I do.
Carol It's just up over the metro tracks isn't it?
Rob Yeah.
Carol 'Cause that would tie in, you know, getting there, doors open at five to seven or whatever.

Rob Yeah. And why I'm at the Mercure, I've no idea 'cause I've been at work.
Carol So maybe… you went passed it and…
Rob And then it dropped out there
Carol and it dropped out.

Rob I can only presume that… the Mercure is, ummm, I've possibly gone past it on my way to work… it's dropped out, and that's where it is or that's where it's last had me, because that would have been a way to work if I would have caught the bus in that day, ermmm
Carol Which you would have done because you didn't cycle in December.
Rob Which I would have done 'cause I didn't cycle in. Ummm, so that's what that is.

If not exactly breaking with the practice of reading of the data as human activity, Carol's choice to question the accuracy of the app's positioning certainly acts to qualify it. She suggests it is still showing human activity, just not precisely the activity it thinks. Rob quickly moves from non-committal ("Mmm") to active participant in this alternative account. To explain the claim about the hotel the account is extended further: Rob passed by the Mercure and "it" "dropped out". This is a quite different argument to Carol's questioning of accuracy, and is worth unpacking further. "It" can be taken to be the internal workings of the app, and "dropped out" to the loss of (GPS) signal, but neither party feels the account needs to explicate this, despite it not directly addressing how the app came to claim that Rob's entire day was spent at a hotel. However, Rob does return to this point two minutes later whilst summarising their account, and offers a slightly more developed articulation – "that's where it's last had me" – which suggests a reading into the black box of an algorithm that treats an absence of signal as evidence that the user remains at the last recorded location, and continues to allocate presence to that position until the GPS signal is seen elsewhere.

Despite little being rendered explicit in the exchange, what appears an instinctive account relies on sophisticated reasoning about the black box's workings. Both parties accept it as credible enough to proceed with, but what secures the account is not reasoning – explicit or implicit – about the inner workings of the technology but rather the deployment of *social understanding* of the organisation of daily life in order to generate a *common-sense* explanation (*Redacted* 2016). The conference centre claim is unravelled by reference to both the time of day, which does not match their understanding of when a conference centre would likely be visited, and the location's proximity to a music venue which *does* provide a destination for activity at such a time. The explanation for the hotel reading, aside from the original doubts about the claimed time spent there during a work day, is bolstered by reference to the likely mode of Rob's commute at that particular time of year. Carol and Rob draw on a shared stock of knowledge regarding the socially organised relationships between times, places, and transitions which is unavailable to the app. That they have no view inside the black box of the system is no impediment to them developing an account based on their reasoning, indeed this void provides a source of ambiguity for accounts to harness according to situated needs.

Before we continue, for our wider interest in the implications of these data management practices around interpersonal data, its perhaps worth noting how situated the sensitivity of such highly granular data is. The gambling claim above in particular seems problematic for Rob, given his existing Saturday ritual of a £1 bet. By contrast,

the discussion concerning the Mercure hotel gives no sense of any concerns on the part of Carol, and yet Moves' claim that Rob spent an entire work day in a hotel could, in particular contexts where, for example, someone has fears about a partner's fidelity, be deeply contentious. In such a situation the partner might draw on a different body of locally-held knowledge, to reach the conclusion that the app claims were accurate. From these examples we see that there is little prospect of developing systems which might identify 'sensitive' data and treat their observability differently from other 'mundane' data. Once this technical data becomes visible to members it becomes amenable to situated social reasoning the parameters of which no technical system can hope to grasp.

Ambiguity extends to ownership

The use of Sam in Rob's account above as the author of a troublesome URL points us towards another element of accounting for digital traces within the home. Without an unambiguous link between *person* and *personal* data, the authorship of any one piece of data – where it is accepted as being human-generated – becomes contestable. The resolution of doubt is filtered through existing family dynamics. In the final exchange we take from this family, Rob is looking at a group of URLs that have been categorised by the data visualisation tool as 'Miscellaneous Gaming'. He again identifies them as being the result of Sam's activities. This time he invites Sam to corroborate the account.

Rob These are all "Miscellaneous Gaming".
Carol Right.
Rob So they are all things that Sam – Sam, come here a minute.
Sam Yeah coming.
Rob What's the two gaming websites you use?
Sam Roblox and Kongre…yeah, I mean, Kongregate.
Rob And then these are all links
Sam Yeah
Rob within those websites?
Sam Ermmm
Rob Yeah.
Carol So is Roblox like a homepage where you can then click on
Sam No. Roblox is like Minecraft mixed with Goat Simulator.
Carol Right.
Rob And Kongregate is where you can click on a game and it will open up in another window, is that correct?
Sam Yeah.
Carol Right okay, yep.
Rob Okay. Thank you. So they are all from Kongregate all games that Sam would have tried out at some point, and it takes up most usage of the laptop [laughs]. It's the same with the football. That would all be down to Sam because they're not football sites that I would go on to.

When asked to confirm his father's account, Sam offers only a non-committal response, before confirmation is given for him. Sam's mother proceeds to develop the account further, inviting his involvement but without offering him an opportunity to return to the central claim that his activity is the actual source of what is recorded in the logs. His limited status in the exchange, and thus scope for equal participation, is reflected in his status in the turn-taking as a specifically selected (rather than self-

selecting) participant, restricted to answering his parents' questions which are constructed to seek confirmation of select features of the account they are generating. The account ends with a formulation by Rob that extends Sam's culpability even further, to include the websites categorised as 'Football' by the visualisation. Sam is not even asked to confirm this claim, despite still being present. As in previous examples, here we see the accepted reading of the data is deeply situated in local relationships and knowledge, with the machine-based record serving almost entirely as a resource for the construction of a locally coherent account.

Discretion and the management of observability

New demands of accountability are not only generated by the new scope for observation, but also for those who, wittingly or otherwise, may become potential observers. They are equally accountable to the setting's moral orders, and in utilising new technological capacities to observe that which is not within plain sight, they come into contact with existing notions of the boundaries of personal preserves. In the following exchange, Susan and Frank look at the sensor data from their home from which inferences can be made about when rooms have been occupied.

Susan So, I'm aware that there's evidence that Sally's [daughter] gone for a wee. She's spent most of her life trying to define her space, and David [son] is defining his space. So now there's evidence – now I can see into these spaces - so there's a sense of invasion. I can now look and find out who went for a wee when and where they went.

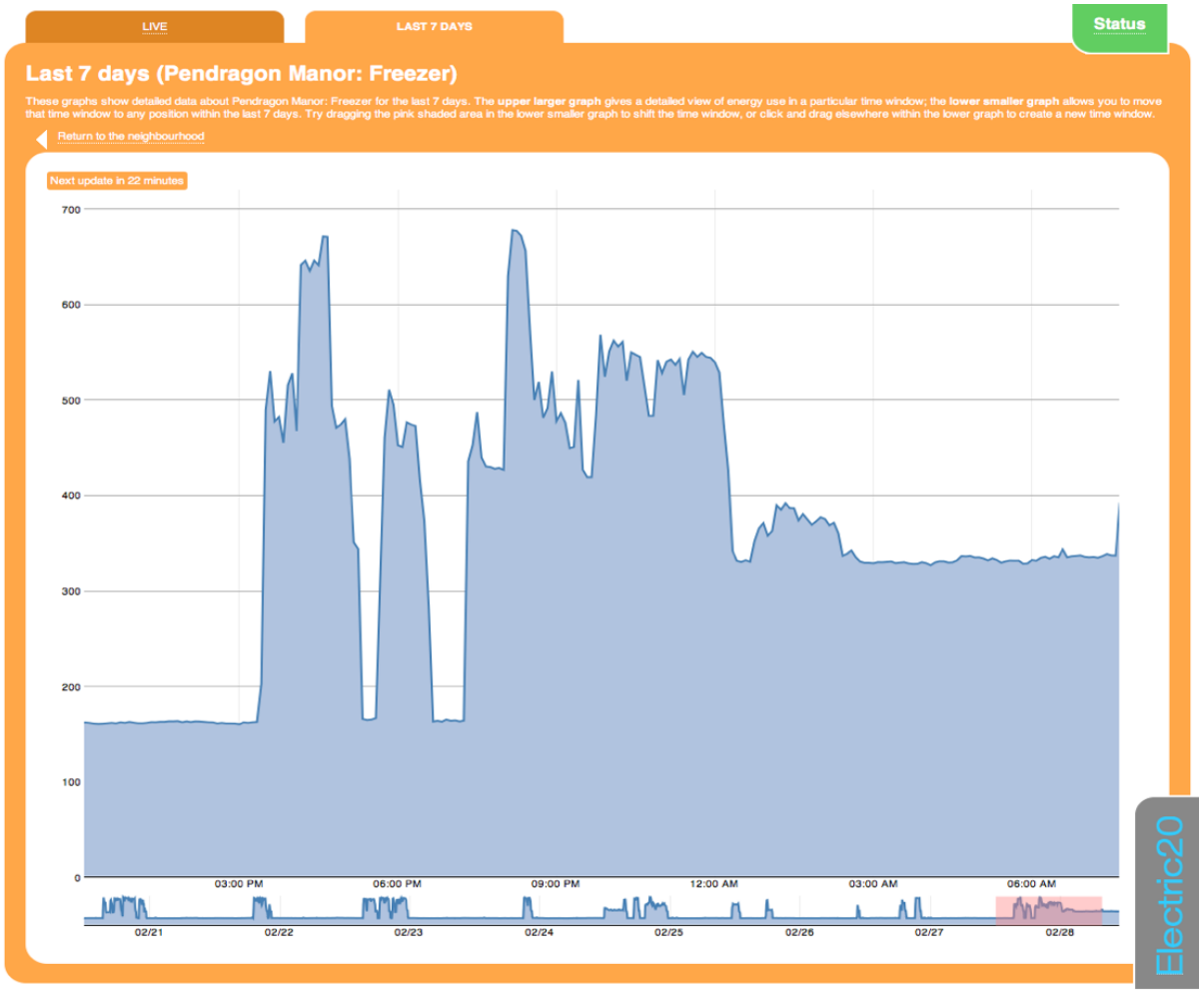
Frank You know when Sally's been there because she always puts the toilet roll on the floor.

Susan's discomfort here stems from the distinction between what *can* be seen and what *should* be seen. These technologies radically extend what can be seen, and so the role of discretion becomes correspondingly greater, in order to manage this distinction.

Here, it is in the specificity of this particular form of observability that the tension between *can* and *should* emerges – the response of Frank suggests that the capacity to remotely (temporally if not spatially) detect Sally's use of this space has actually always been possible, or at least as long as she has left the toilet roll as she does. In leaving behind a trace of her presence Sally can be read as complicit in this form of observability. Should she care about being unseen she has the option of leaving the bathroom exactly as she found it: "*what is not concealed may be known, and what is not revealed may yet not be known*" (Simmel 1906:453). The use of embedded sensing to derive the same information offers no such agency to the observed, short of vandalising the sensor itself. Without this choice, moral expectations fall on the observer alone to determine what it is that should be seen. It is this that separates Susan's observing from that of Christopher's parents in boyd's (2014) example. For Christopher, the teen whose social media passwords are entrusted to his parents, the performing of observation is undetectable, just as it is for Susan's children. The status of the (potential) observer is different in the two cases however. Christopher's parents are not invading his information preserve, because their ability to observe has been reached by negotiation, not just technological fiat. This negotiation had not had the opportunity to take place in the study involving Susan and her children.

We flagged earlier how the nature of our study removed the choice of discretion from participants, effectively tasking them with exercising no discretion. In Susan's account we see how even within the study's confines she begins to reflect on whether this absence of discretion is appropriate. What we are seeing is the beginning of a process by which the technology of sensing itself is incorporated into the moral order. This is not the fixing of a new set of orderings within the home which redraw the boundaries between individuals' preserves, but rather *initial* challenges to existing orderings. Were such sensing to become a permanent feature of the setting, as it might be in a smart home, some form of shared understanding as to the acceptable use of it within local ordering would emerge over time. In other words, the real question is not how these technologies will determine the moral ordering of pervasively-sensed spaces, but how the two will come to co-produce one another through the performance of day-to-day life within them.

As Frank's comment shows, one dimension of the technology's moral appraisal is the specific form of its observation. Another concerns the account given for the technology's introduction. Our final example is taken from an entirely different study, and is used here to highlight how the legitimation given for the system's presence has implications for its use. The study was concerned with collecting domestic electricity consumption data and using it to motivate participants to reduce their energy use. The study used circuit-level monitoring of the home, allowing different areas of the house to be distinguished from one another, and then made this data available to the participant as a timeline that could be accessed via a webpage. One participant shared the screengrab below with the project team, along with the following account:



Nick The 150W baseload is a PC and Ethernet switch in the computer room. The excursions up to 700W are active Xbox gameplay. And then he forgot to switch it off at 1 A.M., hence the extra 150W all night.

The screengrab shows an overnight period whilst Nick was away from home. The account he gives is of the activities conducted by his son during that time, as derived from this electricity trace. As this was on a school night, this activity was considered to be in breach of acceptable behaviour and his son was later spoken to about it. Nick's account is interesting in that he not only highlights the use of Xbox when his son should be in bed, but also the immorality of *leaving stuff on*. Nick's accountability as observer here is met by reference to the premise that this observation is an accidental affordance of a pro-environmental project, and is in that sense moral. The detection of deviance was accidental. Similarly, the framing of smart homes and new data management models is around many things, none of which are surveilling other occupants of the space. Yet the same kinds of affordance are created by systems of pervasively sensing, processing and collating data. Nick stated he would not dream of installing a system for monitoring his children remotely, yet as a side effect of the electricity sensing he was able to. To maintain the credibility of such an account, the observer would have to avoid being seen to use this affordance for remote policing *purposefully*. But as in Bentham's panopticon, even if the observer limits themselves from doing so, the observed is left with the knowledge that this potential exists. This inevitably has consequences for the dynamics of moral accountability and how individual preserves are delimited within the setting. Whether these consequences are felt as a strengthening of trust through the

enacting of discretion, or as the imposition of inescapable prying, or something else entirely, is unknowable outside of the particular circumstances of specific settings where such technologies are used.

Conclusion

Whilst we cannot know the concrete forms of smart- and mobile-ICT which might emerge in the years to come, it seems highly likely, given current developments, that the domestic collection and processing of sensed data will become ever more pervasive. We have suggested, again looking to current trends, that new models of personal data management will have to emerge with them. To what degree this data becomes referenced in day-to-day lives we also cannot say, but certainly there are good reasons to believe that the digital data generated around our everyday activities will come to be far more available to us than is currently the case.

As the home itself becomes a mediated space this opens up new challenges. Current debates around digital data, ownership and privacy focus on the *personal data* of individuals. In the mediated home, this becomes *interpersonal data*. The traces generated around members' activities become observable to other members. Our article though is not an account of the emergence of a domestic Big Brother, but rather how members' communication practices adapt to mitigate such outcomes. What we do see in the accounts above is the existing local moral order, and its regimes of observability and accountability being breached, and some of the strategies that play out as members orientate to this breach through the reflexive utilisation of their information preserves, and those of others in the setting. Elucidating these processes suggests that the implications of these new socio-technical developments is likely to be less radical than they might at first appear.

Far from reconstituting the setting under a new technologically-mediated omnipresent gaze, it is striking just how subservient this technical data is to human reasoning situated within existing local knowledge, particularly in the form of information preserves shared between members, and the members' hierarchies. For all its apparent precision, the ill-defined relationship between sensed data and human experience renders it highly equivocal. Ambiguity is sourced in the inevitably fallible nature of these technical systems, and the paucity of contextual information such as the identity of the member whose activities are implicated. This ambiguity becomes a resource for asserting the primacy of local knowledge in accounts, and reasserting the moral order.

Perhaps most important of all though, we see how these demands for accountability may be avoided in the first place, by the use of discretion to manage observability. Through these technologies we see a seemingly radical adjustment in what *can* be observed. The importance of what *should* be observed becomes more pressing as a result. The presence of technologies which enable remote monitoring will not, de facto, render remote monitoring acceptable. Indeed, this affordance may ensure – certainly if the design of the technology is clumsy – that such systems go unadopted.

Nevertheless, in the context of interpersonal data, the otherwise laudable goal of giving individuals greater ownership of their data becomes highly problematic. Should such systems be installed, the *potential* for the monitoring of other members, whether

transgressive or legitimate, exists. Some of this data may reveal breaches of the moral order and so carry considerable consequence. Our studies suggest that there is also a very real danger that, depending on local circumstances, data is *read* as revealing a transgression when none took place. The notion of '*nothing to hide, nothing to fear'* is of little value in a world in which *so much* data is being made visible by so many black boxed, imperfect systems.

It is beyond the scope of this article to solve these challenges. What we can say is that the moral ordering of the home is reliant on delicate, only occasionally explicit, negotiation of what is normal, what must be accounted for, and what should be left unseen. These negotiations are embedded in the concreteness of the setting. Pervasive computing cannot 'solve' these negotiations within the technology. Indeed, how could it without somehow understanding and encompassing all of the different moral accountabilities in play in each specific instance of its deployment? Instead, there will be a need to develop tools which allow for ongoing negotiation between members of the space themselves. What should be captured and what should be seen, at what granularity, and by whom – these are decisions which can only be reached with the input of members.

Acknowledgements

The authors wish to thank Professor Bob Anderson and Professor Robert Dingwall for their comments on drafts of this work.

Funding The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: This work was supported by the Horizon Digital Economy grants (EPSRC grants EP/G065802/1 and EP/M02315X/1), and the European Commission's Seventh Framework Programme grant no. 611001 (User-Centric Networking).

Notes

1. As an example of the distinction between human experience and machine activity, consider the URLs captured by the study. Participants approached these as lists of webpages they visited. Actually they were logs of network activity. To the network, the single 'webpage' experienced by a participant might consist of content drawn from a dozen different URLs, with text, video and advertising coming from different sources. As a result, the machine view differs significantly from the human view.

References

boyd, d. (2014) It's Complicated: The Social Lives of Networked Teens. Yale University Press, New Haven.

Crabtree, A., Tolmie, P. & Rouncefield, M. (2013) 'How many bloody examples do you want?' - fieldwork and generalisation, *Proceedings of the 13th European Conference on Computer Supported Cooperative Work*, Paphos, Springer, pp. 1-20.

Goffman, E., 1971. Relations in public: microstudies of the public order. NY: Basic Books.

Hargreaves, T., Nye, M., Burgess, J. (2013) Keeping energy visible? Exploring how householders interact with feedback from smart energy monitors in the longer term. *Energy Policy* 52, 126–134.

Kjeld Schmidt, K, & Bannon, L. (1992) Taking CSCW seriously, *Journal of CSCW*, 1 (1): 7-40.

Mäkinen, L.A. (2016) Surveillance on/off: Examining home surveillance systems from the user's perspective. *Surveillance Society*, 14: 59–77.
McLean, A. (2011) Ethical Frontiers of ICT and Older Users: Cultural, Pragmatic and Ethical Issues. *Ethics and Information Technology,* 13: 313–326.
Neyland, D. (2007) Achieving Transparency: The Visible, Invisible and Divisible in Academic Accountability Networks, *Organization* 14: 499–516.
Norberg, P.A., Horne, D.R., Horne, D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, *Journal of Consumer Affairs* 41: 100–126.
Oudshoorn, N., Rommes, E., Stienstra, M. (2004) Configuring the User as Everybody: Gender and Design Cultures in Information and Communication Technologies. *Science, Technologies & Human Values* 29: 30–63.
Redacted (2016)
Richardson, H.J. (2009) A "smart house" is not a home: The domestication of ICTs. *Information System Frontiers* 11: 599-608.
Sacks, H., (1984) Notes on methodology. In: Maxwell, J.M. & Heritage, J. (eds) *Structures of Social Action: Studies in Conversation Analysis*, Cambridge: Cambridge University Press. pp. 21-27.
Sharrock, W. & Randall, D. (2004) Ethnography, ethnomethodology and the problem of generalisation in design, E*uropean Journal of Information Systems*, vol. 13: 186-194.
Shove, E., (2003) *Comfort, Cleanliness and Convenience: The Social Organization of Normality*. Berg, Milton Keynes.
Simmel, G., (1906) *The Sociology of Secrecy and of Secret Societies*. American Journal of Sociology 11: 441–498.
Wessels, B., (2012) Identification and the practices of identity and privacy in everyday digital communication. *New Media & Society* 14: 1251–1268.