Chapter 3

Accountability in ordinary action

Peter Tolmie[1] and Andy Crabtree[2]

This chapter explores the notion of accountability in ordinary action and how it applies to our understanding of privacy. It reflects findings from a range of ethnographic studies in the home that highlight that privacy is a matter of accountability management. This is organised through common-sense methods that exploit physical resources alongside digital methods of cohort management to control the disclosure of information. The studies also highlight how and why privacy breaches occur and that digital innovation poses particular threats to privacy by rendering ordinarily invisible activities visible and open to account. This development undermines members' competence, autonomy and trust in the digital world.

3.1 Introduction

As we saw in the previous chapter, the legal concept of accountability is essentially concerned with demonstrable compliance with the law. This contrasts with accountability in ordinary action, which refers to the 'observable and reportable' character of human action in everyday life [1]. If you cast an eye around you, it takes no great effort to observe and report what the people around you are *doing*. You may see people out on the street 'walking along the road', 'crossing the road', 'driving cars', 'parking', 'talking on their phone', 'going into a shop', 'coming out of a shop', etc. In an office, you may see people 'reading e-mail', 'writing a document', 'taking a phone call', 'having a meeting', 'processing an order', 'checking the status of an account', 'having a coffee break', etc. In a factory, you may see people 'checking the machine settings', 'stacking the orders', 'loading the van', etc. On a train, you may see people 'reading a newspaper', 'looking at the messages on their phone', 'texting someone', 'looking out the window', 'checking tickets', etc. Wherever we look we find that human action is observable and reportable by and to *members* [2]. This is in contrast to strangers such as, for example, a Western tourist visiting an ethnic hill tribe in Laos or Myanmar who may find that many aspects of everyday

[1]Information Systems and New Media, University of Siegen, Siegen, Germany
[2]School of Computer Science, University of Nottingham, Nottingham, UK

life are opaque, especially if they do not speak the local language. As members, we can often see and hear at-a-glance what those around us are doing and if not, we know that an account can be provided that will render their actions intelligible. Accountability is an unremarkable fact of everyday life and *that* we know and rely on it not only to see, recognise and understand what is going around us but, just as importantly, to coordinate our actions accordingly *is* a taken-for-granted feature of our competence as members of the social settings we inhabit. This includes digital settings. Accountability in ordinary action is, in short, the glue of social life.

Despite the ubiquity and pervasiveness of ordinary, naturally occurring accountability, it has largely been ignored in the digital domain, perhaps because of its utter mundanity [3]. One persistent, if relatively small thread of interest relates to how computing systems might make visible to their users 'what they are doing' as a resource for human–computer interaction. This notion can be traced back to the work of Dourish [4–6], Dourish and Button [7], Belloti [8], and Belloti and Edwards [9] and has resurfaced more recently in the context of AI, where it has been framed within a growing body of work on the 'transparency' of algorithms and algorithmic decision-making [10]. There has been some discussion in the design literature regarding notions of 'personal accountability', especially in relation to matters such as sustainability and energy consumption [11], but the focus here is on persons' adherence to overt moral agendas rather than accountability in ordinary action. There has also been some work regarding what is termed 'accountability theory' [12], which focuses on how people consider themselves to be accountable to others for certain actions and how this can then be fateful for the things they do and the decisions they make, including how they use technology. Recent work examines how the use of digital technologies impacts upon the accountability of people in the workplace [13], though this is more focused on the risks posed by digital technology for rendering workers open to formal account for their work practices to management. Some specific studies examine natural accountability in terms of how routine activities are treated as unremarkable [14–17], and how digitally mediated activities are routinely made accountable to the 'gambits of compliance' [18] implicated in organised conduct [19–22]. And, as we have explicated at some length elsewhere [23, 24], there is some treatment of how accountability is handled as a matter of policy by users in the privacy and data sharing literature. What is absent from all of this is a discussion of how naturally occurring accountability impacts our understanding of privacy and data sharing.

What is typically missed by the design literature is the *indexical* relationship between natural accountability and the *reflexive* production of the social and moral order [1]. What we mean by this is that in speaking and/or performing some action (e.g., taking one's place in a queue, waiting to catch a driver's eye before crossing a busy road, turning the indicator on before making a turn in a car, waving at a friend in airport lobby, etc.) we are not only making what we are doing observable and reportable to others, we are also *at the same time* ordering what we are doing, where the 'we' refers to not only to ourselves but to the others who are party to what is being done. There is, then, a reflexive relationship between natural accountability and the production of social and moral order and one only need try walking to the

front of a queue to witness it in action. It is not that there is naturally accountable action on the one hand and the social and moral order on the other. The two are entwined, they are *locally* and *mutually constitutive* [25], which means that in ignoring natural accountability, in taking it for granted and passing it by due to its utter mundanity, we also ignore the *real-world, real-time social organisation* of naturally accountable phenomenon, analogue and digital alike.

What we want to do here is consider the findings from a range of field studies conducted over a 10-year period and what they reveal about the observable and reportable, naturally accountable organisation of people's digital privacy and data sharing practices in a domestic context. The studies focused on the mundane use of wireless networks in the home and how online activity is constituted as an ordinary part of everyday life [14], how people interact with and account for data generated by connected devices [26] and how they understand and construe of privacy in a massively networked world [23, 24]. The studies were conducted as part of a number of funded projects including the EU project 'User-Centric Networking', the EPSRC-funded projects 'Homework' and the 'Hub of All Things' and the EPSRC Fellowship 'Privacy by Design: Building Accountability into the Internet of Things'. As catalogued in the papers referenced above, participants in the studies came from a wide variety of demographic backgrounds. This gave us an opportunity to explore the naturally accountable organisation of members' mundane interactions with domestic networks, devices and data from different perspectives, with people from different walks of life, living in different circumstances, with different occupations and interests, across rural, urban and suburban environments in both the United Kingdom and France.

Abstractly, various concepts of privacy posit axioms that essentially revolve around the *disclosure* of personal information or 'data'. Often cited definitions thus inform us that privacy is the ability to *control* the disclosure of personal information [27], to create and manage *interpersonal boundaries* [28] and to employ *contextual norms* to regulate the ad hoc flow of personal information between people [29]. Concretely, the studies make it visible that privacy ordinarily and accountably revolves around managing a polymorphous array of mundane activities in which the digital is embedded in the ongoing conduct of manifold human relationships. Within this lively context, the disclosure or sharing of personal data is accountably organised in terms of managing members' access to devices, applications and content through situated practices, procedures or methods that exploit the local ecology, device visibility and recipient design. The studies make it perspicuous that members' concern with privacy is a concern to manage their accountability in the digital world and that manifest in data sharing practices is an evolving *calculus of accountability* employed to manage the potential attack surface the digital creates in everyday life. That the digital poses a threat to privacy and therefore undermines *societal trust* in the digital is broadly acknowledged. Much less well-known and understood is how and why this happens and what kinds of steps beyond demonstrable compliance with the law might need to be taken to remedy the situation.

3.2 The naturally accountable organisation of digital privacy in the home

Managing digital privacy is intimately bound up with the observability and reportability of one's digital activities and how other people might be able to *see* them in the first place. Developers and security analysts alike recommend passwords as the first line of defense to protect oneself from prying eyes. Yet there is a more fundamental naturally accountable organisation to privacy in the real world, as one of our participants, Paul (not his real name), tells us:

> **Paul:**
> I'm not particularly fussed about setting up passwords and things. I mean there's no threat of network hijacking here. We live in the middle of the countryside, miles away from another house, it's just not an issue.

So as Paul makes accountable, one of the simplest and most ubiquitous ways to constrain access and protect privacy is by controlling access to the environments in which our digital activities occur, i.e., controlling access to the places in which digital devices are kept.

Paul's was not the only example of password suspension for devices considered inaccessible that we encountered in our studies. It was commonplace for devices that always stayed in the home, such as desktop PCs, tablets and media servers. The reasoning generally bound up with this is that the people who have rights of access to the network and the devices on it are the people who have rights of access to the environment in which those devices are located. This point was underscored by Christine, a 63-year-old reflexologist who runs her practice from home:

> **Christine**: I'm big on making sure that the whole house isn't open to their view. I'm forever closing doors and shutting things off. I make sure everything is clear that I consider sensitive. When I used to be in that smaller room particularly, I did not want my laptop there open while I was about to start a treatment.
>
> **Fieldworker**: So that window into your digital world you prefer to have closed to clients as well?
>
> **Christine**: Closed off. Absolutely. Absolutely. And obviously I have to make sure that I don't leave information about previous clients lying around for clients to see.
>
> **Fieldworker**: So it's both professional and personal reasons kind of wrapped in together?
>
> **Christine**: Well absolutely because you know, I could be sued if people felt it was a breach of data protection. So I have to be aware of that. I don't have anything lying around that in any way gives any window into anything. I don't keep my purse or my phone in the room with me either.
>
> **Fieldworker**: OK, and with regard to the network, if you had clients backing up, where one was waiting for another one to go, would you give them access to the network?

> **Christine**: No. Absolutely not. No, no. I wouldn't even give them access to the televisionunless Brian's [her husband] in the room watching it!

This vignette elaborates the fairly blanket operation of a situated privacy practice designed to minimise the risk of the incidental sharing of personal information of any kind – analogue or digital – with visitors to the house where the relationship is confined to business. Despite the account being directed towards breaches of data protection, Christine is also closing doors and generally constraining the movements of her clients. It is not just data relating to other clients but also of her own personal life she is keeping from view. What this makes particularly clear, however, is that *physical barriers* such as doors (and curtains, and hedges, etc.) are the principal gateway controlling access to personal information.

Privacy is also managed through device visibility, which is not only controlled through physical barriers but by members proximity to screens. This is observably and reportably the case for participants who wanted to share very specific content where that content was a feature of activities and repositories described as private. Here Evelyn, a 21-year-old student is talking about how she might occasionally share content with others around her on Tumblr:

> **Evelyn**: I don't like anybody seeing what's going on on Tumblr. Occasionally I'll show Susan [her sister] a picture or a gif of a cat. But I don't.
>
> **Fieldworker**: You show it to her?
>
> **Evelyn**: Yeah.
>
> **Fieldworker**: Rather than you let her watch you doing the posting?
>
> **Evelyn**: Yeah. Being on a phone it's a smaller screen so there is less oversight. I tend to keep it quite close to me anyway. So I'm fine with browsing Tumblr when, like, I'm sitting on a chair downstairs and there are people walking about, or when we're about to watch something.

Evelyn can and does manage to keep what she is doing private by relying on the size of the screen. However, the way she *positions* the screen in relation to herself and others is not incidental. Indeed, insofar as screens are positioned not to disclose content then there is a mutual orientation to that content that it is not for general consumption. This of course is common practice, found in all kinds of settings. Dourish *et al.* [30] found, for example, that computer screens are often positioned such that visitors to an office cannot see them, and Klasnja *et al.* [31] found that people try to preserve their privacy when using devices in public places by 'finding a seat against the wall' or 'tilting or dimming the screen'.

Members have a mutually understood right to keep things from view that they routinely trade upon, such that, what might at first sight be viewed as guarded behaviour is nothing of the sort, but rather an everyday method for making manifest the status of particular kinds of personal data as 'not to be shared'. So, as a matter of method, privacy can be and is managed by controlling how one physically enables others in the environment to see one's devices. There are a number of permutations

whereby this can be brought about. It might be that the recipient is in an adjacent position and it is just a matter of locating the thing to be shared and then re-angling the device so that they can see it. It may also be the case that the device is not mobile, in which case sharing may involve calling the recipient over to the device. Locating the data may also be something that is done prior to sharing it or may be done once the recipient is actually co-present. But, however it occurs, privacy and data disclosure are routinely managed through the social positioning of devices and content in interaction.

Now none of this is to say that passwords are not used. It is simply to recognise what we all take for granted: that privacy is principally managed through the methodical use of physical barriers to control members' access to the places where devices are located; and by controlling the access to devices themselves through their social positioning and making content selectively available to others by allowing them in various ways to see screens. That said, our participants did have 'occasion' to use passwords, as Mike and Alice elaborate:

> **Mike**: The PC upstairs occasionally has a password. It usually doesn't. It's in the back room. The last time I put a code on was when we had a decorator in to do that room. I've done it once or twice when we've had guests staying.
>
> **Alice**: Yeah, when my nephew comes, 'cause he just logs into everything.
>
> **Fieldworker:** It kind of depends on the guest?
>
> **Mike**: Yeah.
>
> **Fieldworker**: 'cause you see it as a potential risk?
>
> **Mike**: Yeah.
>
> **Fieldworker**: What would be a potential risk?
>
> **Mike**: Basically, er, adult material on there. So potential embarrassment I guess.
>
> **Mike**: With the decorator guy, it was more the general principle. There's personal information on there.
>
> **Alice**: Bank details and stuff, so we don't want them.
>
> **Mike**: Yeah, whereas if it was like family staying there, it's more like the scenario where they just use the PC for something and stumble across a folder I'd rather they don't stumble across.

It would be easy to render what Mike is saying here as being that he and Alice use passwords to ensure data privacy. They do, of course, want to protect their 'bank details and stuff', but there is more to it than that. Insofar as they do use passwords to ensure data privacy, then they do so on a *selective basi*s, rather than as a blanket policy. This will no doubt cause security advisors to throw their hands in the air. However, it is accountably the case that what drives the use of passwords is the *social relationships* that hold between members. Be it 'the decorator guy', 'guests', 'my nephew', 'family', etc., who someone is, what relationship holds between them and those they are visiting in the home and why they are visiting determines the use of passwords. We, therefore, found that family members, friends, friends of the kids

and baby-sitters were routinely *given* passwords to access networks, devices and applications, whereas tradesmen and the customers and clients of home-workers were not. In cases where visiting was premised upon purely professional relationships, we found that access was more heavily controlled, with participants entering passwords into visitors' devices if necessary. Some even monitored visitor's behaviour, 'sticking around' to ensure they did not do anything they did not want them to do.

However, what is notable about Mike and Alice's occasioned use of passwords is that it is also driven by an accountable concern with risk, not in terms of data privacy but *to members*, e.g., to the nephew who just logs into everything and might be exposed to adult material, or to the family staying in Mike and Alice's backroom, who might be embarrassed by such material, just as Mike and Alice might be embarrassed by them seeing it. Our studies are shot through with this accountable concern with risk, which is why we hesitate to render the occasioned use of passwords as a matter of data privacy. Rather, privacy is a gloss for a host of situated practices designed *by* members to manage the risks that the digital poses *to* members. We thus find that commonplace practices such as the setting of passwords is as much about protecting children from harmful content, as it is about protecting data from harmful actions. Equally commonplace, but more rarely recognised, are the situated practices for managing the manifold risks of accountability in the digital world and what can therefore be observed and reported about oneself.

3.2.1 Privacy as accountability management

Passwords are an obvious means of managing accountability – if one's devices cannot be accessed, what one does online cannot be rendered observable and reportable and thus be opened up to account. However, it is in the nature of living with other people that devices are accessible to them. Joe and Carrie tell us something of what organises device access:

> **Joe**: My wife might use my phone if it's handy, or I might use hers, you know. It's not a big deal for us. But my daughter [who is 17] has got a PIN number on hers, and I think my son [who is 21] has as well. He's got his locked.
>
> **Fieldworker**: You don't know the PINs?
>
> **Joe**: No, no. They have all their feeds coming in, Snapchat and Twitter and god knows what.
>
> **Carrie**: We consider their stuff asprivate. We don't need to nose in.

As Joe and Carrie make perspicuous, managing accountability is not simply a matter of putting passwords in place, but very much turns on appropriate relationship-relevant behaviour and thus on *cohort-relevant access*. While members of the 'husband and wife' or 'partner' cohort, such as Joe and Carrie, may routinely access one another's personal devices, they do not necessarily access devices belonging to members of the 'children' cohort (whether members do

or do not very much depends on the children's age and the expectations that go along with that). It is also the case that, while members of the 'partner' cohort may routinely access one another's devices, they do not have blanket access. They may use a partner's phone to call someone if it is handy to do so, but accessing other applications is an occasioned matter, e.g., one might read a social media post because their partner has asked their opinion of it, or read out loud a text message that has just arrived because their partner is busy doing something else. Perhaps surprisingly, the restricted nature of cohort-relevant access is not principally driven by a concern with privacy – many a partner told us they had 'nothing to hide' from one another – but with social relevance. Simply put, what one does online is not seen or treated as *relevant* to one's partner by default. Privacy only becomes a concern when cohort-relevant access is disregarded, which would ordinarily be an accountable matter (e.g., what are you doing?) and be dysfunctional and even dangerous if it persisted [32].

An equally obvious means of managing one's accountability is to clear caches, cookies and browser history and/or use private browsing modes.

> **Fieldworker**: Do you clear caches, cookies or search histories?
>
> **Kit**: The only time I've done it is when it's like Tim's birthday and I try to do things secretly so he doesn't know. I put private browsing on and I – I've asked him before and he told me how to empty things.
>
> **Tim**: Clear the cache, yeah. Yeah the only other times I could see mild embarrassment is if you've gone out and I've got Netflix to myself and then I'll be like, right, good car chase film – when do I ever get to watch good car chase films? But then obviously it comes up, doesn't it, you know, like next time you go on Netflix, you've been watching …
>
> **Kit**: Oh! Hmmm.
>
> **Tim**: So you can log onto Netflix and delete these things.
>
> **Fieldworker**:And do you?
>
> **Tim**: No I don't actually. Well, if I did, I wouldn't tell you, but I don't. But I definitely wouldn't answer that honestly if I did.

As Tim somewhat amusingly makes visible in this vignette, owning up to clearing caches and histories can be a thorny issue, but rendering one's on online behaviour invisible and thus unaccountable to other members of the home is not done merely to mask embarrassment, mild or otherwise. As noted above, there is a strong presumption of cohort-relevance built into our online activities and this warrants the occasional use of procedures to ensure the confidentiality not only of *what* we do, but *who* we do it with or for. So, while these procedures can be used to protect one's privacy, they are also quite often used for the benefit of others (e.g., to avoid special occasions and surprises alike being spoiled).

Cohort-relevance drives *cohort separation* to ensure that one is only accountable to those one needs to be accountable to, and nowhere is this more pronounced than on social media.

> **Fieldworker**: And the Facebook friends are, er, who?

> **Chloe**: People I know. Basically, most of my family, and my friends and a few people that I know from school who asked me so I just accepted 'cause I know them. But if it's anybody I don't know I won't accept.
>
> **Fieldworker**: And do they overlap with your Twitter people? Do you have the same Facebook friends that you're following on Twitter or following you?
>
> **Chloe**: No.
>
> **Fieldworker**: No connection between them at all?
>
> **Chloe**: No, my social life has nothing to do with my Twitter life. Twitter life is Internet life. Facebook life is social life.

As Chloe makes clear, it is common practice amongst people who employ multiple social media channels to use them to facilitate the separation of cohorts and to reflexively enable, as a matter of method, the management of friend and follower relationships. Along with this, they can manage the relationship-based tailoring of personal content to particular channels and cohorts. The methodical separation of cohorts is bound up with an abiding practical concern to avoid having to endlessly account for one's online activity to the people one knows best in everyday life, such as one's friends and family. Members do not seek to dispense with accountability entirely, only to manage *just who* they might be accountable to and for what, so they exploit different channels to design personal content for different categories of recipient. Recipient design even includes adopting pseudonyms, which not only averts the potential need to account for turning down friend or follower requests from people one is routinely accountable to in other ways, but carries the advantage that there will be less chance of sharing personal data with people one would not ordinarily wish to share it with. While this is common practice there is, we note, no stability in the choice of channels (e.g., that Twitter is used for a certain kind of cohort and Facebook for another). Nor is there any stability in the purposes for which different channels are used (what one person uses Twitter for another may use Facebook or any other social media channel for instead). What we do see, regardless of matters of personal choice, is that different channels are *tied* in practice to different cohorts and the particular kinds of relationship that hold between their members.

Against this background, data is shared on the basis of an assumed and accountable *right of disclosure*, which is commonly understood by recipients and further limits the potential impact of posting personal data online.

> **Samantha**: I wouldn't mind somebody seeing something that I was sending, but I'd be uncomfortable about somebody seeing something that Tom [her brother] had sent me.
>
> **Fieldworker**: OK. Why's that?
>
> **Samantha**: It would feel like more of a breach of privacy, because it's something he's sending specifically to me. Often it is just like photos of him and Rick [his partner], or food that he's made or things that he's seen that reminded him of me, and things like that. It would feel much weirder for somebody to see what he was sending me.

> **Fieldworker**: Why would it feel weird? What would feel wrong about it?
>
> **Samantha**: Well Tom is a very private person and I wouldn't like to share stuff with other people that he's sent specifically to me without having asked his permission to do so.
>
> **Fieldworker**: OK. So you need the right to be able to share it you feel? And you wouldn't just have that right automatically to share it?
>
> **Samantha**: No.
>
> **Fieldworker**: OK. Does that go for other content that you receive from other people on social media?
>
> **Samantha**: Yeah, I don't share stuff like that because, as I said, it's something that's been sent specifically to me and I wouldn't share it without asking somebody if they were OK with that.

Something that Samantha makes evident is that one's accountability for data that has been shared with you by other people is not necessarily handled in the same way that you would handle your own data. There are chains of accountability to be considered, such that the onward sharing of data is organised around one's right to share it. This right may be presumptive, or someone may quite literally be given a legal right to share data. However, the presumptive right largely obtains in mundane interaction, even when the recipient knows that the data shared with them may well have been shared with others. Indeed, while Samantha often discussed Tom's social media posts with family members, she was not given to showing them the actual messages he sent her, that would feel like a breach of privacy.

3.2.2 Breaching privacy

Members routinely manage their privacy through situated practices that have become common-sense ways of managing one's accountability in the digital world. Thus, we find that members observe cohort-relevant access as much (if not more) than they use passwords to control interpersonal use of devices and their content. They implement cohort separation and tailor personal content to the members of particular cohorts through the use of dedicated communication channels, limiting unintended disclosure and personal exposure through the use of multiple channels and identities. Data is shared under a presumed right of disclosure that limits onward distribution. That said, as attested to by a host of studies [33–40], the digital world frequently manages to breach one's accountability and privacy. What we want to do now is consider some of the ways in which that routinely happens.

An increasingly diverse array of everyday activities is now geared towards interaction with parties and organisations online. These parties may, in principle, be located anywhere and be oriented to either as known members of various cohorts or unknown or unknowable, beyond what common-sense assumptions may be made about them and their interests. This has an important impact upon people's sense of accountability, as data sharing is predicated on the vital interplay of mutually assumed rights and expectations accorded to the specific relationships in play. In short, if there is no established relationship because a party is unknown or

unknowable, then the grounds of mutual accountability are hard to assess, which in turn informs a generic data sharing policy:

> **Christine**: There was a hideous picture [once], but if it was something that I considered to be *that* sensitive I wouldn't use it. If I'm not happy to share it, then it doesn't go anywhere.
>
> **Alice**: I wouldn't put anything on that I wasn't happy for anybody to see. Managing real private stuff is – stuff shouldn't exist, that's the level of it: it doesn't get written down; it doesn't get put in a photo; it doesn't exist. Definitely do not put online.

As Christine and Alice make clear, the sensitivity of data and the risk of personal exposure furnishes a general account for not sharing something. Nonetheless, people often share things online that they subsequently regret. The literature is replete with examples of postings on social media that have escaped the control of their authors and resulted in embarrassment. So, while many people, like Christine and Alice, entertain a generic data sharing policy, there is evidently an inherent tension between that policy and actual occasions of data sharing. The tension is often referred to in terms of the 'privacy paradox', which privacy expert Daniel Solove [41] dismisses as a myth on the basis of 'a series of improper generalisations from people's behaviour'. We concur, but this does not dispense with the inherent tension between general data sharing policies and specific occasions of data sharing, which can and do lead to privacy breaches. The difficulty lies not in the seemingly paradoxical relationship between members' reasoning and their behaviour (what they say versus what they do), but in the *mismatch between members' reasoning and the operation of digital systems*.

This mismatch is made perspicuous when we consider the mundane challenges of managing accountability in a digital world where members are inherently connected, socially as well as technologically.

> **Michel**: One of the reasons why Carrie is not so sensitive about posting family photos on Facebook is because pretty well the only network who get to see that are family and friends. Whereas with me, the network who can actually see that includes work colleagues, some of whom I don't even know very well. I mean, we've had photos of me in fancy dress for instance on Facebook and it's become clear that other people have had access to those things!
>
> **Fieldworker**: So it's other people's stuff that you're in and they've put up?
>
> **Michel**: It's never stuff that I share myself, no, 'cause I don't do that kind of stuff.
>
> **Carrie**: I do, of fancy dress (laughs). Have you seen that one (Carrie holds up her iPad to Paul, and then turns it to show the fieldworker).
>
> **Fieldworker**: (Laughs at photo of them both in fancy dress).
>
> **Michel**: (Laughs).
>
> **Carrie**: It's stuff like that he doesn't want me to put on.

> **Michel**: This is the problem for me. I can control it all I like myself, but I have no control over what other people do.

Here, we can see that Michel expresses his frustration with the limited resources he has available for controlling what kinds of things get shared with whom on Facebook, and his frustration reveals the extent to which managing accountability through friend and follower relationships is a blunt instrument. The issue here is not so much to do with the fact that other people can post data about you, or data that involves you, but is more to do with how to manage distinctions between people who have access to that data. The distinctions that hold between 'family' and 'friends' may be relatively straightforward to make but those that hold between 'friends' and 'work colleagues' are certainly more blurred, where the latter may also include the former as well as people one does not know very well, if at all. Differences in relationship are accompanied by differences in accountability, and this applies even when one is a member of the same cohort. Consider the accountability that holds within the family between one's partner and children, for example, and with it the different rights and obligations that hold between different members of the same cohort. The digital world rides roughshod over such differences and pushes people into what amount to *generic data sharing mechanisms*, which assume that all people in the same bucket (e.g., friend or follower) are essentially the same. They are not. Furthermore, there is no way to express or reflect the nuances in human reasoning and human practice where members manage *just what* is made visible and *just who* it is made visible to. Nor is there any way to reflect the range of common-sense methods that exploit place, physical barriers and proximity to control *just when* things are said, *just where* they are said, *just how* they are said and so on. Generic digital data sharing mechanisms inhibit embodied methods of recipient design. So, in the digital world, where the operation of these methods is restricted by technical mechanisms, members must live with the consequences and have to manage breaches as they occur.

The mismatch between human reasoning and the operation of digital systems is further underscored by members efforts to account for privacy breaches. Members do not stop reasoning about why things happen just because they are encountered in the digital domain. They hold the digital accountable and attempt to find reasonable, ordinary, everyday explanations for the things they see and experience there. Now, to presume that digital systems reason in the way that human beings do, and to hold them intersubjectively accountable on those terms, is admittedly problematic. However, it does not prevent members from reasoning about the digital in this way and it does not mean that this way of reasoning is inconsequential for how members proceed.

> **Sara**
>
> There's one thing that worried me. Do you remember that time – my family's Jewish, and my uncle sometimes posts things, just once or twice, about searching for family in the Ukraine and stuff – and I was starting to find a shop selling everything Jewish coming up advertising on my page. So they've obviously made a connection that somewhere in the family

> there is somebody Jewish, and they've advertised that to me so that means obviously that it's visible to somebody. It makes you very aware that people are watching what you're doing. It's like I was explaining to Hannah [Sara's teenage daughter] the other day. She was getting ads for pregnancy tests and she says, why am I getting this stuff. I said it's targeted because you're a teenage girl. And she said, but I've never gone on any site like that, I've never looked at anything. I said it doesn't matter, they can tell by the type of sites that you do go on to – they can put you within an age group and sex group and so you're targeted. She really doesn't understand that even so. She says I go on gaming sites, I could be a boy. Yeah, you could, but even so the indications that you give are a flag to somebody.

Sara invites us to consider two distinct but interrelated matters here. The first reflects widespread societal concern that personal data is accessed and used by parties who are not party to our online interactions, i.e., a third party, and an anonymous one at that. The second matter for consideration is that Sara does not understand how her data has been acquired by a third party, because she has not knowingly shared her data with somebody outside her online interactions. The same applies to Sara's daughter as well, just as it does to many millions and indeed billions of people. So, Sara makes it visible that *what counts as data sharing* in the digital world is deeply problematic. From a members' perspective, data sharing in the digital ecosystem is evidently opaque. This lack of accountability – of observability and reportability – and with it the ability to see, recognise and understand what is happening goes beyond what we have been saying about the crudity of tools for managing relationships online and the way they pre-configure sharing on a generic basis. We can see now that this goes beyond digital systems obliging members to engage in generic rather than situated reasoning about data sharing, thereby disrupting the ordinary grounds of accountability. They also do not necessarily count as sharing what members *recognise* as sharing practices and do not make themselves evidently accountable for handling what is shared in the same way. This, of course, goes to the core of understanding what counts as data, and, more than this, what digital systems can do with personal data, as opposed to what other *people* can do with it, where intersubjective reasoning and ordinary accountability can be assumed to hold.

This mismatch between human reasoning and digital operations is further evidenced in the occasioned sharing of data.

> **Sylvie**
>
> I tried for a while having people graded by their friendship status. So I'd have like real true friends, and then I had my work friends who would ask me to be their friend but I felt kind of like socially awkward saying no on Facebook, so I had them as acquaintances. It got really confusing, you know. Someone might graduate from being an acquaintance to an actual friend but they still work with you, and then they come into work and say, 'Oh I saw that picture of you at the park, it was really cute' and everyone else goes, 'What picture? I didn't see that on Facebook.' So I've given up on that. It just got really hard.

Sylvie's experience with Facebook makes it perspicuous that data sharing in the digital world is essentially marked by *a lack of reciprocity*, which is key to ordinary accountability. Reciprocity means that the world 'as I see it for all practical purposes' (in contrast to theoretical, political, ideological or religious purposes, etc.), is the world 'as you see it for all practical purposes'. If this were not the case, I would not be able to see what you were doing (e.g., waiting to cross a busy road) and to coordinate my actions accordingly (e.g., to slow my vehicle and wave you safely across regardless of whatever theoretical, political, ideological or religious thoughts might be running through either of our heads). Now this is obviously not case for Sylvie and her friends, be they 'real true friends', work friends, actual friends or acquaintances. The practices she devised for sharing data and managing her accountability were not practices that *others* were able to recognise and organise their own interactions around in response. Of course, people were being embarrassed by awkward revelations long before digital technology arrived on the scene. However, the interesting thing here is that the source of trouble is not so much the content itself, as the lack of *intersubjective understanding* of the practices involved in the management of digital content: how might Sylvie's Facebook friends have *known* that she was adopting a practice of organising them in such a fine-grained fashion, when there is nothing within the digital domain that makes her situated practices observable and reportable? There is no reciprocity of perspectives. This is not only problematic for members like Sylvie, who are concerned to manage the day-to-day sharing of data and their concomitant accountability, it is also, as Sara highlighted for us above, a source of widespread complaint. Thus, a general lack of reciprocity in the digital world not only renders invisible the situated practices members devise and use to manage data sharing, thereby enabling privacy breaches, it *also* masks the practices of others who might access their data without their knowledge.

The operation of digital systems poses further challenges to members' efforts to manage their accountability by *rendering the ordinarily invisible visible*. As the digital reaches further into our physical and social environment, it increasingly renders members accountable for things that are outside of their control, surfacing information about members' activities that they would usually expect to remain out of view and creating circumstances where they are obliged to account for things for which accounts would never ordinarily be sought.

> **Susannah**: (Reading a time series graph of motion and humidity sensor data from the bathroom). So what are we saying? We're saying the 5th, that was Mary being off, and the 6th was you being at home. Oooh, what did you do?
>
> **Frank**: I didn't do anything.
>
> **Susannah**: You did. At 12 o'clock. Look at that.
>
> **Frank**: Where? Nothing.
>
> **Susannah**: No, here.
>
> **Frank**: I could have been up late, 'cause I've had this headache thing. I've been a bit poorly – oh give me sympathy – so that's probably me

> getting up late isn't it. Having a late shower. It's high for along time. I don't remember having that long a shower.
>
> **Susannah**: Yeah, but you could have had a shower and then you could have had a shave.

It is a brute fact of life, as Frank can testify, that the cohort most likely to call members to account for their activities is their family and those with whom they have the most intimate relationships (parents, siblings, partners, etc.). Now, it is of course the case that member's bathroom practices can be called to account as an ordinary feature of everyday life in all sorts of ways: toothbrushes may be left in the 'wrong' place or the toothpaste squeezed in the 'wrong' way; towels may be left in a heap on the floor; all of the hot water may have been used up and so on. Members may also make their own bathroom practices visible to others: calling out to say they are about to have a shower, so that others do not turn on taps and make the shower run suddenly hot or cold; saying where one likes to keep their towel because someone keeps moving it; calling out their weight from the bathroom because they have just stood on the scales and it is gone down; etc. All of this is a normal and a naturally accountable part of the daily round. However, the presence of a new digital window onto what members do, created by an increasing array of sensor-based devices, stands outside ordinary everyday reasoning. This is especially the case with respect to how knowledge of one's activities might be made visible and the concomitant possibility of needing to provide an account for them. This has the scope to cause serious trouble, disrupting in a pejorative way the foundations of everyday life.

Let us hover for a moment longer in the sensor-equipped bathroom of the imminent future to underscore the seriousness of rendering the ordinarily invisible visible.

> **Susannah**
>
> I'm aware that there's evidence that Sally's gone for a wee when she's spent most of her life trying to. At the moment, she's defining her space, and David [their 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.

As Susannah makes perspicuous, rendering the ordinarily invisible visible creates a sense of invasion, allowing one to now look and find who did what, when and where. This is problematic in various respects. It obviously breaches members' privacy, but there is more to it than that. The issue is not simply that the digital furnishes Susannah with evidence that Sally has gone for a wee. Parents often have cause and need to observe and remark on their children's toilet habits. But it is when their habits cease to merit observation and report, when they become *unremarkable*, that matters. Then the child may be said to have mastered the art and demonstrated their competence in the ordinary affairs of everyday life. Just to be clear, it is not that the child can go for a wee on its own that marks their competence, but their ability to do so without occasioning the need to pass, or for others to pass, remark during or after the event. That everyday activities and accomplishments *are* unremarkable

is not just a practical matter, but a moral one essentially concerned with the orderly nature of our conduct. So, when a technology is introduced into the world that makes whatever mundane, unremarkable things members are doing visible and open to account, it breaches fundamental expectations about how social life is organised. Susannah's sense of invasion is not about Sally's privacy per se, then. It is not to do with the fact that she can see that Sally has had a wee, but apodictically in doing so that she puts Sally's competence and with it her growing sense of independence at risk. Furthermore, accountability cuts both ways, which is to say that it is not only the data subject who is rendered potentially accountable. Members who disclose their knowledge of ordinarily invisible activities are just as likely to find themselves accountable for why they have taken an interest in them in the first place. Thus, in rendering the ordinarily invisible visible and open to account, the digital world *disrupts the unremarkable foundations of everyday life*, not only impacting members' privacy but in doing so their competence or ability to conduct their everyday affairs in an unremarkably orderly manner, thereby undermining their autonomy.

3.3 Discussion

Privacy is routinely breached in the digital world not because there is a mismatch between what members say and what members do, but because of the mismatch between members' reasoning and situated practices on the one hand, and the operation of digital systems on the other. In the analogue world, members exploit an array of embodied practices to manage their accountability. This is done by carefully designing data disclosure for particular recipients, i.e., controlling *just what* is made visible and *just who* it is made visible to through a range of common-sense methods. These methods exploit place, physical barriers and proximity to control *just when* things are said, *just where* they are said, *just how* they are said and so on. However, in the digital world, the operation of these methods is restricted by generic data sharing mechanisms that designate members as friends or followers, for example, without respect to the nuances that hold within a cohort let alone between them. Then there is the fact that what counts as data sharing in the digital world is deeply problematic. Digital systems do not necessarily count as sharing what members recognise as sharing and do not make themselves accountable for the handling of what is shared in the same way. There is also a lack of reciprocity in the digital world, which renders invisible the situated practices members devise and use to manage data sharing. More than this, it masks the practices of others who might access their data without their knowledge. We can add to this how the digital increasingly renders the ordinarily invisible visible, thereby disrupting the unremarkable foundations of everyday life. Put these things together and it becomes perspicuous how and why privacy breaches occur. We have seen that privacy is not simply a matter of controlling one's accountability, but that doing so is essential to members' autonomy and their ability to conduct their everyday affairs in an orderly manner, unhindered without due cause by others. Little wonder then that the digital undermines *societal trust* at scale.

It might be said that it is blindingly obvious that privacy is essential to members' autonomy, but that merely begs the question why, then, have we built a destabilising infrastructure into the fabric of everyday life? The answer is no doubt complex and turns as much on accident or at least the lack of foresight as it does intent, but it is the question of trust that occupies us here. This ordinary language concept has been, and will no doubt continue to be, subject to heterogeneous treatments. Thus, trust is commonly understood as an attitude and matter of choice as much as it is to do with assessing risk, all of which runs alongside domain considerations such as 'trust and the family' or 'trust and political systems'. The social theorist Pierre Bourdieu [42] construed of trust as 'habitus', a defining feature of how members perceive and orient to the social world, whereas Luhmann [43] sees trust as performing a sociological function. Gambetta's rational choice theory [44] is concerned with the 'conditions under which trust is justified', and Coleman's [45] influential modification of this theory focuses upon trust as a calculated and calculable risk 'taken about the performance of others'. We take the rather mundane view that trust is a 'background condition' of ordinary action [46], something that members for the most part have no need to call into question. As Watson [47] notes,

> When the trust condition is not in place, participants experience bewilderment, confusion, frustration or indignation, or they attempt to make sense of or normalize the events in different terms – as a joke, or hoax, a deliberate provocation, obtuseness or whatever.

Now this *attempt to normalise* situations in which trust is breached is key to members' efforts to incorporate the digital world into ordinary action. The attempt consists of exploiting an evolving calculus of accountability to manage the 'attack surface' the digital creates in breaching privacy and disrupting the unremarkable foundations of everyday life.

The notion of the attack surface in a digital context is usually invoked with respect to security, which emphasises the management of unauthorised access to hardware, software, firmware and networks as a general panacea to privacy concerns [48]. Technically the attack surface is understood as the sum of the different points in a computational environment where an unauthorised party might get into that environment and get data out [49]. This contrasts with the attack surface in everyday life, which we might understand as the sum of the points in a computational environment where ordinary action can be made observable and reportable. The human attack surface is increasing exponentially with the emergence of sensor-based devices in everyday life and the so-called 'Internet of Things' or IoT. As we have seen, the IoT surfaces information about ordinary action members would usually expect to remain out of view, creating circumstances where they are obliged to account for things that they would never ordinarily have to account for. The attack surface in the connected home consists not just of desktops, laptops, tablets and smartphones, but an increasing number of smart products [50] including wearables, household appliances, embedded devices and fast-moving consumer goods that are starting to be wrapped in increasingly intelligent packaging [51]. We are on the cusp of an explosive increase in the domestic attack surface. Industry analysts [52] predict

that 29.3 billion devices will be connected to IP networks by 2023, that the share of machine-to-machine (IoT) connections will grow to 50% in the same period, that the consumer segment will account for 75% of total devices and connections, and that connected home applications will account for the 'largest share' of these.

Right now, members are managing to protect themselves in circumstances where the attack surface is constituted by an average of ten connected devices per household [53]. They do so by physically controlling who has access to the places where digital devices are situated and by exploiting physical barriers, people's proximity and the positioning of devices to manage the availability and visibility of personal information. We have also seen that the social relationships that hold between members is a primary determinant of digital access controls, with the use of passwords being driven as much by a concern to manage cohort-dependent risks and protect others from exposure to inappropriate digital content as it is to protect personal data from harm. We have further seen that members exploit cohort-relevant access controls to manage the interpersonal use of personal devices, effect cohort separation (e.g., through the use of bespoke social media channels and identities) to manage their accountability in sharing personal information online, and handle data shared by others under a presumptive right of disclosure that restricts sharing and onwards distribution. In these ways, i.e., through situated practices, members attempt to normalise the effects of a destabilising infrastructure on everyday life. These practices are constitutive of a *calculus of accountability* – a set of common-sense methods rooted in ordinary action that are evolving to enable members to manage the observability and reportability of their online activities. Time and again, the reasoning driving this evolving body of practice amounts to avoiding real-world accountability for the things done online in order to carefully manage just who it is one might be accountable to and in what ways. This reasoning is imbued with a strong (moral) preference that one's actions are found to be naturally accountable and therefore ordinary and unremarkable features of everyday life. The evolving calculus governing privacy and data sharing in the digital world thus seeks to *constrain* the accountability of persons and their digitally mediated interactions to being seen in this way.

We find, then, that members manage their accountability locally by managing access to their devices and data. In this way, they can control just who can see what and what might therefore be treated as a topic of remark or conversation. The practices involved in doing this are utterly taken for granted and routine. Thus, when people keep things from view, the fact they are doing this is in no way treated as remarkable, but rather as a naturally accountable feature of ordinary action in its own right. When it comes to the sharing of personal data online, members also orient to what is or is not made visible and to whom and seek to manage that accordingly. However, what is different in the online world is the relatively crude tools available for managing just who the information will be shared with and what kinds of accounts can be shaped within and around the content of the data being shared. We find, then, that members take great care over the management of cohorts, identities and the visibility of the digital self, methodically employing multiple social media channels to limit the impact of the digital on their accountability and the

accountability of their actions. And, we find in these situated practices that managing the potential attack surface is increasingly becoming a matter of routine. That members are, on a daily basis, and in a great many cases, able to exploit the calculus of accountability to bring about their online activities and digitally mediated interactions as naturally accountable, ordinary and unremarkable features of everyday life.

That members are finding ways to normalise a destabilising infrastructure and manage the attack surface created by the digital on their accountability and integrity as autonomous human beings, is no reason to be complacent or to assume that digital systems are already good enough and that it is simply a matter of time before people come up to speed with innovation in the ecosystem. For all that people evidently can make do with what the digital world provides them, it is also evident that it is routinely encountered as a troublesome place that breaches the calculus of accountability. Privacy breaches are commonplace, and members have common cause to complain about the paucity of generic data sharing mechanisms and their inability to enable intersubjective understanding of their own situated data management practices or the practices of others. Add to that the potential for new technology to render members accountable for matters that might ordinarily be expected to remain out of view and be normally and naturally unremarkable, and the capacity for the digital not only to breach the calculus of accountability but also the social and moral order with it, and it becomes apparent that members' trust in the digital world hangs by a rather more tenuous thread.

As Watson [47] elaborates, trust is a necessary background condition of mutually intelligible courses of action, by which he means that the parties to ordinary action must understand that they are engaged in the same practice, must be competent to perform that practice, must actually perform it competently and assume this also of others, and that all parties to ordinary action must therefore be oriented to the same 'rules of engagement' so to speak. As we have seen, competence in a practice is a socially organised, moral matter that turns on ordinary action's unremarkable character and, more specifically, on members being able to bring their activities about in that way, i.e., accountably as naturally occurring, perceivedly normal, ordinarily unremarkable courses of action [1]. We have also seen that technologies that disrupt the ordinarily unremarkable grounds of everyday activities in rendering the ordinarily invisible visible, break the rules of engagement by violating the grounds upon which mutually intelligibility stands. They not only open up ordinarily unremarkable activities to unwarranted account but throw members' competence and autonomy into question by doing so. So, technologies that breach the ordinarily unremarkable grounds of everyday activities are not only disruptive of specific courses of action, they are disruptive of members' trust in the workings of the social and moral order itself.

There is need to proceed with care as the attack surface expands in everyday life. Key to this endeavour is the recognition that there is more to the sharing of personal data than data. It is, of course, still important to articulate what data is being shared, especially with respect to underlying and evolving technological platforms. New data protection regulations and the interest in making algorithms accountable suggest elements of this are already in hand. However, it is also important to transcend

generic mechanisms and support the haecceities of data sharing to enable people to manage just where, just when and just who gets access to their data, and to determine just what gets used, what it gets used for and by whom, whether incidentally or purposefully on a case-by-case basis. This implies that the digital ecosystem needs to provide ways of supporting the sharing of data that move beyond pre-specifying data access policies and sharing permissions. Providing more granularity by giving lots of sub-cohort options [54], for example, will not fix the fundamental problem, because people do not know in advance what every instance of sharing involves and such 'rules' (like any others) are 'merely advisory to action' [55].

Building trust into the digital world requires that members be furnished with resources that support the calculus of accountability and thus enable the attack surface to be managed and contained. While cybersecurity measures may be a necessary part of the mix, they are not sufficient and efforts are also required to build a reciprocity of perspectives into the digital ecosystem. Reciprocity is key to accountability – to the observability and reportability of ordinary action and to its coordination. Without it, it is not possible to see, recognise and understand what another party is doing and to respond accordingly. Reciprocity thus enables members to engage in mutually intelligible courses of action and interaction. This has been markedly lacking in the digital world for a long time [56]. Resources are particularly required to enable intersubjective understanding of members' situated data sharing practices and third-party access to and use of members' data. Reciprocity is not a precursor to action and interaction, but something that is written into its DNA and runs throughout. It cannot be reduced to privacy notices, checkboxes and informed consent, but must be enabled as an accountable feature of ordinary action *within* the digital world and the unfolding, ongoing flow of members' digitally mediated interactions.

3.4 Conclusion

We began this chapter by saying that accountability in ordinary action refers to its observable and reportable character and thus to the mundane fact that members can usually see and hear at-a-glance what is going on around them. We also said that ordinary accountability is a taken-for-granted feature of our competence as members: that it not only allows us to see, recognise and understand what is going around us but that, in so doing, it enables us to coordinate our actions accordingly. On this basis, we said that ordinary accountability is the glue of social life, reflexively constitutive of the social and moral order. In unpacking how privacy is socially and morally organised we have seen that it is essentially a matter of *managing one's accountability*. Members especially seek to avoid real-world accountability for the things they do online in order to control just who they might be accountable to and in what ways. This involves the careful management of cohorts, identities and the visibility of the digital self online. Over the course of these mundane accomplishments, we have seen that members have devised common-sense methods that enable a calculus of accountability that is designed to manage the attack surface created by the digital's incorporation into everyday life. This is growing exponentially with the

introduction of the IoT and threatens to render ordinarily invisible activities observable and reportable at scale.

Now, it be might asked why, if ordinary action is observable and reportable and *the fact that it is so* is essential to the social and moral organisation of everyday life, introducing a technology that renders everyday activities observable and reportable is problematic? The answer, as we have seen, lies in the taken-for-granted nature of ordinary action. It resides in the fact that ordinary action is and is supposed to be *unremarkable*. Member's competence turns on their ability to bring about ordinary action *as* an unremarkable achievement [57]. Imagine a world in which we were constantly asking of one another 'what are you doing?' and 'why?' in the course of going about the ordinary business of everyday life. It is not simply a nuisance to have one's ordinarily unremarkable achievements *opened up* to account. It is consequential. This is not simply because it breaches our privacy but that, in so doing, it interferes with our ability as members to conduct our daily business in a competent fashion. Increasing the potential attack surface and rendering the ordinarily invisible visible at scale thus impinges on members' autonomy, disrupts the workings of the social and moral order, and threatens the fragile trust members have managed to invest, to date, in being able, for the most part, to manage their accountability in the digital world. However, we should not be complacent, especially given the potential impact of the IoT on everyday life. Great care needs to be taken in the emerging digital ecosystem to complement innovation by providing members with the resources they need to manage their accountability. Building-in reciprocity is key.

Reciprocity means that ordinary action is mutually intelligible, that the ways in which members manage their accountability are tied up with intersubjective reasoning about how others will apprehend and understand their actions. In other words, a reciprocity of views is essential for accountability to hold. Our studies make clear that breaches of privacy turn on a lack of reciprocity, making the effective management of accountability difficult. The problem is not so much one of *what* is shared as one of *how* it is shared. Generic data sharing mechanisms are simply not capable of supporting the nuanced situated practices that accountability management turns upon. Building-in reciprocity frames technical development in a different way to current trends in computing, which emphasise pre-specifying privacy policies and sharing permissions, both manually and increasingly automatically through the introduction of privacy assistants and AI. However, reciprocity is not a *precursor* to ordinary action but runs throughout it. Reciprocity thus needs to be engineered into the infrastructure of the digital world to enable intersubjective understanding within the *unfolding, ongoing flow* of ordinary action. Building-in reciprocity is not only a matter of making members aware of what is going on in the digital world and of making machine-to-machine interactions observable and reportable. Members also need to be able to understand how those interactions render them accountable. And they need to be furnished with the resources to manage their accountability online and in the analogue world as connected devices become increasingly embedded in the fabric of everyday life. Right now, that is something the digital is poorly equipped to do.

3.5 Acknowledgements

This research was funded by the EU FP7-ICT Programme (Grant Agreement ID:611001) and the Engineering and Physical Sciences Research Council (grants EP/F0642776/1, EP/K039911/1, EP/M001636/1). This chapter is based on the following original works:

- Crabtree A., Mortier R., Rodden T. and Tolmie P. [10] Unremarkable Networking: The Home Network as Part of Everyday Life. *Proceedings of the ACM Conference on Designing Interactive System*, Newcastle, UK, 11-15 [28] New York: ACM Press, pp. 554-563. https://doi.org/10.1145/2317956.2318039
- Tolmie P., Crabtree A., Rodden T., Colley J, and Luger E. [53] "This has to be the cats" - Personal Data Legibility in Networked Sensing Systems. Proceedings of the ACM Conference on Computer Supported Cooperative Work, San Francisco (CA), USA, 27 February – 2 March 2016. New York: ACM Press, pp. 491-502. https://doi.org/10.1145/2818048.2819992
- Crabtree A., Tolmie P. and Knight W. [8] Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work: The Journal of Collaborative Computing and Work Practices*, vol. 26 (4-6), pp. 453-488. https://doi.org/10.1007/s10606-017-9276-y
- Tolmie P. and Crabtree A. (2018) The Practical Politics of Sharing Personal Data. *Personal and Ubiquitous Computing*, vol. 22, pp. 203-315. https://doi.org/10.1007/s00779-017-1071-8

References

[1] Gambetta D. 'Can we trust trust?' in Gambetta D. (ed.). *Trust: Making and Breaking Co-operative Relations*. **1998**. Oxford: Basil Blackwell; 1988. pp. 213–37.

[2] Garfinkel H. 'A conception of, and experiments with, 'trust' as a condition for stable concerted actions' in Harvey O.J. (ed.). *Motivation and Social Interaction*. New York: Ronald Press; 1963. pp. 187–238.

[3] Page X., Knijnenburg B., Kobsa A. What a tangled web we weave: lying backfires in location-sharing social media. Proceedings of the ACM Conference on Computer Supported Cooperative Work; San Antonio (TX), USA, February 2013; 2013. pp. 273–84.

[4] Cognizant. Rise of the smart product economy. May 2015. Available from https://www.cognizant.com/InsightsWhitepapers/the-rise-of-the-smart-product-economy-codex1249.pdf [Accessed 11 November 2020].

[5] Crabtree A., Rodden T., Tolmie P., *et al*. 'House rules: the collaborative nature of policy in domestic'. *Personal and Ubiquitous Computing*. 2015;**19**(1):203–15.

[6] Dourish P. Culture and control in a media space. Proceedings of the European Conference on Computer-Supported Cooperative Work; Milan, Italy, September 1993; 1993. pp. 125–37.
[7] Dourish P. 'Seeking a foundation for context-aware'. *Human–Computer Interaction*. 2001;**16**(2-4):229–41.
[8] Crabtree A., Tolmie P., Knight W. 'Repacking 'privacy' for a Networked World'. *Computer Supported Cooperative Work*. 2017;**26**(4-6):453–88.
[9] Abdul A., Vermeulen J., Wang D., Lim B.Y., Kankanhalli M. Trends and trajectories for explainable, accountable and intelligible systems: an HCI research agenda. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Montreal, Canada, April 2018; 2018.
[10] Tolmie P., Benford S., Flintham M., *et al*. 'Act natural – instructions, compliance and accountability in ambulatory experiences'. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Austin (TX), USA, May 2012; 2012. pp. 1519–28.
[11] Garfinkel H., Sacks H. 'On formal structures of practical action' in McKinney J.C., Tiryakian E.A. (eds.). *Theoretical Sociology: Perspectives and Developments*. New York: Appleton-Century-Crofts; 1970. pp. 338–266.
[12] Vance A., Lowry P.B., Eggett D. 'A new approach to the problem of access policy violations: increasing perceptions of accountability through the user interface'. *MIS Quarterly*. 2015;**39**(2):345–66.
[13] Karr-Wisniewski P., Wilson D., Richter-Lipford H. A new social order: mechanisms for social network site boundary regulation. Proceedings of the Americas Conference on Information System; Detroit (MI), USA, August 2011; 2011.
[14] Bourdieu P. *Outline of a Theory of Practice*. Cambridge: Cambridge University Press; 1977.
[15] Dourish P., Grinter R.E., Delgado de la Flor J., Joseph M. 'Security in the wild: user strategies for managing security as an everyday, practical problem'. *Personal and Ubiquitous Computing*. 2004;**8**(6):391–401.
[16] Lampinen A., Tamminen S., Oulasvirta A. All my people right here, right now: management of group co-presence on a social networking site. Proceedings of the Conference on Supporting Group Work; Sanibel Island (FL), USA, May 2009; 2009. pp. 281–90.
[17] Solove D.J. 'The myth of the privacy paradox'. *SSRN Electronic Journal*. 2020;**3**.
[18] Altman I. *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding*. Monterey: Brooks Cole; 1975.
[19] Cisco. Annual internet report (2018-2023) white paper. 9 March 2020. Available from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html [Accessed 11 November 2020].
[20] Dourish P. 'Accounting for system behaviour: representation, reflection and resourceful action' in Kyng M., Mathiassen L. (eds.). *Computers and Design in Context*. Cambridge (MA): MIT Press; 1997. pp. 145–70.

[21] Ghaani M., Cozzolino C.A., Castelli G., Farris S. 'An overview of the intelligent packaging technologies in the food sector'. *Trends in Food Science & Technology*. 2016;**51**(10):1–11.
[22] Stutzman F., Hartzog W. Boundary regulation in social media. Proceedings of the ACM Conference on Computer Supported Cooperative Work; Seattle (WA), USA, February 2012; 2012. pp. 769–78.
[23] Coleman J.S. *Foundations of Social Theory*. Cambridge (MA): Harvard University, Belknap Press; 1990.
[24] Tolmie P., Crabtree A. 'The practical politics of sharing personal data'. *Personal and Ubiquitous Computing*. 2018;**22**(2):293–315.
[25] Rosenquist M. *Navigating the Digital Age*. Chicago: Caxton Business and Legal Inc; 2015.
[26] Tolmie P., Pycock J., Diggins T., MacLean A., Karsenty A. Unremarkable computing. Proceedings of the SIGCHI Conference on Human factors in Computing Systems; Minneapolis (MN), USA, April 2002; 2002. pp. 399–406.
[27] Westin A. *Privacy and Freedom*. New York: Atheneum; 1967.
[28] Crabtree A., Mortier R., Rodden T., Tolmie P. Unremarkable networking: the home network as part of everyday life. Proceedings of ACM Conference on Designing Interactive Systems; Newcastle, UK, June 2012; 2012. pp. 554–63.
[29] Luhmann N. *Trust and Power*. Chichester: Wiley; 1975.
[30] Dourish P. Process descriptions as organisational accounting devices: the dual use of workflow technologies. Proceedings of the ACM Conference on Supporting Group Work; Boulder (CO), USA, September 2001; 2001.
[31] Humbert M., Trubert B., Huguenin K. 'A survey on interdependent privacy'. *ACM Computing Surveys*. 2019;**52**(6).
[32] Dourish P., Button G. 'On "Technomethodology": Foundational Relationships Between Ethnomethodology and System Design'. *Human-Computer Interaction*. 1998;**13**(4):395–432.
[33] Heath C., Luff P. Disembodied conduct: communication through video in a multi-media office environment. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Louisiana (LA), USA, April 1991; 1991. pp. 99–103.
[34] Klasnja P., Consolvo S., Jung J., *et al*. When I am on Wi-Fi, "I am fearless" – privacy concerns and practices in everyday WiFi use. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Boston (MA), USA, April 2009; 2009. pp. 1993–2002.
[35] Nissenbaum H. 'Privacy as contextual integrity'. *Washington Law Review*. 2004;**79**(30):101–39.
[36] OWASP. Attack surface analysis cheat sheet. 2021. Available from https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet [Accessed 11 November 2020].
[37] Sacks H. 'Doing 'being ordinary' in Jefferson G. (ed.). *Lectures on Conversation*. Oxford: Blackwell; 1992. pp. 215–21.

[38] Sleeper M., Cranshaw J., Kelley P.G., *et al*. 'I read my Twitter the next morning and was astonished – a conversational perspective on Twitter regrets'. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Paris, France, April 2013; 2013. pp. 3277–86.

[39] Watson J., Besmer A., Richter Lipford H. '+Your circles: sharing behavior on Google+'. Proceedings of Symposium on Usable Privacy and Security; Washington (DC), USA, July 2012; 2012.

[40] Wisniewski P., Lipford H., Wilson D. Fighting for my Space: coping mechanisms for SNS boundary regulation. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Austin (TX), USA, May 2012; 2012. pp. 609–18.

[41] Sharrock W., Watson R. 'Autonomy among social theories: the incarnation of social structures' in Fielding N. (ed.). *Actions and Structure: Research Methods and Social Theory*. London: Sage; 1988. pp. 54–67.

[42] Aviva 'Tech nation: number of internet-connected devices grows to 10 per home'. 15 January 2020. Available from https://www.aviva.com/newsroom/news-releases/2020/01/tech-nation-number-of-internet-connected-devices-grows-to-10-per-home [Accessed 11 November 2020].

[43] Kristiansen K.H., Valeur-Meller M.A., Dombrowski L., Holten Moller N.L. Accountability in the blue-collar data-driven workplace. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Montreal, Canada, April 2018; 2018.

[44] Freed D., Palmer J., Minchala D., Levy K., Ristenpart T., Dell N. A stalker's paradise" – how intimate partner abusers exploit technology. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; Montreal, Canada, April 2018; 2018.

[45] Bellotti V., Edwards K. 'Intelligibility and accountability: human considerations in context-aware systems'. *Human–Computer Interaction*. 2001;**16**(2-4):193–212.

[46] Furniss D., Blandford A., Mayer A. Unremarkable errors: low-level disturbances in infusion pump use. Proceedings of the 25th BCS Conference on Human Computer Interaction; Newcastle, UK, July 2011; 2011. pp. 197–204.

[47] Watson R. 'Constitutive practices and Garfinkel's notion of trust: revisited'. *Journal of Classical Sociology*. 2009;**9**(4):475–99.

[48] Patil S., Norcie G., Kapadia A., Lee A.J. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. Proceedings of the Symposium on Usable Privacy and Security; Washington (DC), USA, July 2012; 2012.

[49] Newman M.W., Ducheneaut N., Edwards W.K., Sedivy J.Z., Smith T.F. 'Supporting the unremarkable:experiences with the obje Display Mirror'. *Personal and Ubiquitous Computing*. 2007;**11**(7):523–36.

[50] Bittner E. 'The concept of organisation'. *Social Research*. 1965;**32**:239–55.

[51] Garfinkel H. *Studies in Ethnomethodology*. Englewood Cliffs (NJ): Prentice-Hall; 1967.

[52] Bellotti V. 'Design for privacy in multimedia computing and communications environments' in Agre P., Rotenberg M. (eds.). *Technology and Privacy: The New Landscape*. Cambridge (MA): MIT Press; 1997. pp. 62–98.

[53] Tolmie P., Crabtree A., Rodden T., Colley J., Luger E. "This has to be the cats" - personal data legibility in networked sensing systems. Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing; San Francisco (CA), USA, February 2016; 2016. pp. 491–502.

[54] Hardstone G., Hartswood M., Procter R., Slack R., Voss A., Rees G. Supporting informality: team working and integrated care records. Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work; Chicago (IL), USA, November 2004; 2004. pp. 142–51.

[55] Zimmerman D. 'The practicalities of rule use' in Douglas J.D. (ed.). *Understanding Everyday Life: Toward the Reconstruction of Sociological Knowledge*. Chicago: Aldine Publishing Company; 1970. pp. 221–38.

[56] Guo Y., Jones M., Cowan B., Beale R. Take it personally: personal accountability and energy consumption in domestic households. CHI '13 Extended Abstracts on Human Factors in Computing Systems; Paris, France, April 2013; 2013. pp. 1467–72.

[57] Pollner M. *Mundane Reason: Reality in Everyday and Sociological Discourse*. Cambridge: Cambridge University Press; 1985.