Un-Paradoxing Privacy: Considering Hopeful Trust

BRAN KNOWLES, Lancaster University, UK
STACEY CONCHIE, Lancaster University, UK

Extant literature has proposed an important role for trust in moderating people's willingness to disclose personal information, but there is scant HCI literature that deeply explores the relationship between privacy and trust in apparent privacy paradox circumstances. Attending to this gap, this paper reports a qualitative study examining how people account for continuing to use services that conflict with their stated privacy preferences, and how trust features in these accounts. Our findings undermine the notion that individuals engage in strategic thinking about privacy, raising important questions regarding the explanatory power of the well-known privacy calculus model and its proposed relationship between privacy and trust. Finding evidence of *hopeful* trust in participants' accounts, we argue that trust allows people to morally account for their 'paradoxical' information disclosure behavior. We propose that affecting greater alignment between people's privacy attitudes and privacy behavior—or 'un-paradoxing privacy'—will require greater regulatory assurances of privacy.

CCS Concepts: • **Human-centered computing** → **HCI theory, concepts and models**; • **Security and privacy** → **Social aspects of security and privacy**.

Additional Key Words and Phrases: trust, privacy, consent, GDPR, fair information practices

ACM Reference Format:
Bran Knowles and Stacey Conchie. 2023. Un-Paradoxing Privacy: Considering Hopeful Trust. In *TOCHI'23 submission.* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The reasons why privacy matters are varied and numerous, but in the broadest terms, privacy matters as a control on *power* [85]. As Neil Richards (ibid) explains, those with access to information about a person have power over that person—the power to reveal something that makes them socially or politically vulnerable, the power to use that information to manipulate their behavior, the power to grant access to this information (and power) to other parties, and so forth. It makes a certain sense, then, that the matter of trust frequently arises in explorations of privacy. A paradigmatic feature of trust is the 'willingness to be vulnerable' [23], and being willing to disclose personal information ostensibly suggests that one trusts the entity in question to responsibly wield their power in ways that do not result in (privacy) harm to the individual. Further, because privacy is typically framed as a *concern* [25], trust is potentially implicated in privacy matters when defining trust as a 'willingness to be or remain within [an entity's] power. . . and to give them discretionary powers in matters of concern to us' [7]. So in apparent privacy paradox [80] conditions—when people disclose personal information in ways that are inconsistent with the high value they claim to place in privacy—one explanation is that they do so because they trust the entity receiving this information not to abuse their power (i.e. one has assessed the risks of information disclosure to be low because of the trustworthiness of the entity in question). For this reason, it has largely been taken for granted that 'trust directly influences privacy behavior' [80].

Empirical evidence showing a strong effect of self-reported trust on information disclosure behavior (to cite only a few examples: [25, 28, 53, 92, 113]) has been offered in support of the moderating effect of trust on privacy concern. This interpretation seems, however, to rest on three unproven assumptions: 1) that people actively consider matters of trust and privacy in their decision making around information disclosure and/or consent; 2) that people's self-reported trust in services they use accurately reflects their trust (both in amount and quality) at the point of making a disclosure/consent decision; and 3) that people are making a choice to disclose information and, thus, a choice to trust services with their privacy. Consider, instead, the likelihood that a person would consent to disclosing information to online services not because they have carefully considered available evidence of their trustworthiness, but rather because they feel they require that service. In such circumstances, they are not necessarily willingly making themselves vulnerable to betrayals of their privacy by these services and deeming that vulnerability sufficiently low-probability—indeed, they are not necessarily trusting the service with their privacy at all. It is plausible that, given they have nonetheless entered into a trust relationship (i.e. where their vulnerability might be betrayed), people might seek to 'manage their accountability in the digital world' [101] by emphasizing their trust in the services when self-reporting trust in study conditions. This suggests a radically different relationship between privacy and trust: Rather than directly influencing privacy behavior, trust is mutually implicated with privacy in accountability management by allowing people to morally account for their otherwise 'paradoxical' information disclosure behavior.

This paper attends to the need for in-depth examinations of the relationship between privacy and trust in apparent privacy paradox circumstances. While it may be intuitive, and 'reasonable to expect', that trust positively influences attitudes around privacy concern and information disclosure [89], we propose that the relationship between trust and privacy is more complicated than has previously been supposed. In this paper we report the findings of a qualitative study examining how people account for continuing to use services that conflict with their stated privacy preferences, and how trust features in these accounts. The paper begins by providing a more thorough background on the relevant literature at the intersection of privacy and trust. We then provide details of the study design and analytical approach, followed by the findings and discussion their implications for Human-Computer Interaction (HCI). The study ultimately finds that people's trust in online services is characteristically *hopeful*; and we argue that *hopeful trust* is a 'pragmatic response' to inchoate privacy protection regulation [42], a means of compensating for the absence of assurances of the trustworthiness of online services in matters of privacy. This paper helps counter the harmful narrative that 'privacy is dead' (see [85]), as people's hope indicates, above all, a desire for their privacy to be preserved in their online engagements.

2 BACKGROUND AND RELATED WORK

2.1 The Privacy Paradox and Critiques of Privacy Self-Management

The General Data Protection Regulation (GDPR) came into effect in 2018, seeking to empower individuals to more easily and effectively manage their personal data. A central focus of the regulation is the requirement for consent on the part of individuals giving their data—that consent must be given freely and be informed, with plain language provided around what/how data are collected, how/why it is processed, and with whom the data are shared. While hefty penalties for GDPR violations provide some incentive for service providers to handle personal data more responsibly, it is not clear that the regulation succeeds in empowering users to enact their privacy preferences.

This is somewhat unsurprising, as consent has long been critiqued as a mechanism for preserving privacy. As argued by Hull [49], making consent a legal requirement places the onus on the individual to self-manage their privacy in ways they are guaranteed to fail, arising from:

(1) *Explanations that are inadequate for enabling users to understand the consequences of their consent.* There is empirical support for the argument that people disclose personal information more than their privacy preferences would predict because they lack understanding of the consequences of that disclosure to their privacy [2, 40, 42, 60]. Much has been made of the fact that people do not read privacy policies (e.g. [76, 79, 97]). In part this is because they are long, and an annoying interruption to what one is otherwise getting on with, but they are also too complicated for the majority of the population to understand [65], and it is unclear whether/how an adequate understanding could be better supported [66]. As Barocas [9] notes, it may not be possible to provide explanations that are simple enough to be accessible and invite engagement while also providing enough detail for a user to fully understand the consequences of their information disclosure (a tension termed 'the transparency paradox'). Furthermore, investing in becoming sufficiently knowledgeable of the costs of information disclosure is itself costly, explaining a strategy of 'rational ignorance' (or purposely ignoring privacy policies) [36].

(2) *The unreasonable burden involved in the effort required to actualize one's preferences.* Another explanation of the privacy paradox is that even with good understanding of the consequences of information disclosure, people may lack skills to effectively manage their disclosure [36, 42]. This is not helped by the fact that services are constantly changing their privacy settings [42]. Furthermore, people tend to feel comforted when provided the apparent option to control aspects of their information disclosure, which perversely makes them less likely to exercise that control (a phenomenon termed the 'control paradox' [1, 13]).

(3) *The clear disincentives to preserving privacy.* The literature also cautions against viewing information disclosure (beyond preferred levels of privacy) as a failure to control information and/or preserve privacy, as there are social benefits to disclosure that may win out against the competing impulse to withdraw [36, 66, 103]. There are, as well, such strong incentives to using services that require information disclosure [40, 42, 99]—people are socially entangled [81] with services in their private lives and in their employment and/or education—that opting out of their terms of use is tantamount to opting out of society [86]. In practice, non-disclosure of one's personal data non-viable [49], despite regulatory framing of disclosure as a 'choice'.[1]

Hull argues that these challenges to privacy self-management represent a 'successful failure' [49], in that while consent regimes do not protect people's privacy, they transform that failure into a choice that is governed by the logic of market exchange. Having users click to accept terms of service reifies the illusion of choice, and 'legitimiz[es] nearly any form of collection, use, or disclosure of personal data' [97]. In addition, this practice 'habituates [users] into thinking that less privacy is what normal people want' [49]; and most insidiously, 'Even if that narrative is ultimately untrue, it has the further function of neutralizing and depoliticizing the distributional effects of treating users' information as sources of capital accumulation' (ibid). Ultimately, not only does this undermine privacy as a value, but it invites users to view this as 'the way the world works' (ibid). As Couldry and Mejias explain, people are compelled to enter, seemingly voluntarily, into 'data relations' [54] which 'make the appropriation of human beings' data seem normal, just the way things work' [17, p.12].

In this paper, we build on these critiques, exploring how people account for their use of online services in relation to a struggle to effectuate their privacy preferences even when provided information about a service's privacy policies. We argue (in agreement with van Ooijen and Vrabec [108]) that the assumptions GDPR makes regarding privacy decision making do not hold—specifically, we show that our participants do not really engage in privacy self-management, and consequently we argue that focusing on consent as a means for managing privacy is to obscure how morally accountable

[1] Richards & Hartzog [86] refer to this as the 'Control Illusion', not to be confused with the 'illusion of control' [13].

action is actually accomplished (e.g. in relation to social expectations [66]). Following from this, and building on prior work [56], we contend that consent (as implied by use of a service) should not be interpreted as being indicative of feeling satisfied with the privacy balance one has negotiated nor of trust in a service.

2.2 The Relationship Between Privacy and Trust

Irrespective of whether GDPR and privacy policies actually promote successful privacy self-management, it is worth considering their effect on trust in attempting to understand the relationship between privacy and trust—particularly given the recurrent argument for privacy protection as a trust promotion mechanism [18] and, thus, its critical role in maintaining a vibrant economy [110]. As a key headline, GDPR on its own has not promoted trust in data collectors [10]. Further, the mere presence of privacy policies may or may not have any effect on reported trust [52, 75], particularly since users often fail to notice these policies [30]; however, studies generally support the conclusion that people report trusting companies more when they are seen to respect privacy [29, 62, 113], and have greater trust in (and greater customer loyalty to) websites they believed securely handled their private data [33]. Even still, there is research showing that despite evidence of privacy violations and resulting loss of trust, people nonetheless find it difficult to discontinue use of popular apps [106]. Lastly, readability of privacy policies may or may not affect trust: While one study found that readability was positively correlated with trust [31], another found no such effect [84], though did find a positive correlation between trust and perceived control over privacy and perceived transparency of privacy policies.

According to the *privacy calculus model*, people's behavioral intention is to maximize their own benefits, so they will choose to disclose information in ways that gain them more than the risks of that disclosure. In Dinev and Hart's [25] highly cited configuration, willingness to disclose personal information is influenced on balance by: 1) one's personal interest in the internet (or, borrowing from Technology Acceptance Model parlance, the perceived usefulness of the online tool/service [20, 21]); and 2) perceived risk, which is moderated (negatively) by *privacy concerns* and (positively) by *trust* of the internet. Experimental studies have since tested these factors. A positive correlation has been found between trust and willingness to disclose personal information online [113]. While privacy concern has been shown to affect people's decision making around online purchasing [69] and disclosure of personal information [19], studies have also shown that 'privacy concerns are not a valid predictor of privacy behavior' [41]; nor is high distrust a predictor of more careful online behavior [67]. Research also suggests that trust may have a moderating effect on privacy's impact on behavior ('high trust compensates for low privacy, and vice versa'), but that information disclosure is not affected by differences in dispositional trust (i.e. tendency to trust) as much as by contextual cues [53]. Overall, studies have found a much stronger influence of personal interest / perceived benefits (e.g. benefits to be gained through personalization of content [5]) on people's intention to disclose information than perceived risk [36, 109].

The privacy paradox presupposes that people are, first, making *decisions* regarding their privacy, and secondly, that such decision making is *rational* [12]. Some have argued that the privacy paradox can be explained by bounded rationality [36, 93], i.e. that people's capacity for rational reasoning about and valuation of privacy (in cost/benefit terms) is limited and prone to miscalculation [1, 64]. Others, however, have questioned the core idea that people rationally negotiate 'privacy concern'. The crux of the privacy paradox lies with inconsistency between how much they say they care about privacy and what they do to protect it; and there appears to be some empirical evidence that people are 'privacy fundamentalists' in the abstract but 'privacy pragmatists' in context [112]. People's apparent inconsistency may stem, therefore, from the abstract nature of privacy [1]: Perceived risk is more salient to individuals when focused on hypothetical scenarios [34], but decision making in the moment is dominated by more concrete considerations. Phelan et al. [82], for example, propose that people engage different modes of thinking about privacy concern when directly prompted (System 2 thinking, rational assessment) versus when acting (System 1 thinking, intuitive assessment). Going even further, however, Crabtree, Tolmie and Knight [18] found that privacy practices *in situ* are not reflexively organized around a concern with privacy, but are instead bounded up with activities of managing relationships—specifically managing the intrusions of the digital into their every day lives, or as they put it, 'a concern to manage the potential "attack surface" of the digital on the manifold relationships implicated in their everyday'. What this shows is that while privacy may be a concern for people—they can, after all, talk about this concern—privacy is not necessarily a *practical concern*, or at least cannot be reasoned about independent of more complicated arrangements of practices.

As we will show, the results of our study resonate strongly with this latter perspective on privacy concern, revealing an incompatibility between the rationality implied by the privacy calculus model and the situated reasoning people engage in adopting digital practices that may have privacy consequences. We build on Crabtree, Tolmie and Knight's [18] insight to understand how people morally account for their competence in their privacy practices (which are typically habitual, routinized, and therefore unexamined) through a study design that deliberately throws their competence into question.[2] We further explore Tolmie and Crabtree's proposition that 'privacy is a matter of accountability management' [101], with the aim of understanding how trust is implicated in participants accounts of their privacy competence.

2.3 Trust-Motivation Theory and Hopeful Trust

As frequently noted in literature on 'trust', the concept is variously understood, with strong disciplinary tendencies to focus on particular types and/or dimensions (e.g., see [110]). The privacy calculus model, above, offers a narrowly doxastic account of trust, i.e. characterizing trust as (only) a *belief*—or more specifically, 'a confidence belief' [25]. By their own admission, Dinev and Hart [25] chose not to incorporate affective (non-doxastic) elements of trust which feature in other highly influential models of trust, such as Mayer, Davis and Schoorman's Ability-Benevolence-Integrity, or ABI, model [71] (even ignoring ABI within other explorations of online / e-commerce trust they cite [35, 74]). Corritore, Kracher and Widenbeck [16], in contrast, adopt a view of trust not as a belief, but instead an *attitude* 'of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited', and propose that trust is moderated by perception of credibility, perception of ease of use, and perception of risk (with perceived control being one of many external factors moderating perceptions of credibility, ease of use, and risk). Importantly, however, in speaking of 'risk', Corritore, Kracher and Widenbeck are not referring to privacy risks, but rather risks such as an online purchase going unfulfilled and online information being unreliable.

In challenging the rationality underlying the privacy calculus model (§2.2), we also suggest that trust is implicated in matters of privacy in much more complicated ways than the model accommodates—perhaps explaining the inconsistency in findings between studies. Renowned trust scholar Annette Baier argued strongly that trust is comprised of interlinked cognitive (belief-based), affective, and conative elements [7]—the latter encompassing 'judgments, decisions, intentions and resolutions which lead to a disposition to trust' [94]. Dinev and Hart's [25] model appears to treat motivation as a separate non-trust factor (namely, personal internet interest). This is problematic, as trust is rarely 'a straightforward function' [105] computed on the basis of evidence and/or trustworthiness cues (cf. e-commerce literature: [4, in [110]]). *Motivated cognition* helps explain certain instances of individuals trusting when 'rationally' they should not: As van der Werff et al. [105] explain, people may engage subconscious 'discrepancy reduction strategies' of discounting or downplaying evidence of untrustworthiness if highly motivated to trust, and vice versa. As Dinev and Hart [25] themselves

[2] Here we take inspiration from Tolmie and Crabtree's [101] analysis that technologies that 'breach the ordinarily unremarkable grounds of everyday activities' ... 'not only open up ordinarily unremarkable activities to unwarranted account but throw members' competence and autonomy into question by doing so'.

rightly note, the benefits to be gained through use of online services continues to increase; this would, ostensibly, create a powerful motivation to trust these services that may override more typically 'rational' processes. In our study, we explore how trust is bound up with matters beyond what is overtly presented by services themselves (*viz.* evidence of trustworthiness), and how motivation to trust drives participants' accounts of trust.

Even beyond motivated cognition, the phenomenon of *substantial trust* 'renounces the very process of weighing whatever evidence there is in a cool, disengaged, and purportedly objective way' [73]. McGeer (ibid) explores the character of substantial trust as a 'state of mind' (beyond mere belief), considering how people may, for example, trust a friend even in the face of damning evidence they have committed a crime. Substantial trust often requires that one feel (seemingly unreasonably) *hopeful* about the person in question. McGeer's key insight regarding hope is that it reflects an appreciation of the limits of one's own 'agential powers'—that one can only do so much to bring about the end they desire, and hope allows one to 'rid[e] out' worries and self-doubt; in short, it creates 'affectively charged scaffolding' for doing what one *can* do in the situation (ibid). We may think of hopeful trust, then, as a form of substantial trust which, being underwritten by hope, allows a person to reframe their own agency in a more positive light, to be empowered to act at all.

In this paper, we explore the role of hope, as opposed to strategic reasoning, in trust of online services. Like McGeer, we resist viewing hopeful trust as irrational; instead we argue that hope makes trust in online services (even those that violate one's privacy preferences) rational because it enables one to engage in the digital world despite practical difficulties in negotiating privacy. Our analysis explores indications of hopeful trust when a person is made to face the limits to their agential powers.

3 STUDY DESIGN

The study was designed to explore how individuals justified their continued use of digital services once they were presented with information that such services' privacy policies conflicted with their stated privacy preferences. To allow for examination of potential differences in responses between age cohorts (see §4, below), we recruited participants from an older adult population (categorized as aged over 65 years)[3] and a younger adult population. In total, 4 older adults (P1–P4; all retired) and 6 younger adults (P5–P10; all University undergraduates, 4 studying computing, 1 studying law (P9), 1 accounting and finance (P10)); 5 males (P1–P2, P5–P7), 5 females (P3–P4, P8-P10) took part in the study. Informed consent was obtained via a participant information sheet and consent form, and participants received a £10 voucher as compensation for their time. This research received ethics approval from Lancaster University.

Participants were interviewed individually by the first author. Half of the interviews took place in person prior to the pandemic, and the other half were conducted online using a video conferencing tool of the participant's choice. In all cases, the same interview protocol was used. This protocol involved the use of Qualtrics to step participants through three stages of the interview. In the first stage (page one on the Qualtrics survey), participants were asked to indicate which of a list of online services they use. The list included the following popular services: • Wikipedia; • Google / Android / Gmail; • Amazon / Prime Video / Echo / Dot; • BBC iPlayer; • WhatsApp; • Facebook; • Skype; • eBay (note: when a choice contained multiple services, these were covered by shared terms). A range of services was chosen in the hopes that all participants were likely to use at least one. The interviewer entered the selection for the participant if being interviewed remotely; but in all cases, participants were asked to elaborate on their responses, explaining their choice to use, whether their usage had changed over time, and their feelings about or beliefs toward the service.

[3] While 'older' is variously defined in the HCI literature [87], this categorization is aligns with the age British citizens (the study being undertaking in the United Kingdom) typically transition to retirement, marking a new stage of life [58] where one is freed from workplace obligations to use particular services.

The interview progressed (page 2 of the survey form) by presenting participants with a series of statements that were characteristic of terms they were likely to encounter in signing up for a service. Indeed, these statements were adapted from the privacy policies for the above listed services, as much as possible using their exact language to retain some of what makes these terms cumbersome, though shortened in some cases. Where two or more terms were in essence the same but used slightly different language between services, they were amalgamated, preserving as much of the original language as possible. There were 19 statements in total (order not randomized, see Table 1), with particular effort to choose terms that appeared across multiple of our chosen services. Participants were prompted with: *If you saw these terms for a service, would you agree or disagree to them?* They were asked to share their interpretation of the statements, and how strongly they felt—including whether any of these were 'deal-breakers', i.e. if seen in a service's privacy policy it would cause them not to use the service. After responding to all 19 statements, participants were given another chance to identify statements that they felt especially strongly about (indicated with bold font in Table 1).

These amalgamations may not have perfectly preserved the legal subtleties of these terms; but they suffice for prompting discussion around which terms were disagreeable to participants and how their willingness to use a service changed in light of awareness of a clash between their stated preferences and a given privacy policy. To explore reactions to these clashes, we included a reveal stage. The survey back-end linked the answers provided regarding services used to the terms for those services (as we interpreted them), and participants answers about whether they agreed or disagreed with those terms. The next page of the survey presented participants with an apparent clash, showing which terms they disagreed with were included in the privacy policies for the services they currently use: *There are conflicts with your stated preferences.* The interviewer then elicited reactions to services in the light of any conflicts, e.g. asking how they felt, what they thought the term meant in the specific context of the service in question, and whether this new information was likely to influence their use of the service in the future.

The interview concluded with a general discussion around data privacy, during which participants typically attempted to summarize their stance toward privacy policies and what kind of agency they felt they had in enacting their privacy preferences. The interview closed by informing participants that: *We did the best we could to link these terms to the services, but it's possible that we made mistakes. If you are concerned or interested in finding out more, we encourage you to read the privacy policy directly.*

4 ANALYSIS

At the outset, we were particularly interested in seeing whether older adults were more likely than younger adults to resolve a conflict between their privacy preferences and a service's privacy policies through discontinuance of the service; and also whether older and younger adults accounted for their intention to continue using services in different ways, e.g. the extent to which these drew upon normative expectations for technology use for their age cohort [57]. Once underway, our attention was drawn to the striking similarities between the accounts of old and young participants, in particular the fact that all participants were unwilling to discontinue using services they were already using despite an apparent clash. This is not to say that there are no interesting differences to unpack—having interviewed so few from either category, we cannot claim to have done a deep investigation of age-cohort differences. But having conducted 10 interviews, we paused to more closely examine here the interactions between our study design and participants' accounts of their decision making. Specifically, we became aware of how the 'reveal' stage deliberately raised questions about a service which are more typically backgrounded in users' interactions—indeed, it seemed to bring into focus questions of trust which might otherwise exist as a "'background condition" of ordinary action' [101] (see also [111]). If, for

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
1. We collect information and store this information with unique identifiers tied to the browser, application or device being used.	A	A	D	A	A	A	A	A	A	A
2. We collect personal information when you use our service.	D	A	D	D	A	A	A	D	A	D
3. We collect information on location data.	D	A	D	D	A	D	A	D	D	A
4. We use your data to troubleshoot, develop our services, measure how services are used, and test the safety and reliability of the service.	A	A	U	A	A	A	A	D	A	A
5. We use algorithms, automated systems and analyse the content of your data (some of this is done by third parties).	A	D	D	D	A	D	D	D	D	D
6. We share your personal information with trusted third parties for external processing (e.g. for advertising and analysis of aggregated statistics).	U	A	D	D	A	D	D	**D**	D	D
7. We use your information with social media sites you already use to tailor content.	D	A	D	D	A	**D**	D	A	A	A
8. We share your information if we believe it's necessary with regards to potential illegal activity.	D	A	D	A	D	D	A	A	A	A
9. Third party advertising partners may collect information about you when you interact with their content (this is governed by their own privacy practices).	D	D	D	D	D	A	A	D	D	D
10. We may retain your information as long as necessary, potentially indefinitely.	A	A	D	D	A	D	A	U	A	D
11. We share information with other affiliated companies when we learn of misuse or harmful conduct by someone using our services.	D	A	A	D	U	A	A	D	A	A
12. We collect information about others that you interact with through your communications with them; and others that you communicate with using our service may share your data.	D	U	D	D	**D**	D	A	D	D	D
13. We share non-personal data with researchers.	D	A	D	A	A	D	A	A	A	A
14. We collect information about people, pages, accounts, hashtags, and groups you are connected to.	D	A	A	D	A	D	A	D	A	A
15. We collect device information (e.g. operating system, hardware, behaviours performed on the device, device signals, data received through the device, network and connections).	D	A	U	A	**D**	D	D	D	**D**	D
16. We collect telephony log information (e.g, phone number, calling-party number, receiving party-number, time and date of call and messages, duration calls, routing info) and website activity information (e.g. duration).	D	D	D	A	A	D	D	**D**	D	A
17. We collect information on purchase transaction (e.g. card number, other card information, authentication information, billing).	A	**D**	U	A	A	A	A	A	**D**	**D**
18. Facial recognition software is used to recognise you in photos, videos and camera experiences.	D	A	D	**D**	D	D	D	**D**	A	D
19. We use content that you share or upload (for example we may copy and redistribute that content until deleted by you).	D	D	D	D	D	A	A	D	D	D

Table 1. Participant preferences; A=Agree; D=Disagree; U=Unsure; bold **D** indicates a 'red line' (i.e. 'If a service included this term I would not use the service') or strongest possible disagree.

example, the service in question is *trusted*,[4] raising questions about its trustworthiness (with respect to its 'competence

[4] We do not claim here that *using* a service is equivalent to *trusting* a service—a point we elaborate later in the paper.

and willingness' [6] to look after the data entrusted to its care) in effect forces the participant to creatively justify their trust of that service—all the more so if they had earlier in the interview elaborated their especially strongly held stance about one of the terms of service only to then find it to be a term stipulated by one of their 'trusted' services. On the other hand, if the service is *not trusted*, raising such questions somewhat implicitly raises the follow up question of why the participant is using the service (i.e. do they trust it in *some* sense?).

Given the above ways our study design engaged participants in 'practical reasoning' [46], we adopted an analytical perspective suited to the examination of that reasoning, focusing on how individuals *present themselves* to the interviewer (their moral standing being at stake in the interview), and through their linguistic accounts *make sense* of their practical actions [100]. More specifically, we adopted a 'specimen perspective' (as opposed to 'factist perspective'), which is untroubled by participants' possible 'confabulations'; such confabulations are relevant to how people present themselves and thus do not invalidate the data [100]. This means that we need not be concerned here if people's accounts of their decisions hinge on seemingly incorrect interpretations of the statements drawn from the privacy policies (or our misrepresentations of them); nor that articulation of accounts in the interviews may be distinct from how decision making plays out when an individual is faced with privacy policies *in situ*. Our approach to the data draws from the ethnomethodological tradition, involving immersion in the data without commitment to any particular formal method of analysis, with the aim of producing descriptions that make 'real worldly activity mutually intelligible' [83]. This is to say we did not use a formal coding process, e.g. the use of code books, nor did we seek to validate our interpretation of the data through inter-rater reliability—described by Lynch as 'taking up a gratuitous "scientific" instrument' [68]. Ethnomethodology is 'indifferent' to such formal approaches, and derives inferences through ordinary communicative faculties, by making sense of what participants say. In terms of the practical activity of analyzing the data, author one used the comment function in Word to mark up interview transcripts with thoughts provoked by specific passages; author two responded to these thoughts also using comments; and this was followed by email-based discussions about our evolving interpretation of the data.

This approach focused our analysis on questions of how individuals praxeologically account for their reasoning about privacy, what their responses communicate about how they see the world (what they see as 'rational social behavior' [26]), and how people 'make moral sense of themselves' [44]. Trust was explicitly raised in some instances during the interviews, almost always unprompted; but most often it was *morally implicated* in participants' accounts in various ways that are under-examined in extant literature on privacy. The applicability of the notion of 'saturation' is questionable for our chosen analytical approach [90]. Our 10 participants provided ample accounts for developing our theorization of the relation between privacy and trust, while still leaving open the opportunity to further probe aspects of this relation through follow on studies.

5 FINDINGS

We present our findings in three stages, as follows. In section §5.1 we consider how participants reason about matters of privacy and trust. Participants' accounts reveal that they struggle to articulate privacy concern with respect to privacy policies. This finding not only undermines the explanatory power of the privacy calculus model [25]; it also contradicts notions of trust in online services as *contractual* in nature (e.g. as implied by Culnan and Armstrong [19]), with explication of privacy policies facilitating contractual trust. In section §5.2 we explore the different ways that participants account for what they are giving away when disclosing information, and how these accounts differentially articulate the moral probity of their (continued) use of online services. The findings show that privacy does not actively feature in consent; instead, consenting to the terms of online services is a routinized practice: The decision to use a service is bound up with other (non-privacy related) morally accountable action, and consenting remains accountably reasonable, and routinized, in the absence of evidence of privacy-related harms. In section §5.3 we return to the character of people's trust in online services, if not contractual. We find evidence, instead, of *hopeful trust*, which on the one hand enables participants to make moral sense of their (continued) use of online services in the face of severe limitations in effectuating their privacy preferences, but on the other hand exposes them to greater risk of betrayals of their privacy.

5.1 Struggles articulating privacy concern

Data collection does not necessarily on its own raise privacy concerns [79], and by participants' own accounts, there is an important difference between disclosing information and compromising their privacy. Even still, participants recognized that disclosing enough information can have privacy implications; and in accounting for their continued use of services whose privacy policies contained terms they stated they disagreed with, every participant made a point of minimizing the amount of information they gave to these services. For example, in speaking about Google, P1 explained, *'I just don't use it unless. . . I occasionally use Google Maps, I have to confess. . . And I suppose I don't care that much if some distant body knows that I've been walking in The Dales or something.'* P8 explained of Facebook, *'I can use Messenger without having Facebook, and even then I barely use Messenger, I just use if for the groupchat.'* Likewise, in responding to term 5, P6 stated: *'I certainly wouldn't put any information on a site that had that clause. . . So if it's something like, for example, Facebook I will only use that for receiving things, like group posts or Messenger. I won't actually, I don't make posts on Facebook.'* And P9, who was strongly against the collection of location data, spoke about using location tracking only briefly when absolutely needed: *'say for like 10 minutes, and then I'll turn it off.'* While participants conceded that they could not always control the amount of information disclosed to any given service, their accounts would minimize the number of trust relationships they entered into. As P3 put it, *'You know, your privacy is part of your identity and you don't disclose everything to everyone you meet. You're selective. And I said, I don't have apps from here, there, and everywhere. I have, like, handfuls of apps, you know, that I [use].'* P8 explained a similar strategy: *'With Amazon, it's just a compromise, really, because if I just reduce the amount of services that I allow doing that then there's less of a web.'*

We could interpret the above as participants demonstrating privacy competence through inventorying the ways they mitigate risks entailed in using services (elsewhere termed 'compensatory calculus' [59]). But prior research has shown that people regularly disclose a lot more about themselves than they realize [1]. Whether they do, in fact, undertake the controlling work they are describing, the salient point is that in accounting for their information disclosure practices, participants made a point of emphasizing actions that helped them create certain conditions for 'sensible trusting' [8] *despite* disagreeable terms in a service's privacy policy. And yet, even while generally presenting themselves as confident that they are not sharing more information about themselves than they are comfortable with (*'I'm quite careful with what I put online'* [P8]; *'I just think if there's a risk like, I wouldn't want to put myself in that, so I just limit that a little bit'* [P9]), participants also admitted that the privacy implications of their data disclosures are not always accessible to them as a user: *'I actually don't know the implications of giving that data away'* [P10]. Participants had wildly different interpretations of the meanings of the privacy terms we presented them, and expressed particular difficulty in translating these terms into risk or privacy concern. The study design undoubtedly contributed to this, as participants were initially presented the terms out of context (see §5.2); but even when later linked to specific services, participants were still confused as to *'why an application would need'* [P8] the data they were asking for: *'it's just like why do they need it'* [P9]? In some cases, participants were so surprised to learn that services they used conflicted with their privacy preferences that, instead of acknowledging that the service violated their privacy preferences, they proposed that perhaps their interpretation of the term was incorrect. For example, in learning that WhatsApp's policy allowed them to collect information about interacting partners (term 12), one of P5's 'deal breakers', he responded, *'That I was not aware, and I'm still not sure it means exactly what I think it means.'*

Overall, the data showed that participants struggled to make moral sense of their information disclosure (i.e. with respect to the boundaries they were setting around their privacy) due to the lack of explicitness of privacy policies. For example, when asked whether she agreed or disagreed to term 14, P8 responded:

> *'It depends on what they're collecting it for. I'd say no, because, just because of that. If they're collecting it to recommend me things, no. If they're collecting it to distribute, no. If they're collecting it generally just keep it on store so I could access what I've done, yeah.'*

P2 also explained that it is not clear to a user from these terms what can be gleaned from the different bits of information they disclose to a service:

> *P2: 'I think if people were– if it was put back to people and said, "Okay, you've told us this, this, this, and this," and shown people, "can we keep it?" Then I think a lot of people would say, "No!" But it's when it's, you know, like this [a list of terms] where it hasn't got a meaning, really. . . it's people not realising what they're giving away. It's all wrapped up in a sort of a phrase rather than itemised.'*

As P5 said, *'It's just I just feel like they could exploit you somehow since you don't know what you're agreeing to.'*

Our participants' accounts suggest that they do not fully understand what vulnerability they are entrusting to the care of these service providers or what harms might arise in different scenarios relating to the service provider's handling of the data (or 'contingencies', to use Baier's [6] phrasing). This has important implications regarding the nature of this trust relationship, as it means that while privacy policies have the appearance of a formal contract, both in their particular turns of phrase and in functioning to extract user consent, they lack an essential quality of contracts: *viz.* making 'explicit provisions for such contingencies as we imagine arising' [6]. The question we answer in §5.3 is, if this trust relationship is not, then, *contractual* in nature (i.e. with these privacy policies establishing mutually agreed grounds of accountability), how might we characterize the trust participants had in these services?

For now, we note that in contrast to how difficult it was for participants to articulate the privacy risks of their information disclosures, they had no difficulty at all articulating the benefits of services they used, and this may explain why information disclosure behavior is much more strongly influenced by perceived benefits than perceived risk [36, 109]. The question we turn to next is to what extent this should be characterized as a form of privacy calculus.

5.2 Differential accounting

During the interviews, it was apparent that participants struggled with the task of agreeing or disagreeing with the terms we presented them stripped of context. For example, P1's response to term 1 was, *'I suppose that would depend on how much I trust the particular body, wouldn't it?. . . Or how much I wanted to use it'*; and in trying to decide how to respond to term 10, P9 said, *'I probably, I'd want to disagree. I really would but then I think I would agree. . . Depends how much I want to use the application [laughs].'* And indeed, for services they found useful, participants were willing to tolerate violations of their stated privacy preferences:

> *P1: 'I would happily do all that [consent to disagreeable terms] with Wikipedia. . . I consider nowadays Wikipedia is such an important part of my life, I wouldn't, I wouldn't do without it.'*

> *P3: 'Amazon is sort of like my left hand. I need to use that. So of course, they got all that data about me.'*

> *P7: . . . [Facebook] do have some really not okay practices that they get away with and I'm less happy with that. But at the same time like I'll use the platform because it's so useful to me personally.*

When presented with a conflict, participants seemed unable to justify their abstract opposition to terms if they could not point to any harm having come from use of services whose policies contained similar terms. P9, for example, considered her feelings on Google's policies clashing with her previously stated preferences:

> *'Um, I don't like it. Yeah, I don't like that, but, I think it's more– It's one of those things, if you're using these applications and you actively keep getting, say, hacking attempts or someone like cold calling or something like that, you would sort of notice that it's linked to the application and you'd probably stop it. But the fact that you rarely ever get things coming back at you, in that sense you sort of, I don't know, you don't like it but you think well, there's not too much hassle with it.'*

And P7 accounted for continuing to use Amazon and Google despite multiple clashes with his stated preferences as follows:

> *'Like I know whenever I use a website like Amazon and Google it's like, "They're tracking me, great [sarcastic]." Again, I've never experienced like a negative effect from it, it's just something that like if I think about it too much I'll go, "Ugh, damn it!"'*

But further, the fact that these services were, evidently, not using the data they collected in ways that harmed them made it easier for participants to conceive of benign interpretations of these *'open ended'* [P7] terms. For example, P10 disagreed with the term about collecting information about others she is connected with (term 12) *'because I fear they'll be spying on my conversations with others, and that's an invasion of privacy for sure,'* but her response to learning that WhatsApp did so was:

> *'Yeah, I mean, in a way, it's kind of justified because they actually do need the data for me for to connect one and another. Like, as they're like, yeah, . . . it depends on the intention, on how to use that data and what they want to use that data for. If there's really no other way around it, I would say yeah, I would definitely say yeah.'*

P6 similarly qualified his abstract opposition to indefinite retention of his data (term 10): *'I would disagree with that. But I know for technical reasons you'd probably just have to agree with it. I know plenty of services for actual technical reasons have it, it is difficult to actually remove user data just because the structure of their databases.'* Having discussed the potential of these services to abuse their privacy (and seemingly choosing instead to use the data to deliver functionality) might even have validated more well established trust relationships with these services; at least, participants did not respond to revelations of conflicts with services they used with statements such as, 'Now I don't trust them.'

On the other hand, there were a number of services people used that they readily admitted to distrusting, and revealing conflicts with their stated preferences only reaffirmed their distrust. As P5 explained, *'I mean, in general [the term] just seems really scary and then when you put when you put the app's name to it you realize, oh I already knew I was accepting that anyway. . . I mean, Facebook. Everybody knows about them and data sharing.'* Many participants were unmoved by the study's 'reveal' stage; their accounts focused less on how they could justify continuing to use services that appeared to violate their privacy preferences and more on why they were using services they did not trust. In particular, and in agreement with Palen and Dourish's observation of privacy 'as a social phenomenon' [81], participants described being socially entangled with services (see also Hargittai and Marwick [42]). P8 stated, *'Honestly, if it wasn't for the fact that my [work] rotas were put on Facebook, I wouldn't have it.'* Despite not liking some of what Facebook are doing, P4 emphasized the essential role it played in maintaining a sense of closeness with extended family: *'I'm not going to stop using it because as I say, [for] the first time in my life since [my grandchildren were] very small children and you could see them, that I actually get to know what they're up to.'* Also in regards to Facebook, P6 indicated he felt the choice of whether to use Facebook was essentially made for him: *'If I had the option, if nobody else is using Facebook, then I also wouldn't be.'*

Participants also noted how the pandemic intensified their dependency on these services. Speaking about Amazon clashing with two of his preferences, P7 justified continuing to use Amazon because, *'like there isn't really a major alternative... like I can't just walk into a John Lewis store or like nearby ASDA or Argos and go, "Hi, can I get this?"'* Even when posed as a general question, how she felt about privacy policies now having done the interview, P10 responded:

> *P10: 'I would still use it.'*
> *Interviewer: 'Yeah.'*
> *P10: 'Mainly because like this is such a peak time to use technology.'*
> *Interviewer: 'We can't not use it.'*
> *P10: 'And there's no other. Yeah. We can't do any social interaction face to face. Yeah. I would still use it, definitely.'*

These accounts suggest that participants were not, in fact, actively weighing risk, calculating the value of the privacy they are exchanging, or examining evidence of the trustworthiness of the service; rather, participants recognized compelling reasons to enter into trust relationships with services which rendered moot the examination of their 'beliefs and/or expectations about others and about the risks involved' [15]. In fact, they remarked upon the futility of even engaging with deliberations on privacy concern: They noted their inability to selectively reject terms within privacy policies, very much seeing them as bundled and even essential to the functionality they desired. For example, responding to conflicts with Amazon's terms, P8 explained, ... *'as much as I would like to have them, you know, to be able to turn around and say no [to a given term in a privacy policy] and still use the service, I can't.'* P9 said, ... *'just sharing data in general I wouldn't be like happy about if I could like not share it I would.'* P5 said, *'Honestly we'd like it to be disagree with everything, but we know we're not going to get anything if not [if we don't accept the terms].'*

The data generally supports Draper's observation of 'resignation' to some degree of privacy violation [27], and Hull's thesis that the inability to make meaningful choices about their privacy habituates users into thinking perhaps privacy doesn't matter so much [49]: In the interviews, participants provide 'accountably sufficient' [44] justifications for their actions through reference to what they present as a shared 'common-sense world' [95] in which users routinely give away more than they are strictly comfortable with—there being no privacy online (see also Phelan, Lampe and Resnik [82])—and in which it makes little practical sense to concern oneself with this state of affairs. For example, while P4 said of term 9, *'I don't really agree with that,'* she added, *'But I know it will happen.'* P5 discussed his dislike of being *'tracked'*, but conceded:

> *P5: But I know, it's just kind of inevitable almost. So that's why I agree to it.*
> *Interviewer: OK. So in an ideal world, I guess you would you would prefer that they didn't?*
> *P5: Of course.*
> ...
> *P5: Like I said, most of [these terms] I feel like we already agreed to like all of these things, but we don't know it. But obviously speaking in a– if I was to actually read that [policy] every time, and I was to see that and it wasn't an app that I was a hundred percent required to have, I probably wouldn't accept that.*

In this sense, privacy (the preservation of it) does not have the character of strategic decision making. As P9 explained of Google, for example, *'like I kind of have to use it, . . . [and] you just sort of do.'* One is merely getting on with life in the modern world (see [43, p.313]), using appropriate tools as needed, and paying the cost of use with whatever data is demanded of them. Information disclosure is 'routinized' [24], taken for granted as a premise of action (i.e. being able to use a service).

This begs the question, then, whether trust is any more pertinent to the matter of providing consent. In the next section, we explore the relationship between privacy and trust in apparent privacy paradox circumstances. We propose that trust can be bound up with matters other than a service's handling of privacy; and that although this trust may not overtly feature in decision making, it is key in enabling people to make moral sense of their information disclosure.

5.3 Hopeful trust

The discussion above provides ample evidence that, in Baier's words, 'We can still rely where we no longer trust' [6]. We observed this most in responses to the 'Big Five' tech giants, where participants described relying on these services despite distrusting them (e.g. *'I don't like it, but then I do think Google, like I kind of have to use it, there's no other, really, alternative'* [P9]). And yet, while there is an element of reliance in the accounts, there are hints that participants are not *merely* relying, but indeed *trusting*—or at least, trust has explanatory value when morally accounting for their information disclosure.

While participants at times indicated they lacked confidence in their own abilities in preserving their privacy, they expressed (arguably unjustified, or *hopeful*) confidence in the capabilities of others in managing matters of privacy. For example, P1 explained that he trusted his daughter-in-law to tell him which services were okay to use; and in accounting for his use of Amazon stated, *'She doesn't stop me from using Amazon, particularly when it's giving presents to her kids.'* We also noticed some hedging in participants accounts—that even if they distrusted the service provider, they trusted that certain forces were functioning to keep them honest. Participants cited the power of the masses to sanction companies that violated trust through social media take-downs. P7 explained:

> *'I think I trust Amazon overall because like if they were to try something, something underhanded, like I always have the ability to turn around and go, "You WHAT?" and like, have some, like kick something up. . . The thing is, there's always someone watching, especially with companies like Amazon.'*

P9 explained similarly:

> *'[Apple] are such a big company, that they have so many people that they couldn't possibly do anything that's that bad otherwise they'd have so much backlash, that you sort of trust it in that way. So like if they did breach anything or anything, then you think that everyone else is doing it so if there was an issue, everybody else wouldn't be happy with it.'*

Likewise, P3, who confessed she is *'not techy enough'* to determine for herself what ought to be trusted, found it easier to trust these services on the basis that others were paying close attention: *'But the lovely thing for me is, there are people with skills that I don't have that have these same concerns.'* In the words of P2, *'You can marshal small armies these days.'* Believing, or perhaps *hoping*, in the latent power of these armies of angry customers (none actually provided examples of these armies in action) made it easier for participants to *'sort of trust them a tiny bit'* [P9], thereby justifying their continued use of these services in moral terms beyond reliance.

It was also evident from these accounts that participants trusted service providers to not do anything that would violate GDPR or other laws.[5] P9 explains, *'they would suffer the repercussions if people's data did get lost. Like it would be such a big thing and they'd have, they'd be like sued so much, like millions, or billions.'* P6 suggests that they can be trusted with purchase transaction data because, *'they're probably subject to very strict laws on what they can and can't do.'* And P7 explains that having a computing background and awareness that *'they're not going to be allowed to do certain things'* makes him *'more confident with giving them certain things… because I know that they would get done for like GDPR, like under the law. Like if they're storing things that identify me as an individual to my computer and what I do that would be illegal.'* Several also extended this logic from law to ethics, stating that they trusted service providers to be careful not to anger or alienate their customer base, and therefore not do anything to cause too great a harm to users:

> *P2: 'And I think, with the bigger companies, they tend to be pretty good about– they're protecting an asset, their customers, from leaving them, they don't want the customers to leave them, so they tend to be pretty good at recognising– 'cause more people will complain about something and they seem to react to it when they know that "we're putting our jewels at risk here."'*

This was a surprisingly common rationale (and is consistent with Lau, Zimmerman and Schaub [61]), though it seems disproven by these same participants' admission that a violation would need to be extremely egregious to make them stop using the service. This logical disconnect suggests an element of hoping beyond reason, with that hope being the mechanism that enables trust.

We also found that participants' accounts frequently acknowledge disagreeable terms in privacy policies as *'the price you pay'* [P2] in contemporary society: *'You just have to compromise'* [P3]; *'… you've got to accept it or else we've got to change, go back to slates'* [P4]; *'… at the end of the day, nothing's ever free'* [P8]; *'… you're using the service for free, buddy, they're gonna take something back'* [P7]. In part, these admissions emphasize their 'structural inferiority' [39] and, thus, the limits of their own agency. In the words of P3, *'I'm the little person who's like smaller than an ant beneath their feet.'* And given that *'we can't really stop these people from taking your data they shouldn't'* [P8], participants described coping mechanisms to reduce mental distress. P3 termed her coping strategy *'planned ignoring'*:

> *'… it's a bit like my eyes are open, but in my ears I'm going doo doo doo doo doo doo doo like that with my fingers in my ears… cognitively, I know; emotionally it presses a few buttons; but this is life, and I'm old enough to know that success in life is dealing with the crap that life throws at you and surviving it and being adaptable… it's like lots of unpleasant things in life. You just, can just put them on the back burner, like a parrot on your shoulder. You know they're there, occasionally things will happen and it squawks in your ear. But most of the time you're just aware and it's resting. That's the way I look at it.'*[6]

This appears to go beyond 'rational ignorance' [36] of privacy policies, however. The above extract reveals a desire to 'act as if we are sure while we actually are not' [55] when using digital services, closely resembling Keymolen's characterization of trust as 'a functional fiction': 'When we trust, we set aside possible bad outcomes and act instead' (ibid). In other words, without this *'planned ignoring'*, P3 might not be able to adopt any of these services that she otherwise finds so useful.

The clearest example of hopeful trust was described by P2, who explained his inclination *'just to trust'*:

[5] This is not necessarily the same as believing these laws provide adequate privacy protection.

[6] We note as an aside that this would seem to align with an understanding of rationalization as 'performative pretense' [22], with some awareness of pretending.

> *P2: Yeah. I don't have a problem with most of these things, because I just believe the whole world works in mostly an honest way. And if somebody really wants to get the things to harm you with, they'll have to do a lot of work, probably, to get it. It's easier just to trust people… I just remember– I know it's funny, but I watched a film many years ago, probably twenty years ago, he was a bit of drunk this chap in the film and he had his arm around somebody at the bar and he just said, "I just trust people. It's easier that way." And I thought about that, and I kind of tried it out in a few situations and I thought, "Yeah it is!" Mostly people are trustworthy. So I decided to adopt that policy.*
>
> *…*
>
> *P2: 'I mean, I hark back to a shipmate of mine when I was in the navy back in the 60s and he used to just say, … "If it matters it matters; and if it doesn't matter, it doesn't matter." … It's knowing the difference, and what it means to you. But yes, I used to hang on to lots of stuff. And it wasn't good for me. Because I kept feeling anxious. And end up on some little pills and beta blockers and things like that.'*
> *Interviewer: 'Yeah, so you can trade the constant anxiety for potentially higher vigilance over small things which you maybe might not even be able to influence anyway. Or you can opt for just general wellbeing and you're at the same risk you were before to any of these.'*
> *P2: 'Yep. And I opt for the general wellbeing.'*

While not everyone claimed to actively choose trust over worry in this way, they hinted at some awareness that, on the one hand, *'Nobody does really [control or oversee what these big tech companies do]'* [P6] and *'I probably shouldn't trust them'* [P9], and yet, *'I actually do [trust them]'* [P3]. As P5 explained, facing real barriers to *'understand[ing] what exactly I'm accepting here… makes it easier to remain ignorant and just be like, oh, I'm sure it's fine'*.

We propose that hopeful trust is a perfectly logical means of enabling one to continue to do the best one can reasonably do in navigating the digital world in the absence of more robust assurances of their privacy. The study design forced participants to directly face the 'limits to their agential powers' [73], to face privacy concern in a way that they generally background in their use of digital services, and in presenting themselves as competent agents in the interview, participants staked their service use and related information disclosure (which was at odds with their more abstract ideals about privacy) on their ability to trust these services.

While this hopeful trust appears to serve an important function for individuals, we wonder whether hopeful trust also functions as a moral pressure valve for resolving the contradictions of consent which contribute to the privacy paradox. Baier [6] questions the casual assertion that good things thrive in conditions of trust, and by extension more trust is always better; and she makes the point that, 'Exploitation and conspiracy, as much as justice and fellowship, thrive better in an atmosphere of trust'. Trust relationships between 'the powerful and less powerful' (ibid) are typically inclined toward dependency and, with that, exploitation. As the interviews show, participants felt they had little freedom to exercise choice, which makes it all the more problematic that one is forced to rely on services without strong assurances of their trustworthiness. We suggest that hopeful trust arises because existing approaches to privacy self-management do not adequately attend to the dynamics of dependency, but that hopeful trust may in turn allow for the continuance of the very conditions for privacy violations to thrive—that is *unless* it is recognized as a strong signal of a desire for privacy preservation.

6 DISCUSSION

Contradicting prior work that suggests a competitive advantage for companies that handle customers' privacy ethically [19], this study reveals that there is effectively no penalty for a service that violates users' stated privacy preferences. Even when made to face discrepancies between these preferences and the policies of specific services, participants were unwilling to discontinue use of the services. We note the prevalence of a similar logic surrounding trust: e.g. Goldberg et al. [38] argue that 'Companies will need to start building systems that show their interest in behaving ethically because only then will they be trusted.' Our study challenges this reasoning, as people are able to find reason to trust services they feel they need to use. By extension, any claims of the instrumental value of privacy protection or indeed trust—a seeming vestige of a disproven logic that the market will guarantee freedoms without need of regulation [3]—are critically undermined by the finding that the bigger and more useful a service is, the more untrustworthy behavior they can get away with without losing customers.

Our point is not that trust is less relevant to privacy than scholarship has supposed; quite the opposite. While 'privacy can and should be thought of as enabling trust in our essential information relationships' [86], the current regulatory apparatus appears to be driving a wedge between these concepts—a sign that it is fundamentally broken. Specifically, privacy policies do not appear to be maintaining, let alone *promoting*, trust: Participants' accounts do not hinge on the trustworthiness of these privacy policies; rather, their accounts more or less sidestep the specifics of these privacy policies in morally accounting for why they are choosing (in some ways, beyond 'reason') to trust certain services. We find ourselves in agreement with Richards and Hartzog [86], who argue that 'modern privacy law is incomplete' because, in focusing on avoidance of harm, it fails to account for trust as a substantive value, a prerequisite of a flourishing society. Succinctly, they contend that *'privacy matters because it enables trust'* (ibid; emphasis added)—or at least this would be a basis for a healthier dynamic, one in which individuals can use digital services without concerning themselves with privacy self-management. This would require, however, that the law be written to recognize the implicit *promise* made by service providers to their customers and enforce consequences of betraying trust similar to those of committing fraud; and to emulate fiduciary law, which prevents against 'self-dealing at the expense of the entrustee' [86] (for example, by profiting off uses of customer data at the expense of their privacy; see also, [96]). This further entails the need for a shift in the tenets of privacy law from non-disclosure to 'discretion'; transparency to 'honesty'; security to 'protection'; and introducing the concept of 'loyalty'; in short, the 'rejuvenation' of Fair Information Practices [86], which gave way to contemporary consent regimes such as GDPR.

But what might the role of HCI be in bringing privacy and trust into more benefic alignment? A major area of focus in the field has been supporting individuals in making 'better' trust decisions[7] [64], including: automatic simplification of privacy policy language [11], visualizing an app's data collection and data sharing activities [77, 106, 107], and providing 'actionable choices' to better exercise control [91]. These approaches assume, we think incorrectly, that people make privacy *decisions*. To the contrary, our findings suggest that privacy may not even feature as part of people's reasoning in circumstances where they provide consent. In that case, what of solutions that automatically recommend [63] or delegate responsibility for making consent decisions to a third party (trust proxy) more informed on the matter [78]? We would argue that these kinds of approaches take for granted the notion of consent as a valid and ethical starting point for ensuring privacy. Aligned with critiques emerging in the medical field (e.g. [32]), in this paper we challenge the very notion of consent as being related to strategic decision making around privacy or trust (importantly: as opposed to being undermined

[7] While there is a longer theoretical discussion to have regarding how to evaluate 'good trusting' [14], it is our position that hopeful trust is a pragmatic stance that clearly makes sense, so could therefore be considered 'good'.

by ‘impediments to rational decision making’ [97]), thus fundamentally questioning the moral basis for consent as a tool for ‘managing’ privacy.

While this does not lead neatly into a set of actionable design recommendations, it points to some high level design aims for HCI. The first of these would be the need for structural protections for those entrusting themselves to services. We concur with Acquisti et al. [1] that ‘a goal of public policy should be to achieve a more even equity of power between individuals, consumers, and citizens on the one hand and, on the other, the data holders such as governments and corporations that currently have the upper hand.’ Though occasionally doing privacy damage control, by their own accounts our participants were not engaging in privacy self-management (concurring strongly with Crabtree, Tolmie and Knight's discussion of people instead managing the potential ‘attack surface’ they present online [18]); rather, their accounts suggest they respond, *reflexively*, to the usefulness of the service offered. (Bearing in mind that our study forced participants to consider their decision making, we should assume that in their everyday lives, ‘decisions’ to use, if we can call them that, are largely habitual and firmly rooted to the accomplishment of a given task.) If users are unable to leave these services, if market forces do not apply as a check against the service's power, then what is going to keep these services honest and serve as a bulwark against the erosion of privacy?

It could be argued that what is needed is the development of some kind of apparatus whereby people can exercise their mundane competence as effectively online as offline. Our intention is ultimately to stimulate debate, though we have doubts about the feasibility of such an apparatus. People are demonstrably capable of employing a battery of practices and techniques for managing privacy and trust in their everyday lives (say, within interpersonal relationships), but when interactions move online, these ordinary competencies can no longer be so easily exercised [101]— online relationships are just qualitatively *different*: less richly colored, more at-a-distance.[8] Our study gives cause for concern about the consequences of leaving the individual as the ‘sole gatekeeper of [his/her] welfare’ [9], at least until a new user sensibility for managing privacy and trust co-evolves alongside a new sensibility for designing technologies that prioritize privacy and trust.

We propose, therefore, that stronger protections are needed to ensure that when individuals use online services they are not risking their privacy. In seeking to enhance safeguards, individual autonomy can and should be respected through democratic deliberations with the public regarding their privacy preferences (see, e.g., methodologies of informed public dialogue by The Ada Lovelace Institute [50, 51, 102]; also Hartman et al. [45]). This study really underlines that these preferences should be uncovered through consultation, rather than assuming that what people are willing to consent to maps to their actual preferences. HCI is well-placed to make important contributions to the development of appropriate methodologies for linking individuals' (various and differing) privacy preferences to an emergent set of norms; translating these norms to the technical practices of the services (not necessarily the terms of the privacy policies); developing a framework for managing privacy trade-offs at multiple scales and contexts; creating standards that can be enforced; and devising (and evaluating the impacts of) interventions to preserve privacy. A potential indicator of the impact of such a substantive change of approach to privacy would be whether and how the character of trust changes from ‘hopeful’ to something more like ‘confident’.

7 CONCLUSION

This study affirms much of what is known about privacy, *viz.* people struggle to understand the terms in privacy policies [88] as well as the potential uses of their data [72]; they are more protective of privacy in the abstract [1]; people disclose

[8] Do certain trust mechanisms even apply online? It is interesting to consider, for example, whether hopeful trust can possibly elicit trust-responsiveness—i.e. a desire to live up to the trust others place in oneself—in trusted services as it does in trusted parties within interpersonal relationships [73].

personal information to services considered 'socially relevant' [99] (also [81]), and they continue to use services deemed useful despite inconsistencies with their privacy preferences [106]; they resolve discomfort regarding the collection of personal data [37] in part through a 'bandwagon heuristic' [98] and in part through a logic of free market economics [3]; they in fact do care about their privacy and try in their way to protect it [70], though they also feel they have little choice but to consent [27, 47, 104, 114].[9] There is, arguably, still value in showing how these are drawn together in participants' accounts, though our primary contribution is revealing the complicated relation between privacy and trust. People have a strong motivation to trust—driven by the usefulness of services, their broad social entanglements, and the restrictions these create on people's freedom to avoid/discontinue use of services. This trust motivation strongly influences people's moral reasoning about their information disclosure behavior, which is ultimately justified through hopeful trust in services with which one is inextricably bound. Thus, in the face of practical challenges to informed consent (as required of GDPR, Article 12), hopeful trust neatly absolves the individual of having to engage in a task they are unlikely to succeed in, namely privacy self-management. This does not mean that privacy concerns disappear (participants can express these concerns when asked about them directly); it simply means that such concerns must be backgrounded to be able to get on with daily life, and therefore are not salient to decision making about whether or not to use a service. In this sense, we might say that *hopeful trust enables the privacy paradox*.

This backwards relationship between privacy and trust indicates that something is awry—privacy *should* enable trust (and well-placed trust, at that). In failing to design regulations that protect individuals' privacy by default, and placing an unreasonable burden on individuals to protect their own privacy, the only way for most individuals to function without constant worry is to choose trust, to *hope* that this trust is well-placed. The only way to *un-paradox privacy*, then, is to create conditions for well-placed trust in digital services by ensuring that these services respect the high value people place on their privacy so that people's trust is grounded not in hope but in a confident expectation of trustworthiness.

8 ACKNOWLEDGMENTS

This research was supported by the EPSRC as part of the funded project PACTMAN: Trust, Privacy and Consent in Future Pervasive Environments (EP/N028228/1) and received ethics approval from Lancaster University's Faculty of Science and Technology Ethics Committee (approval number FST18139). We thank Mateusz Mikusz for help in designing the study and interpreting findings, Richard Harper for his guidance with early drafts of this work, and our participants for taking part. We would also like to thank the reviewers for providing such helpful input to the paper.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. Science 347, 6221 (2015), 509–514.

[2] Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers 6. Springer, 36–58.

[3] Philip E Agre. 1999. The architecture of identity: Embedding privacy in market institutions. Information, Communication & Society 2, 1 (1999), 1–25.

[4] Studio Archetype. [n.d.]. Sapient, & Cheskin Research.(1999). ECommerce Trust Study ([n. d.]).

[5] Naveen Farag Awad and Mayuram S Krishnan. 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS quarterly (2006), 13–28.

[6] Annette Baier. 1986. Trust and antitrust. ethics 96, 2 (1986), 231–260.

[7] Annette Baier. 1991. Trust, the tanner lectures on human values. Princeton: Princeton University (1991).

[8] Annette C Baier. 1992. Trusting people. Philosophical Perspectives 6 (1992), 137–153.

[9] There are many more examples we might have cited as illustrative of each of these points. We also found evidence that they are uncomfortable with the loss of control relating to third party data sharing [48], though we did not expound on this in the paper.

[9] S Barocas and H Nissenbaum. 2014. Computing Ethics: Big Data's End Run Around Procedural Privacy Protections–Recognizing the Inherent Limitations of Consent and Anonymity.

[10] Paul C Bauer, Frederic Gerdon, Florian Keusch, Frauke Kreuter, and David Vannette. 2021. Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. Information, Communication & Society (2021), 1–21.

[11] Rajesh Bejugam and Kristen LeFevre. 2011. enlist: Automatically simplifying privacy policies. In 2011 IEEE 11th International Conference on Data Mining Workshops. IEEE, 620–627.

[12] Adil Bilal, Stephen Wingreen, and Ravishankar Sharma. 2020. Virtue ethics as a solution to the privacy paradox and trust in emerging technologies. In Proceedings of the 2020 the 3rd international conference on information science and system. 224–228.

[13] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. Social psychological and personality science 4, 3 (2013), 340–347.

[14] J Adam Carter. 2022. Trust as performance. Philosophical Issues 32, 1 (2022), 120–147.

[15] Marc A Cohen and John Dienhart. 2013. Moral and amoral conceptions of trust, with an application in organizational ethics. Journal of business ethics 112, 1 (2013), 1–13.

[16] Cynthia L Corritore, Beverly Kracher, and Susan Wiedenbeck. 2003. On-line trust: concepts, evolving themes, a model. International journal of human-computer studies 58, 6 (2003), 737–758.

[17] Nick Couldry and Ulises A Mejias. 2019. The costs of connection. In The Costs of Connection. Stanford University Press.

[18] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'privacy'for a networked world. Computer Supported Cooperative Work (CSCW) 26, 4 (2017), 453–488.

[19] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science 10, 1 (1999), 104–115.

[20] Tomi Dahlberg, Niina Mallat, and Anssi Öörni. 2003. Trust enhanced technology acceptance modelconsumer acceptance of mobile payment solutions: Tentative evidence. Stockholm Mobility Roundtable 22, 1 (2003), 145.

[21] Fred D Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly (1989), 319–340.

[22] Jason D'Cruz. 2015. Rationalization as performative pretense. Philosophical Psychology 28, 7 (2015), 980–1000.

[23] Jason D'cruz. 2015. Trust, trustworthiness, and the moral consequence of consistency. Journal of the American Philosophical Association 1, 3 (2015), 467–484.

[24] Bernhard Debatin, Jennette P Lovejoy, Ann-Kathrin Horn, and Brittany N Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of computer-mediated communication 15, 1 (2009), 83–108.

[25] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. Information systems research 17, 1 (2006), 61–80.

[26] Paul Dourish and Graham Button. 1998. On" technomethodology": Foundational relationships between ethnomethodology and system design. Human-computer interaction 13, 4 (1998), 395–432.

[27] Nora A Draper. 2017. From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates. Policy & Internet 9, 2 (2017), 232–251.

[28] Catherine Dwyer, Starr Hiltz, and Katia Passerini. 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. AMCIS 2007 proceedings (2007), 339.

[29] Nico Ebert, Kurt Alexander Ackermann, and Peter Heinrich. 2020. Does Context in Privacy Communication Really Matter?—A Survey on Consumer Concerns and Preferences. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–11.

[30] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–12.

[31] Tatiana Ermakova, Annika Baumann, Benjamin Fabian, and Hanna Krasnova. 2014. Privacy policies and users' trust: does readability matter?. In AMCIS.

[32] Ulrike Felt, Milena D Bister, Michael Strassnig, and Ursula Wagner. 2009. Refusing the information paradigm: informed consent, medical research, and patient participation. Health: 13, 1 (2009), 87–106.

[33] Carlos Flavián and Miguel Guinalíu. 2006. Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Industrial management & data Systems (2006).

[34] Christian Flender and Günter Müller. 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. In International Symposium on Quantum Interaction. Springer, 148–159.

[35] David Gefen. 2000. E-commerce: the role of familiarity and trust. Omega 28, 6 (2000), 725–737.

[36] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & security 77 (2018), 226–261.

[37] Isha Ghosh and Vivek Singh. 2017. Using cognitive dissonance theory to understand privacy behavior. Proceedings of the Association for Information Science and Technology 54, 1 (2017), 679–681.

[38] Ian Goldberg, Austin Hill, and Adam Shostack. 2001. Trust, ethics, and privacy. BUL Rev. 81 (2001), 407.

[39] Harald Grimen. 2009. Power, trust, and risk: some reflections on an absent issue. Medical anthropology quarterly 23, 1 (2009), 16–33.

[40] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In Proceedings of the 2018 CHI conference on human factors in computing systems. 1–15.

[41] Cory Hallam and Gianluca Zanella. 2017. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Computers in Human Behavior 68 (2017), 217–227.

[42] Eszter Hargittai and Alice Marwick. 2016. "What can I really do?" Explaining the privacy paradox with online apathy. International journal of communication 10 (2016), 21.

[43] Richard Harper. 2014. Trust, computing, and society. Cambridge University Press.

[44] Richard Harper, Sean Rintel, Rod Watson, and Kenton O'Hara. 2017. The 'Interrogative Gaze': Making video calling and messaging 'accountable'. Pragmatics 27, 3 (2017), 319–350.

[45] Todd Hartman, Helen Kennedy, Robin Steedman, and Rhianne Jones. 2020. Public perceptions of good data management: Findings from a UK-based survey. Big Data & Society 7, 1 (2020), 2053951720935616.

[46] Stephen Hester and David Francis. 1994. Doing data: The local organization of a sociological interview. British Journal of Sociology (1994), 675–695.

[47] Chris Jay Hoofnagle and Jan Whittington. 2013. Free: accounting for the costs of the internet's most popular price. UCLA L. Rev. 61 (2013), 606.

[48] Nicola Howe, Emma Giles, Dorothy Newbury-Birch, and Elaine McColl. 2018. Systematic review of participants' attitudes towards data sharing: a thematic synthesis. Journal of health services research & policy 23, 2 (2018), 123–133.

[49] Gordon Hull. 2015. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics and Information Technology 17, 2 (2015), 89–101.

[50] Ada Lovelace Institute. 2021. The Citizens' Biometrics Council. Available at: https://www.adalovelaceinstitute.org/project/citizens-biometrics-council/.

[51] Ada Lovelace Institute. 2021. Participatory data stewardship. Available at: https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/.

[52] Carlos Jensen, Colin Potts, and Christian Jensen. 2005. Privacy practices of Internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies 63, 1-2 (2005), 203–227.

[53] Adam N Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B Paine Schofield. 2010. Privacy, trust, and self-disclosure online. Human–Computer Interaction 25, 1 (2010), 1–24.

[54] Helen Kennedy. 2016. Post, mine, repeat: Social media data mining becomes ordinary. Springer.

[55] Esther Keymolen and Astrid Voorwinden. 2020. Can we negotiate? Trust and the rule of law in the smart city paradigm. International Review of Law, Computers & Technology 34, 3 (2020), 233–253.

[56] Bran Knowles and Vicki L Hanson. 2018. Older adults' deployment of 'distrust'. ACM Transactions on Computer-Human Interaction (TOCHI) 25, 4 (2018), 1–25.

[57] Bran Knowles and Vicki L Hanson. 2018. The wisdom of older technology (non) users. Commun. ACM 61, 3 (2018), 72–77.

[58] Bran Knowles, Vicki L Hanson, Yvonne Rogers, Anne Marie Piper, Jenny Waycott, Nigel Davies, Aloha Hufana Ambe, Robin N Brewer, Debaleena Chattopadhyay, Marianne Dee, et al. 2021. The harm in conflating aging with accessibility. Commun. ACM 64, 7 (2021), 66–71.

[59] Roderick M Kramer. 2009. Rethinking trust. Harvard business review 87, 6 (2009), 68–77.

[60] Mary Jane Kwok Choon. 2018. Revisiting the privacy paradox on social media: An analysis of privacy practices associated with Facebook and Twitter. Canadian Journal of Communication 43, 2 (2018), 339–358.

[61] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. Proceedings of the ACM on Human-Computer Interaction 2, CSCW (2018), 1–31.

[62] Thomas W Lauer and Xiaodong Deng. 2007. Building online trust through privacy practices. International Journal of Information Security 6, 5 (2007), 323–331.

[63] Qingrui Li, Juan Li, Hui Wang, and Ashok Ginjala. 2011. Semantics-enhanced privacy recommendation for social networking sites. In 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 226–233.

[64] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM conference on ubiquitous computing. 501–510.

[65] Ewa Luger, Stuart Moran, and Tom Rodden. 2013. Consent for all: revealing the hidden complexity of terms and conditions. In Proceedings of the SIGCHI conference on Human factors in computing systems. 2687–2696.

[66] Ewa Luger and Tom Rodden. 2013. An informed view on consent for UbiComp. In Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing. 529–538.

[67] Christoph Lutz and Pepe Strathoff. 2014. Privacy concerns and online behavior–Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. Viewing the Privacy Paradox Through Different Theoretical Lenses (April 15, 2014) (2014).

[68] Michael Lynch. 1999. Silence in context: Ethnomethodology and social theory. Human studies 22, 2 (1999), 211–233.

[69] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research 15, 4 (2004), 336–355.

[70] Alice E Marwick and Danah Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. New media & society 16, 7 (2014), 1051–1067.

[71] Roger C Mayer, James H Davis, and F David Schoorman. 1995. An integrative model of organizational trust. Academy of management review 20, 3 (1995), 709–734.

[72] Aleecia M McDonald and Lorrie Faith Cranor. 2010. Americans' attitudes about internet behavioral advertising practices. In Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. 63–72.

[73] Victoria McGeer. 2008. Trust, hope and empowerment 1. Australasian Journal of Philosophy (2008).

[74] D Harrison McKnight, Vivek Choudhury, and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. Information systems research 13, 3 (2002), 334–359.

[75] Miriam J Metzger. 2006. Effects of site, vendor, and consumer characteristics on web site trust and disclosure. Communication Research 33, 3 (2006), 155–179.

[76] George R Milne and Mary J Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of interactive marketing 18, 3 (2004), 15–29.

[77] Alistair Morrison, Donald McMillan, and Matthew Chalmers. 2014. Improving consent in large scale mobile HCI through personalised representations of data. In Proceedings of the 8th Nordic conference on human-computer interaction: Fun, fast, foundational. 471–480.

[78] Bettina Nissen, Victoria Neumann, Mateusz Mikusz, Rory Gianni, Sarah Clinch, Chris Speed, and Nigel Davies. 2019. Should I agree? delegating consent decisions beyond the individual. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 1–13.

[79] Helen Nissenbaum. 2020. Privacy in context. Stanford University Press.

[80] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs 41, 1 (2007), 100–126.

[81] Leysia Palen and Paul Dourish. 2003. Unpacking" privacy" for a networked world. In Proceedings of the SIGCHI conference on Human factors in computing systems. 129–136.

[82] Chanda Phelan, Cliff Lampe, and Paul Resnick. 2016. It's creepy, but it doesn't bother me. In Proceedings of the 2016 CHI conference on human factors in computing systems. 5240–5251.

[83] David Randall, Mark Rouncefield, and Peter Tolmie. 2021. Ethnography, CSCW and ethnomethodology. Computer Supported Cooperative Work (CSCW) 30, 2 (2021), 189–214.

[84] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–12.

[85] Neil Richards. 2021. Why privacy matters. Oxford University Press.

[86] Neil Richards and Woodrow Hartzog. 2015. Taking trust seriously in privacy law. Stan. Tech. L. Rev. 19 (2015), 431.

[87] Valeria Righi, Sergio Sayago, and Josep Blat. 2017. When we talk about older people in HCI, who are we talking about? Towards a 'turn to community' in the design of technologies for a growing ageing population. International Journal of Human-Computer Studies 108 (2017), 15–31.

[88] Eric P Robinson and Yicheng Zhu. 2020. Beyond "I Agree": Users' Understanding of Web Site Terms of Service. Social Media+ Society 6, 1 (2020), 2056305119897321.

[89] John-David Rusk. 2014. Trust and decision making in the privacy paradox. In Proceedings of the Southern Association for Information Systems Conference, Vol. 32. 1–6.

[90] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. Quality & quantity 52, 4 (2018), 1893–1907.

[91] William Seymour, Martin J Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the design of privacy-empowering tools for the connected home. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–14.

[92] Kim Bartel Sheehan and Mariea Grubbs Hoy. 2000. Dimensions of privacy concern among online consumers. Journal of public policy & marketing 19, 1 (2000), 62–73.

[93] Herbert Alexander Simon. 1997. Models of bounded rationality: Empirically grounded economic reason. Vol. 3. MIT press.

[94] Thomas W Simpson. 2012. What is trust? Pacific Philosophical Quarterly 93, 4 (2012), 550–569.

[95] Benjamin Six. 2014. A pragmatic contribution for a more reflexive institution-based trust. Journal of Trust Research 4, 2 (2014), 132–146.

[96] Daniel J Solove. 2004. The digital person: Technology and privacy in the information age. Vol. 1. NyU Press.

[97] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. Harv. L. Rev. 126 (2012), 1880.

[98] S Shyam Sundar, Jinyoung Kim, Mary Beth Rosson, and Maria D Molina. 2020. Online privacy heuristics that predict information disclosure. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–12.

[99] Monika Taddicken. 2014. The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of computer-mediated communication 19, 2 (2014), 248–273.

[100] Paul Ten Have. 2003. Understanding qualitative research and ethnomethodology. Sage.

[101] Peter Tolmie and Andy Crabtree. 2021. Accountability in ordinary action. Privacy by Design for the Internet of Things: Building Accountability and Security (2021), 49.

[102] Traverse and the Ada Lovelace Institute. 2021. Public dialogue on location data ethics. Published by The Geospatial Commission. Available at: https://www.gov.uk/government/news/public-dialogue-on-location-data-ethics-published.

[103] Zeynep Tufekci. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society 28, 1 (2008), 20–36.

[104] Joseph Turow, Michael Hennessy, and Nora Draper. 2015. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Available at SSRN 2820060 (2015).

[105] Lisa van der Werff, Alison Legood, Finian Buckley, Antoinette Weibel, and David de Cremer. 2019. Trust motivation: The self-regulatory processes underlying trust decisions. Organizational Psychology Review 9, 2-3 (2019), 99–123.

[106] Max Van Kleek, Reuben Binns, Jun Zhao, Adam Slack, Sauyon Lee, Dean Ottewell, and Nigel Shadbolt. 2018. X-ray refine: Supporting the exploration and refinement of information exposure resulting from smartphone apps. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 1–13.

[107] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J Weitzner, and Nigel Shadbolt. 2017. Better the devil you know: Exposing the data sharing practices of smartphone apps. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. 5208–5220.

[108] Iris van Ooijen and Helena U Vrabec. 2019. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. Journal of consumer policy 42, 1 (2019), 91–107.

[109] Tien Wang, Trong Danh Duong, and Charlie C Chen. 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. International journal of information management 36, 4 (2016), 531–542.

[110] Ye Diana Wang and Henry H Emurian. 2005. An overview of online trust: Concepts, elements, and implications. Computers in human behavior 21, 1 (2005), 105–125.

[111] Rod Watson. 2009. Constitutive practices and Garfinkel's notion of trust: Revisited. Journal of Classical Sociology 9, 4 (2009), 475–499.

[112] A Westin. 1991. Harris Louis & Associates. Harris-Equifax Consumer Privacy Survey. Technical Report. Tech. rep, Conducted for Equifax Inc. 1,255 adults of the US public.

[113] Kuang-Wen Wu, Shaio Yan Huang, David C Yen, and Irina Popova. 2012. The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior 28, 3 (2012), 889–897.

[114] Shoshana Zuboff. 2019. The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019. Profile books.