

REPHRAIN
Protecting citizens online



Home alone? Exploring the geographies of digitally-mediated privacy practices at home during the COVID-19 pandemic

Kim Cheetham, Independent Researcher

Ola Michalec, University of Bristol



August 2023



Cheetham, K., & Michalec, O. (Accepted/In press). *Home alone? Exploring the geographies of digitally-mediated privacy practices at home during the COVID-19 pandemic*. Annual Privacy Forum (Springer).

Early version, also known as pre-print

License (if available):
CC BY

[Link to publication record in Explore Bristol Research](#)
PDF-document

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
<http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

¹ ola.michalec@bristol.ac.uk ,

¹ Paper type: Full paper, original research, student paper

Home alone? Exploring the geographies of digitally-mediated privacy practices at home during the COVID-19 pandemic*

Kim Cheetham¹ and Ola Michalec²[0000–0003–3807–0197]

¹ Independent Researcher

² Bristol Cyber Security Group, University of Bristol

Abstract. During the COVID-19 pandemic, digital technologies have enabled work, education, community activity, and access to healthcare to be situated within our homes. These emerging applications call for a renewed focus on the geographies of online privacy. Thus, this research aims to **explore the geographies of digitally-mediated privacy practices at home during the COVID-19 lockdown** through the method of qualitative in-depth interviews with the lay-users of the Internet. Using Social Practice Theory, the paper explores contextual, collective and spatial dimensions of privacy. In particular, the paper explores how increased use of digital technologies at home during the COVID-19 lockdown has reconfigured practices of self-disclosure, data-sharing and protection of private spaces. First, the paper argues that the use of new work tools, the re-purposing of work tools for social means, and the use of personal devices for work functions, have all affected people’s ability to maintain boundaries between their work and personal lives. Second, the paper uncovers how public health concerns during the pandemic mobilised the collective dimensions of privacy, countering the popular belief that privacy is an individualistic concern. Taken together, these findings point at reorienting digital geographies of privacy towards the people and spaces ‘behind’ the screen.

Keywords: Privacy · Social Practice Theory · Lockdown · digital mundane · work from home.

1 Introduction

The global COVID-19 pandemic—dubbed a ‘great accelerator’ of digital transformation [3]—has led to the adoption of numerous emerging technology trends. Social distancing and ‘lockdown’ measures have created the need for home accessibility, leading to people interacting with online ‘universities of the future’ and work-from-home ‘officeless firms’, maintaining health and well-being through ‘eHealth systems’, receiving policy updates from social-media posts of ‘digital

* Supported by the REPHRAIN National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online.

governments’, and logging day-to-day activities using contact tracing systems [25,20,71,23]. The proponents of this shift to digitally-mediated services have reported benefits in work efficiency, citizen engagement, and entrepreneurial inclinations [30,12]. However, others stress that although COVID-19 has offered a glimpse of a possible digital future, crisis management is not equal to ‘time travel’ and the adoption of digital technologies at home may reconfigure society in ways we cannot yet envision [14]. Cross-disciplinary work finds that the COVID-19 pandemic has amplified existing risks and harms associated with digital technologies including the ‘digital divide’, criminal opportunities, and market failures (such as ‘price gouging’ from hand sanitizer merchants on Amazon) [56,6,49,]. This paper serves as an exploratory study of the digitally-mediated privacy practices performed in the home during the COVID-19 lockdown. Theoretically, it brings attention to the spatial, contextual and collective dimensions of privacy, pointing at the people and spaces behind the digital screens.

The home is protected as a private space in traditional privacy legislation across Europe. The European Convention on Human Rights asserts that ‘everyone has the right to respect for his private and family life, his home and his correspondence’ [16]. Yet, since the introduction of electronic and digital technologies to homes, the home has served as a focal point for the interaction between technology and privacy—from the wiretapping of phone conversations in the early 1960s [52] to the contemporary issues of Intimate Partner Violence threats in ‘smart homes’ [63,68]. Situating sensing, quantifying and monitoring technologies within the home results in an increased capacity to observe actions regarded as private, listen in on conversations thought to be private, collect and exchange information thought to be private, and interpret physiological responses viewed as private [52]. Furthermore, there is the potential for organisations providing digital tools to derive power from their panoptic access to an individual’s histories, activities, communications, thoughts, and proclivities [52]. This is a cause for alarm when users are consenting to giving these private things away unknowingly, or through an all-or-nothing and non-autonomous choice [5].

Internet technologies positioned within the home—whether for work, education, commerce, health, well-being, or entertainment—routinely require users to make choices about their informational privacy. The character of these everyday choices is different from those addressed in previous off-line privacy research, due to the volume of data collection opportunities and people’s capacity to meaningfully consent to a privacy setting [69]. Any change to the number and variety of privacy decisions that users are having to make is of interest because privacy concern is *adaptive* and once an intrusion becomes part of the common fabric of our daily lives, we become less concerned about it [22]. Lockdowns have highlighted a conflict between the need to maintain a flourishing life and the need to protect public health. This conflict necessitates an understanding of to what extent these needs have led to the adoption of new technology practices and how these practices are reconfiguring the notion of privacy. [2].

As such, the research tackles the following questions:

- How has the COVID-19 pandemic impacted people’s privacy protective practices?
- How has the COVID-19 pandemic impacted people’s self-disclosure practices?
- How has the COVID-19 pandemic impacted people’s data-sharing practices?

Through a qualitative analysis based on 18 semi-structured interviews with internet lay-users, this research aims to **explore the geographies of digitally-mediated privacy practices at home during the COVID-19 pandemic**. The use of Social Practice Theory (SPT) [60] enabled the identification of privacy practices as well as the associated methods and meanings.

2 Conceptual Discussions

The following section will present a brief overview of the concept of privacy; highlighting multiple definitions and key research questions concerning scholars over several decades. Following the conventions of qualitative social sciences [32], the aim of the literature review is to present a history of “turns” within the field, i.e., how definitions of privacy changed over time. The authors conducted the review by engaging with the foundational papers on privacy across disciplines, paying attention to theoretical outputs offering novel frameworks. One of the first conceptualisations of privacy in relation to everyday technologies goes back to the 1890s when Warren[73] considered the camera, and its potential for instantaneous photographs, as a reason to grant a legal right to privacy—the ‘right to be let alone’ [73]. Philosophical debates have centred around the questions: ‘what is privacy?’; ‘is it a necessary human value?’; if so, ‘is it a human value that is inherently distinct from other human values?’; if so, ‘why is it so valuable?’.

Schoeman[57] considers the three questions above in depth in his 1984 anthology *Philosophical Dimensions of Privacy*. Considering the question ‘what is privacy?’: depending on the academic discipline, Schoeman writes that privacy can be understood as a *claim*, *entitlement* or *right* of an individual to determine what information about themselves may be communicated to others [57]. Alternatively, the measure of *control* that an individual has over: information about themselves; intimacies of personal identity; or who has sensory access to them [75,1]. These conceptualisations all have their respective criticisms centering around their static nature in the face of changing privacy planes. In order to transcend the definitional debates and focus on empirical experiences of privacy, this paper takes the approach of Solove to consider privacy pluralistically. In this understanding, privacy is simultaneously collective, contextual and spatial [65,24,4]. This approach is flexible enough to accommodate the evolving debate on privacy in the light of COVID-19-induced adoption of digital technologies.

2.1 Privacy is Collective

Privacy is a collective concept in two senses: the interpersonal and the political [42]. With regards to the interpersonal dimension, privacy is key to social

interactions [1], its understandings are products of our own social and cultural development [41], and, finally, privacy is an attribute not only of individuals but also of groups and organisations [52]. Moreover, privacy is a political concept for three reasons [42]: people have a common right to privacy [52], privacy supports and is supported by democratic political systems [52,], privacy is a societal good because it is increasingly difficult for any one person to have privacy unless everyone is granted a similar minimum level of privacy [42]. These emerging collectivist conceptualisations counter the popular notion that privacy is an individualised concern and cannot be mobilised in a way to build communities or enact political change [9].

2.2 Privacy is Contextual

The collective nature of privacy means that privacy management is not just negotiated at an individual level, but between many individuals, often at a group or community level, in a variety of social and practical contexts. To further that argument, scholars such as Altman, Margulis and Solove [1,40,65,] believe that privacy is so dependent on a specific context that it is impossible to develop a one-size-fits-all conceptualisation [64]. What is considered sensitive, and therefore worthy of protection, obfuscation or concealment, varies depending on a range of contextual factors. These could relate to the information usage, spatial setting, and the relationship between the receiver and the sender of the information [45]. For example, situational increases in privacy concern may be triggered by external cues that signal a lack of privacy such as targeted advertisements [33] and situational decreases in privacy concern may occur in response to technological protections such as private browsing mode [27]. Furthermore, privacy has temporal contextuality in that the sensitivity of information may change over time, such as an individual's willingness to disclose their age [45]. Collectively held practices of defining, preserving and subverting sensitivity evolve over time, in response to historical, cultural and geographic influences. Nissenbaum's theory of contextual integrity posits that information technologies violate privacy when the information flows cease to conform with contextual information norms [48]. Using this contextual perspective, privacy can be understood as a process of managing boundaries across different social contexts, which may shift, collapse or reemerge as social circumstances change [76]. Who has the power to make these boundaries visible and negotiable is an inherently political question, therefore worthy of exploration for critical social scientists, including digital geographers.

2.3 Privacy is Spatial

So far, the literature on privacy has emphasised the need to investigate this concept as a collective phenomenon situated in a social context [15,43,48]. As the notion of 'social context' has spatial attributes, it benefits from a cross-disciplinary reading involving human geography theorists. Geography brings attention to the social construction, fluidity and instability of places, spaces and

boundaries between them [35]. Operating across a range of scales, from investigating the mundane activities inside smart homes [36,54], the discourses of smart cities [44,53], to the local embeddedness of seemingly global cyberspace(s) [19], geographers question assumptions held about the relationships between people and places. Within the context of digital privacy, geography offers three core contributions. First, that the private-public distinction is not a reflection of a ‘natural order’, rather, it is an expression of power [35]. Private-public is not a clear-cut binary; rather: “a [private/public] space only gets meaning in context: in relation to the people in it and in relation to its outside; ‘home’ and ‘public space’ are therefore two sides of a coin” [35, pg. 45]. Second, social identities are constructed in spatial settings [35]. Understanding privacy as a freedom to shape one’s identity in a given context (e.g. work, school, domestic) allows making a distinction between researching private practices and private spaces. Finally, geographers argue that researching privacy concerns in spatial settings (e.g. smart homes, smart cities) should move beyond procedural concerns (‘is the connection encrypted? Are datasets anonymised?’) and, instead, ask: ‘whose interests and logics are materialised by the creation of ‘smart’ spaces?’, ‘who has the power negotiate the boundaries of digital privacy and publicity?’ [39]. Here one should note that although the theoretical critiques of ‘smart’ spaces are ample across critical social sciences, they still lack solid grounding in lay-user experiences [31]. As such, the enmeshing of cyber and physical spaces calls for further research on embodied experiences of lay-users [13].

2.4 Privacy in the Pandemic

Widespread fears of loneliness, contagion and illness are affecting the ways we interact with technologies, and technology is being used adaptively to alleviate stress and anxiety [34]. [46] Nabity-Grover et al. have found that people are engaging in self-disclosure on social media to stay connected with others during the pandemic. They theorise that during the COVID-19 pandemic, perceptions of which disclosures serve the public good and which are considered socially inappropriate have altered [46]. For example, the sharing of medical data, traditionally regarded as sensitive, is being encouraged, while disclosing information on social gatherings has shifted to the private realm over the course of lockdown restrictions. To explain this shift, they use the term ‘*inside-out, outside-in*’ and attribute its existence to the performance of *social calculus* (making decisions based on the perceptions of others) in addition to *privacy calculus* (making decisions based on perceived personal benefits) [46].

There is a growing body of work researching the privacy of contact tracing apps. [37] report the widespread acceptance of contact tracing in the UK and suggest that acceptance increases when measures are specifically time-limited and come with opt-out clauses or other assurances of privacy. Furthermore, Vitak and Zimmer [70] use violation of contextual integrity to explain why the contact tracing proposals of Apple and Google were largely considered acceptable by users, whereas the initial suggestions of a centralised and government-led approach were met with strong negative attitudes.

3 Conceptual Framework

This paper draws on Social Practice Theory (SPT) to conceptualise digitally-mediated privacy practices in the time of COVID-19 [60]. A practice can be defined as the integration of elements resulting in a structured arrangement of what people do in a given context. Drawing on Shove [60], these elements fall into one of three empirically helpful categories: *materials* (including things, technologies, and tangible physical entities), *competences* (including skill, know-how and techniques) and *meanings* (including symbolic meanings, ideas and aspirations). A focus on practice allows a researcher to do more than just determine what participants are thinking, facilitating consideration of how practice elements circulate, and how skills are being continually deferred and re-framed, resulting in an interactive, complex and dynamic process that is continually performed [66]. Dourish et al[15] perceive privacy as a continual accomplishment that is perpetually being produced and reproduced, rather than a static need that can be ‘set up’ through a control panel and then left alone. They also characterise it as a pervasive element of everyday settings, which extends beyond the boundaries of any technology system and incorporates organisational arrangements and practices as well as the physical environment [15].

When used within the context of technology, SPT decenters technology and stresses that technology is just a piece of a bigger story [66]. This is particularly relevant when considering the concept of privacy as it far out-dates the modern technologies that are our current concerns (consider Warren [73] being alarmed about the privacy of early cameras). In the view of Dourish [15], technology is just a site at which social meaning can be produced. Thus technology is something that plays a part in helping or hindering our desires for privacy, but privacy does not originate from technology, and this decentering is a key motivation for the use of SPT.

In this view, pro- or anti-privacy actions are not seen as the result of people’s attitudes, values and beliefs, constrained by various contextual ‘barriers’, but as embedded within and occurring as part of social practices [72]. In turn, the performance of various social practices is seen as part of the routine accomplishment of what people take to be ‘normal ways of life’ [58]. Individuals are removed from centre stage and instead become the ‘carriers’ of social practices [51]. Importantly, SPT raises a series of radically different questions about how best to protect privacy. The focus shifts to understanding how people maintain and routinise practices in temporal and spatial dimensions.

Social Practice Theory (SPT) has been broadly applied by scholars across geography and sociology as a means to move beyond ‘behaviourist’ accounts of planet-friendly living [59]. Acknowledging that social practices form at the intersection of material affordances, social meanings and competences, scholars like Shove[60], Watson[74] and Evans[17] counter the popular belief of pro-environmental actions solely resulting from individual rational attitudes and choices. The past two decades have been witness to “a practice turn” in social theory [11], with SPT applied to a range of geographical settings, from water and energy consumption practices [28,67], cycling [8] or grassroots activism [21].

This article presents an opportunity to apply social practice theory in a novel context of digitally-mediated experiences of privacy.

4 Methods

4.1 Research Design: Semi-Structured Interviews

A set of semi-structured interviews were conducted with 18 UK-based participants listed in Table 1 during February and March of 2021. The inclusion criteria required that the participant is an internet ‘lay-person’, defined for this specific purpose as a person with a minimum capability of being able to use an internet search engine, but who is not an IT professional. A proportion of the interviews (n=11) were transcribed by the first author and the remaining (n=9) were transcribed by a professional transcription service. This project received internal ethical approval from the University of Bristol research committee (reference number 97842).

Participant	Age	Gender	Location	Occupation	Education
Rachel (pilot)	62	F	Nottinghamshire	Administration	Undergraduate
Michael	20	M	Leicestershire	Student (Design)	Undergraduate
Jordan	22	M	Nottinghamshire	Student (Engineer)	Undergraduate
Margaret	78	F	Essex	Retired (Teacher)	Postgraduate
Ruth	55	F	Leicestershire	Homemaker	Undergraduate
Greg	21	M	Bristol	Student (Computer Science)	Undergraduate
Edward	22	M	Nottinghamshire	Student (Law)	Undergraduate
Claire	52	F	Berkshire	Technical Writer	Undergraduate
Phillip	81	M	Essex	Retired (Chemist)	High School
Lois	23	F	Cardiff	PhD Student (Biology)	Postgraduate
Luke	21	M	Bristol	Student (Maths)	Undergraduate
Emily	22	F	Derby	Marketing	Undergraduate
Julie	59	F	Essex	Administration	High School
Simon	21	M	Bristol	Student (Medic)	Undergraduate
Archie	20	M	Bristol	Student (Computer Science)	Undergraduate
Sarah	56	F	Nottinghamshire	Homemaker	Postgraduate
Miranda	22	F	Bristol	Student (Vet)	Undergraduate
Joe	21	M	Bristol	Student (Biology)	Undergraduate
Hollie	32	F	Nottingham	Teacher	Undergraduate

Table 1. Interview participant demographics

The interview participants constitute a non-random and non-representative sample with recruitment being performed in a purposive [55] and snowball [26] manner; i.e., through a digital poster displayed via university social media and word-of-mouth recommendations. The sample was purposive because although participants were chosen on a basis of convenience, it was balanced on a range of variables and participants were purposely selected as information-rich and able to

yield insights and in-depth understanding rather than empirical generalisations [50]. Snowball sampling occurred in that the participants were asked to identify individuals that they knew that they thought could meaningfully add to the discussion topic. Due to the exploratory nature of the study, we make no claims to generalisability and recommend further comparative research investigating privacy practices at home across various demographics (e.g., professions or age groups).

The interviews were performed *actively*, meaning that the interviewer and respondent can both be considered as active agents in the construction of the content of the interview [55]. Examples of this included: helping participants better understand their own answers by rephrasing their answers back to them; offering interviewer’s thoughts and feelings on privacy in order to create an environment conducive to intimate disclosure; and providing participants’ with scenarios that the interviewer thought might test their position on an issue, to better understand the limits of their situational understanding. Framing the interviews in this way elicited more latent themes and allowed a deeper understanding of the participants responses [55] but required careful facilitation to minimise bias. Furthermore, respondents were not corrected when they gave incorrect or incoherent information or did not produce an answer that was an obvious fit with the research question. This aided in setting the participant at ease and the misconceptions, misunderstandings, and general musings of participants were a useful basis for latent analysis. Interviews ranged in duration from 50 minutes to 1 hour 40 minutes and were conducted using Voice Over Internet Protocol (VOIP) tools.

Development of interview questions began with the overarching research aim: **“to explore the geographies of digitally-mediated privacy practices at home during the COVID-19 pandemic”**. To make sense of the complex nature of practices, social practice theorists argue that analysts must investigate the four tenets of: materials, competences, meanings and connections [66]. These four tenets became the main areas of inquiry and were expanded into topics of interest which, could then be further developed into interview questions (for further details, please see C). The final topic guide covered the following (for further details, please see A):

1. The participant’s current internet tool usage and usual information disclosure patterns at home.
2. Changes in the participant’s internet tool usage and information disclosure patterns that have occurred during the COVID-19 pandemic.
3. Actions that the participant takes to protect their privacy since the outbreak of the pandemic.
4. The relative importance of privacy to the participant when compared to other actions in the context of the COVID-19 pandemic.

4.2 Data Analysis: Thematic Analysis

Thematic analysis, ‘a method for identifying, analysing, and reporting patterns (themes) within data’ [7], was used. It involved organising and describing the

data set in rich detail, using themes. Thematic analysis facilitates exploration of a thematic range and the analysis of a social group’s knowledge of it, rather than finding a core category and developing theory. The thematic analysis performed was both ‘deductive’ and ‘inductive’ [7]. The analysis was driven by a theoretical interest in the area, coding was performed to match the research question, and significant input for codes was taken from previous researchers’ work on privacy and formulated before the thematic analysis began (deductive coding). However, new codes were also generated as thematic analysis was performed (inductive coding). A code book with example codes is attached in B

5 Results and Discussion

5.1 The Blurring of the Work-Life Divide

The first theme of this research concerns participants’ experiences of their work-life divide, and the privacy-related discomfort of working from home. Although the practice of working from home is not new, the COVID-19 pandemic restrictions have provided many with a novel opportunity (or, indeed, a requirement) to work from home. The interview data shows that the use of new digital tools, the repurposing of these tools for social means, and the use of personal devices for work functions, has affected participants’ privacy practices and led them to conclude that the divide between their work life and their home life has blurred. In addition, when attempting to address these concerns, participants were experiencing privacy stigma.

Negotiating New Tools? The key technologies of concern amongst the participants were found to be business communication platforms and Voice Over Internet Protocol (aka. conference call software). Participants were concerned about the potential for surveillance, disclosure errors and misuse by third-parties. Although neither these tools nor these concerns are new to public debate, for our participants, they presented a novel opportunity to gain first-hand experience of home working or education and associated privacy practices.

Business Communication Technologies A number of communication technologies were introduced during the COVID-19 pandemic to ensure fluid interactions between employees while working from home. Slack is the most commonly used business communication technology amongst the participants and of the four participants that reported regular use, three had never used this tool before. Some participants express difficulty using the tool, leading to errors, and inhibiting use. Participant Lois reports that she feels “really uncomfortable with using Slack” because the different levels of communication (‘channels’, organised by team or project, ‘threads’, for organised side-conversations within channels, and direct-messaging functionality [62]) make it difficult to understand the spatial bounds and persistence of communication. The overlapping of different communication contexts obscures who has access to posts and messages (colleagues?

management? HR?), where they can access them, and for what period of time. This uncertainty causes Lois not to use Slack unless she has to (although this is still “nearly every day”). The confusing interactions with the tool also create an environment conducive to mistakes. Participant Emily shared a story about the time that she accidentally sent a message to the wrong Slack channel:

We have a channel dedicated for non-work related stuff, called The Water Cooler, or something, as a bit of a joke ... and we were talking about something really menial like ice-cream flavours and I accidentally posted “dude, it has got to be mint choc chip” to my project team instead of The Water Cooler chat... I have never been so embarrassed in my life.

The discomfort that Emily feels as a result of this mistake is because the wrong people were the recipients of her self-disclosure, which despite being “menial” information, is more intimate than the norms of a work relationship demand. The context of the information flow—a joke post on a ‘for fun’ Slack channel to co-workers with which she had a friendly relationship—is altered, leading to a violation of contextual integrity and resultant feelings of discomfort and embarrassment. The absence of a social script (should Emily delete the message? Laugh it off? Ignore it?) in these novel situations makes it particularly challenging to adapt and flourish in a remote workplace.

Participants are also suspicious of surveillance while using business communication technologies. For example, both Lois and Emily are unaware of whether their bosses can see their communication in group channels and private messages and admit that this creates a chilling effect when using the tool (Emily: “I have to watch what I say”). Emily is also conscious that potential data violations by coworkers such as screen-shots and copy-and-pasting mean that the audience of her Slack posts might be wider than she can be aware of. Tools like Slack have been in use for a number of years across workplaces, however, they are far from widely adopted communication platforms. When an organisation assigns a new default informational infrastructure in haste, it misses out on an opportunity to re-establish the ground rules of workplace communication and work-life boundaries.

Indeed, Emily and Lois express that business communication technologies have made them more contactable outside of work hours, reducing the separation between their work- and home-lives, making them more likely to work beyond hours and have a poor work-life balance. As comparatively junior staff members (aged 21 and 22), they feel like they have little choice in the use of these tools. This highlights that employers are yet to fully acknowledge workers’ agency (or the lack of such) in the co-creation of digital workplaces. One way to advance this debate would be to shift away from questioning ‘how to make lay-users aware of digital privacy?’ to ‘how can we create environments where lay-users feel empowered to raise privacy concerns?’

Voice Over Internet Protocol In comparison with business communication technologies, participants appeared more comfortable interacting via VOIP. Participant Joe who explains that it is “just like Facetiming six of my mates at the

same time”. Despite participants expressing a higher level of familiarity with the tool, they were still keen to share their privacy concerns. These centre around not wanting professional contacts to get a view into their personal lives, and (in the case of participants whose jobs involve offering professional services) wanting to maintain the privacy of their clients. Participants take a number of privacy protective actions such as ensuring that their background is clear when using camera functionalities, and ensuring they are in a private location where they can not be disturbed or overheard.

Participant Hollie feels that, as a primary school teacher, she has to be especially careful in maintaining her work-life divide. The reasons she cites for this are child safeguarding, her own well-being, and the children’s educational needs. She sees privacy as a defining component of a student-teacher relationship and explains that it is “something that you are taught about extensively in teacher training”. As well as taking steps outside the bounds of the pandemic such as using her middle name instead of her family name on her Facebook profile, she also takes care to ensure that there are no personal items in her background while she is teaching Zoom classes and has moved her desk to give a completely empty screen. Participant Simon, a medical student, has situations in which he has to deal with patient contacts from his room in his shared student house using Microsoft Teams. As a medical professional, he feels the need to take steps to protect his patients’ privacy. Simon only takes meetings using headphones, always faces the camera to prevent being overheard, and uses alphanumerical pseudonyms when writing notes that are visible to others. He asserts that he performs these actions because it is “the right thing to do” and because medicine is built on trust, rather than because there is any immediate consequence within his medical school. In addition, Simon expresses a desire to protect his own privacy and is uncomfortable with the idea of his classmates and patients seeing his bedroom:

I don't like the fact that people are in my private space... Whenever I am using my camera, I am obviously in my bedroom because that is where my desk is ... That is where I sleep, that is where I relax and therefore there is no privacy ... We actually have to show our beds on camera when we are pretending to interact with replica patients. I completely mind.

As well as having concerns grounded in identity management (Simon: “I don’t want anyone to think I am untidy”), he perceives his bedroom (and more acutely his bed) as a part of his most intimate and private sphere and is uncomfortable sharing these on camera with people with whom he does not hold a close intimate relationship. However, because of the nature of his vocation, he feels unable to action his personal privacy concerns. Furthermore, he feels that any request for more privacy would be met with an unsympathetic “deal with it” response from his medical school. Yet again, an accelerated transition into home-based employment and education seemingly closed down the possibility to negotiate what constitutes a ‘good’ digital workplace.

Technology Exaptation The research found that a number of tools and technologies participants previously used for work have been repurposed for social means during the COVID-19 pandemic. This phenomenon is defined here as *technology exaptation*, taking inspiration from the manufacturing use of the term as the ability of a technology to pivot from one use to another without a costly redevelopment process [38]. A prime example of this is the use of Zoom for social events, such as band rehearsals and escape rooms. Lack of access to work equipment has also meant that personal devices such as phones and computers are also being used for work purposes.

All of the participants use VOIP tools for social purposes, and 15 of these had originally used them for work or education purposes. Although Zoom socials have been an integral part of maintaining social connections and mental well-being [34], our paper also suggests that this further blurring of the work-life divide has led to privacy problems such as accidental disclosure. Two respondents (Edward and Luke) reported that they had occasionally accidentally joined professional or educational Zoom meetings with their name still appearing as a nickname from a previous Zoom social—for Luke this was “L-Dog” and for Edward, this was something more “NSFW”³. Both participants felt that they had sufficient rapport with their professional connections to laugh this off but were very aware of the potential consequences of actions that they felt were appropriate within a social context but were not in line with their workplace information sharing norms.

One participant, Emily (who works for a small marketing firm) expresses discomfort regarding her personal devices being repurposed for work. She has concerns that this is encroaching on her privacy and well-being. Emily has been using her home devices for work purposes when working from home during the pandemic. Emily chooses to use her work device (a desktop computer) for most tasks but, in cases where this has been unavailable, she has then used her personal device instead. When interacting with clients, the necessity to screen share has exposed her personal browser bookmarks (including indications of what she feels are potentially embarrassing teenage hobbies), as well as her screensaver (a personal photo of her family). Emily feels that it is the responsibility of the company she works for to change its policy to prevent the use of home devices. Although there is no company requirement for her to use her personal device in these circumstances, because there is no ban on the use of these devices, Emily feels obliged to use them if no other equipment is available.

Privacy Stigma A common thread throughout participants’ responses on the theme of work-life divide was of what we term *privacy stigma*. This was evident when expressing concerns about the use of new tools (including business communication tools and VOIP) as well as about the repurposing of home devices for work purposes. Although participants often had privacy concerns regarding the way that they are having to perform their work and education during the

³ Internet slang meaning “not suitable for work”, used to denote content that is inappropriate for the workplace, usually associated with pornography or violence.

COVID-19 pandemic, they did not often feel comfortable voicing these concerns to their superiors or education coordinators.

For example, Michael doesn't feel comfortable expressing his privacy concerns to his university in case he is seen as a "bit of a Karen"⁴. Emily fears privacy stigma, believing that her boss would tell her to "suck it up" were she to express concerns over using her personal devices for work purposes.

Some participants were resentful of this privacy stigma. For example, Emily expresses her concern about her employers letting privacy fall by the wayside, saying that "it is a really dangerous road to start going down". However, she reflects that the pandemic situation means that she needs her job and wants her career to progress and therefore isn't about to challenge the status quo.

Although the internet has been awash with recommendations [18] and the NCSC [47] and ICOL [29] have stepped in to provide guidance around security and the protection of client data during the COVID-19 pandemic, this work suggests that not enough consideration is being given to workers' and students' privacy. Since participants are not raising privacy concerns because of their worry about privacy stigma, this research argues that companies and educational institutions transitioning to digital activities have not sufficiently considered their implications for privacy, whether for employees, clients or the environment they work and study from. Going forward, highlighting the adaptive, contextual and collective dimensions of digital privacy will be helpful in addressing it as an ongoing socio-technical negotiation between the concerned stakeholders.

5.2 Collective dimensions of privacy in times of pandemic

The second central theme of this research concerns the impact that the COVID-19 pandemic has had on privacy practices because of changing collective norms. There has also been a movement towards participants making privacy decisions based on collective, rather than individual, benefits.

Self-Disclosure Norms The COVID-19 pandemic poses a challenge to interpersonal and community interactions [61] and, indicative of this, all of the participants have lost significant access to their usual in-person methods for socialisation and social connection. This research has already suggested that this change has led to the repurposing of work tools for social means (see 5.1). In addition it has also had an effect on self-disclosure. The lack of usual social contact has led to a shift towards sharing more *opinion based content*. Furthermore, there has been a significant change in what topics are now considered socially acceptable and not socially acceptable to disclose, for which Nabby Grover [46] coin the phrase *inside-out, outside-in*.

⁴ Defined by dictionary.com as a pejorative slang term for an obnoxious, entitled middle-aged women who use their privilege to get their way (<https://www.dictionary.com/e/slang/karen/>)

Opinion-Based Content This research suggests that, during the pandemic, participants are increasingly using social media platforms to post opinion-based content. Participant Claire explains that the Facebook group she is a part of has felt “closer” over the pandemic and she explains that this is because of the opinion-based content that members are sharing. She explained that this opinion sharing gives her a feeling of community membership as well as exposing her to the relationships that she feels she is lacking while being in lockdown in a difficult home situation.

It is people really airing their dirty washing ... I am posting stuff on there that I wouldn't want to share with close family ... It is great to get a second opinion and support with issues, as well as really good discussion about all sorts of things, when I have such a lack of diversity of opinion at home.

However, Joe speaks much more negatively about the increase in opinion-based content that he perceives from his connections on social media.

Say if you were watching a sporting event ... instead of emotionally fueled conversations about the referee decisions happening in person, now people take to social media to air their opinions and that can cause some major issues. The stuff I see posted from some of my Facebook friends, directed at [sports professionals] ... No one wants to see that.

Joe is also critical of opinion-based content outside the bounds of the pandemic, so his reaction to it is not novel to the situation. He finds social media a really uncomfortable place when his connections are sharing opinion-based content, to the point where he takes steps to make himself more comfortable by ‘unfriending’ friends, colleagues and family who he thinks share too much opinion-based content. However, when asked why he didn’t feel the need to post opinion-based content on social media during the pandemic, Joe conceded that he is lucky not to be separated from those friends with whom he can have varied and informative opinion-based discussions. This suggests that the context of a person’s home environment might be affecting the degree to which they feel the need to share opinions on social media. People like Joe, whose shared living arrangements gives them varied social contact, may not feel the need to seek online opinion-based discussions. Amongst the participants, 10 are students who have had comparatively busy and varied social setups during the pandemic, and few of them express a need to share opinions online. In contrast, Lois, who as a result of the pandemic is separated from her close family and friends, believes that she is re-posting more opinion-based content than usual to her Instagram Story.

With all the political stuff going on in the summer⁵, I, like a lot of other people, posted various stories and opinions on my Instagram story be-

⁵ In reference to action from Black Lives Matter, Extinction Rebellion and womens’ safety activists

cause I think it is a really important issue and I wanted to use my platform. But I can't lie, it probably was partly because everyone was ... Sharing the same stories as the people you are close to kind of feels like indirect communication like a kind of "I see you and agree with you" thing going on that you wouldn't need if you were communicating in person.

Inside-Out, Outside-In As presented in 2.4, [46] Nabity Grover et al suggest that during the COVID-19 pandemic there has been an 'inside-out' shift, with things that did not use to be socially appropriate becoming socially appropriate, and an 'outside-in' shift with things that used to be socially appropriate now being met with vitriol. They posit that this is in part because individuals are performing 'social calculus' [46], i.e. considering the perspectives of others when evaluating the costs and benefits of sharing information [10].

This work provides some evidence for this theory. The participants report that they are increasingly sharing information that they would not normally share, including medical information. For example, Lois disclosed for the first time on social media that she has a rare chronic medical condition, in order to establish a COVID-19 advice sharing platform for people with the same condition. Ruth and Claire are also both part of closed Facebook groups which, although intended for other hobbyist purposes, have become platforms where individuals are discussing their symptoms and vaccination status. This research also shows some evidence of the topic of support shifting 'inside-out', with individuals increasingly offering support to their connections and wider community via self-disclosure on social media. The two instances of this were confined to closed online social groups, such as Ruth posting offers of help to collect food for isolating individuals on her community WhatsApp group chat.

The second consideration is the aspects of self-disclosure that have moved 'outside-in'. Nabity-Grover, Thatcher and Cheung suggest that this may include the sharing of activities such as visiting crowded venues because of fear of a negative reaction from connections [46]. Among our participants, Ruth expressed a change in self-disclosure reminiscent of 'outside-in'. She feels uncomfortable sharing her home situation indiscriminately on social media. She explains that she does not want to appear self-entitled and would be uncomfortable if her disclosure was to be seen by connections who did not share her fortune:

I feel like I can't post about things like [my university age children] being at home at the moment as I know so many people haven't been so lucky and I don't want to seem like I am pushing it in anybody's face.

However, in contrast to the suggestions of Nabity-Grover, Cheung and Thatcher, a number of participants explain that the reason that they are not following their normal interaction pattern of sharing information about their activities is because they have "nothing to share", rather than because they are wary of a negative reaction. This makes the 'outside-in' aspect of the theory difficult to validate using the research data. Instead, the data suggests that the lack of

disclosure surrounding activities is less a change in social norms, and more a practical implication of lockdown lifestyle.

Societal Benefit This second sub-theme considers changes to people privacy practices because of perceived benefits to society. The most prevalent example of this is the downloading of COVID-19 monitoring technologies. Participants, in and out of the bounds of the pandemic, are increasingly attempting to wield their data for social good, and some are making an attempt to meaningfully choose recipients of their data based on the perceived effect and contribution that the recipient organisation makes to society.

COVID-19 Monitoring Technologies The two main COVID-19 monitoring technologies investigated in this work are the NHS COVID-19 app⁶ and the ZOE COVID-19 Symptom Tracker⁷. There is widespread acceptance and uptake of the NHS COVID-19 app amongst the participants with 16 using the app. Use of the ZOE Symptom Tracker is less widespread, but of the 12 that are aware of the app, 10 are users. This research suggests that there are different reasons for using each of these apps. The 8 participants who are regular users of the ZOE Symptom Tracker all gave reasons for use that revolve around its capacity to help other people and achieve societal benefit (Sarah: “It feels like I am actually doing something”). Although a proportion of the participants are also using the NHS COVID-19 app for its potential for societal benefit, this was more likely to be performed begrudgingly because of feelings of duty and obligation (Michael: “It is the bare minimum you should do, as a social duty”). Furthermore, 6 of the participants provided reasons for use of the NHS COVID-19 app that were more individualistic, such as Luke admitting “I downloaded it so that I was allowed in to the pub”.

There were also differences in the way that people interact with these two apps. Users of the ZOE Symptom Tracker explain that they are happy to disclose sensitive medical information that they would not normally disclose, as well as a number (n=5) committing to reporting these symptoms daily which, over a year, is a significant commitment as well as a large quantity of data. Of those participants using the app, six explained that they would disclose this data to any medical study, whereas two said they would only do it in a health emergency that was similar in nature to COVID-19. In comparison, four participants explain that although they have downloaded the NHS COVID-19 app, they rarely turn their Bluetooth on, or have downloaded the app but never interact with it. This suggests that although some individuals are willing and able to download the app, their commitment to its use is not that strong. The contrast between the two tools is evident in Lois’s response:

⁶ A voluntary contact-tracing app provided by the NHS for use in England in Wales (see <https://covid19.nhs.uk/>)

⁷ Epidemiological research app developed by researchers in King’s College London (see <https://covid.joinzoe.com/>)

ZOE feels like I am proactively doing something that helps people ... I only remember about [the NHS app] after realising I've had my Bluetooth off for two weeks, it is just not on my radar until I am somewhere with a QR code.

The different levels of commitment to sharing personal data that these technologies invoke may be due to how participants perceive their potential for societal good. A further factor influencing whether participants chose to download these apps was their level of trust in the parties that run them, rather than perceptions of personal or societal gain. The organisation behind the ZOE symptom tracker is known to be a medical and educational institution (Claire: “It might make me a bit of a snob but I trust it because it is a university”), whereas the distrust of some individuals towards government, was evident in some participants perception of the tracker as a government control mechanism (Edward: “I just don’t think the government should have that role”).

Vitak and Zimmer attribute the widespread acceptance of the NHS COVID-19 app to its maintenance of contextual integrity. They posit that contextual integrity is not violated because participants see contact tracing apps as having the same information flow as other non-COVID-related surveillance apps such as navigation and fitness trackers. This research suggests that although there is wide-spread acceptance of the NHS COVID-19 app, a number of participants were highly concerned about it and perceived it as very different from these other suggested technologies. Thus their decision to download the app was often strongly against their privacy concerns and due to a sense of civic duty, rather than because they did not have privacy concerns. These concerns revolved around the aforementioned perceptions of the ‘correct’ role of government and the potential for expanded and continued use post-pandemic. Those participants with strong privacy concerns surrounding the app were able to ‘trade’ these off against the social needs to save lives, and to prevent unnecessary national economic loss. This exposes a gap between individuals privacy attitudes and actions which, without knowledge of the underlying social context, may appear paradoxical. Michael typifies this decision-making process when he explains:

Literally no other circumstance would make me do this. But my privacy has to be nothing in the face of lives ... That is not a hard decision.

Despite steps being taken to make the second version of the NHS COVID-19 app much more protective of its users privacy, the participants were often unaware of the technicalities of the app, meaning that concern surrounding the version 1 app often continued into concern surrounding the version 2 app, with Lois worrying “well it is still a government thing, right?”. Thus although these participants concerns were sometimes unfounded (Julie: “I don’t want Boris ⁸ seeing me go to the shop”), their perceptions of the information flow, whether these were correct or not, violated their perceptions of privacy as contextual integrity.

⁸ The UK’s Prime Minister at the time of writing

6 Future research and Conclusions

6.1 Further research and practice recommendations

It is vital to understand the privacy impact of the interchangeable use of personal and company devices, as well as the lack of agency by people to negotiate privacy boundaries between them and their employers. Following the COVID-19 lockdowns, it is becoming a common practice for companies to allow remote working and enable Bring-Your-Own-Device. The effects on the right to privacy of those practices is an important matter to consider.

We hope this work moves beyond a conceptual remit and will have practical applications. An improved understanding of privacy practices can prompt employers and educators to draw better boundaries between work and personal life and aid privacy engineers with considering novel privacy-preserving features. We outline three key recommendations:

- Both software developers and employers should introduce privacy-preserving mechanisms in workplace/education ICT, which enable protection of employees' and students physical environments, personal identities and relationships outside of work/education.
- Workplaces ought to introduce policies establishing boundaries of communication at work, setting expectations regarding appropriate response time and meeting scheduling.
- Policymakers ought to monitor the development of remote working trends and the associated tracking technologies, so that the provision for workers' rights reflects the adoption of contemporary ICT.

We also recommend that further research explores the evolving technological and legal context of home working and education, i.e. the emergence of worker surveillance tech and obfuscation mechanisms. Finally, future research could validate our initial findings by conducting a comparative survey of privacy practices at home, highlighting similarities and difference across ages, professions and cultures.

6.2 Conclusions

The paper concludes that the 2020 COVID-19 lockdown prompted a re-framing of privacy practices at home: privacy emerged as a collective right as people's perception of privacy is influenced by their relationship with employers, fellow employees, and their respective perspectives on the use of the technology.

Below, we summarise the findings as responses to our initial research questions:

- *How has the COVID-19 pandemic impacted people's privacy protective practices?* While participants took effort to learn and negotiate new ICT tools, they had limited agency over their privacy and experienced privacy stigma while discussing their concerns.

- *How has the COVID-19 pandemic impacted people’s self-disclosure practices?*
In the absence of social script or employer’s guidance, the events of accidental or inappropriate disclosure led to embarrassment and pose a significant barrier to professional fulfillment.
- *How has the COVID-19 pandemic impacted people’s data-sharing practices?*
Participants were overall happy to share personal data when they regarded it as civic duty.

We offer number of theoretical and empirical contributions to the field of digital geography vis-a-vis privacy research. First, we adds to the patchwork of cross-disciplinary literature seeking to understand the role of the COVID-19 pandemic in shaping our society. Second, we argue that an exploration of privacy practices within the novel context of COVID-19 will enrich the debates on collective and spatial dimensions of privacy. This is an important dimension to explore, as the majority of privacy studies consider the technology (network or device) or individual’s cognition (attitudes, perceptions or biases) as a unit of analysis.

In exploring the digitally-mediated privacy practices of Internet lay-users during COVID-19 pandemic, this paper offered a number of empirical findings. First, there is an emerging evidence that the pervasiveness of digital communication technologies as well as technology exaptation in our everyday work and social lives has raised new privacy concerns surrounding the blurring of the work and life boundaries. Second, we posit that these novel concerns are not yet addressed due to the privacy stigma experienced by employees who do not have the capability to negotiate privacy boundaries with their managers. Third, we uncovered the collective motivations for participants’ privacy-protective and self-disclosure practices, countering a popular notion that privacy is a matter of an individualist trade-off.

The technological, social and political change caused by the pandemic has led to the situation of many of our public interactions within the private home, creating opposing social contexts that need to be navigated. Therefore this work seeks to contribute to a broad understanding of digital privacy, not simply as a technical phenomenon but as a concept embedded in collective and spatial contexts. Going forward, we hope that this cross-disciplinary integration of ideas across Social Practice Theory, Digital Geography and Computer Science literature will aid in cultivating environments where lay-users are empowered to raise privacy concerns and, collectively with practitioners, work on co-creating ‘good’ digital workplaces, educational settings and domestic spaces.

References

1. Altman, I.: The environment and social behaviour: Privacy, personal space, territory, crowding. Brooks/Cole Publishing Company, Monterey, CA (1975)
2. Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., Feamster, N.: Discovering smart home internet of things privacy norms using contextual integrity. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. pp. 1–23 (2018). <https://doi.org/10.1145/3214262>

3. Armano, D.: Covid-19 will be remembered as the 'great accelerator' of digital transformation. <https://www.forbes.com/sites/davidarmano/2020/09/09/covid-19-will-be-remembered-as-the-great-accelerator-of-digital-transformation/> (2020)
4. Baruh, L., Popescu, M.: Big data analytics and the limits of privacy self-management. *New Media & Society* **19**(4) (2015). <https://doi.org/10.1177/1461444815614001>
5. Betkier, M.: Privacy online, law, and the effective regulation of online services. Intersentia, Cambridge (2019)
6. de Bolle, C.: Pandemic profiteering: How criminals exploit the covid-19 crisis. Tech. rep., Europol, The Hague, The Netherlands (2020)
7. Braun, V., Clarke, V.: Using thematic analysis in psychology. *Qualitative Research in Psychology* **3**(2), 77–101 (2006). <https://doi.org/10.1191/1478088706QP063OA>
8. Bruno, M., Nikolaeva, A.: Towards a maintenance-based approach to mode shift: Comparing two cases of dutch cycling policy using social practice theory. *Journal of Transport Geography* **86**(C) (2020). <https://doi.org/10.1016/j.jtrangeo.2020.102772>
9. Brunton, F., Nissen, H.: Privacy's trust gap: A review. *The Yale Law Journal* **126**(4), 908–1241 (2017)
10. Buller, D.B., Burgoon, J.K.: Interpersonal deception theory. *Communication Theory* **6**(3), 203–242 (1996). <https://doi.org/10.1111/j.1468-2885.1996.tb00127.x>
11. Cetina, K.K., Schatzki, T.R., von Savigny, E.: The practice turn in contemporary theory. Routledge (2005)
12. Chen, Q., Min, C., Zhang, W., Wang, G., Ma, X., Evans, R.: Unpacking the black box: How to promote citizen engagement through government social media during the covid-19 crisis. *Computers in Human Behaviour* **110** (2020). <https://doi.org/10.1016/j.chb.2020.106380>
13. Cohen, J.E.: Configuring the networked citizen. In: *Imagining New Legalities*, pp. 129–153. Stanford University Press (2020)
14. Coldicutt, R.: Infrastructure not time travel. <https://glimmersreport.net/report/insight> (2020)
15. Dourish, P., Anderson, K.: Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction* **21**(3), 319–342 (2009). https://doi.org/10.1207/s15327051hci2103_2
16. European Convention: Charter of fundamental rights of the european union. Tech. rep., OJ C 326 (EN) (2012)
17. Evans, D., McMeekin, A., Southerton, D.: Sustainable consumption, behaviour change policies and theories of practice (2012)
18. Evans, J.: 12 security tips for the 'work from home' enterprise. <https://www.computerworld.com/article/3532352/12-security-tips-for-the-work-from-home-enterprise.html> (2020)
19. Ferreira, D., Vale, M.: From cyberspace to cyberspatialities? *Fennia-International Journal of Geography* **199**(1), 113–117 (2021). <https://doi.org/10.11143/fennia.100343>
20. Florida, R.: The uncertain future of corporate hqs. <https://hbr.org/2020/09/the-uncertain-future-of-corporate-hqs> (2020)
21. Foden, M.: Everyday consumption practices as a site for activism? exploring the motivations of grassroots reuse groups. *People, Place & Policy Online* **6**(3) (2012). <https://doi.org/10.3351/ppp.0006.0003.0004>
22. Francis, L.P., Francis, J.G.: Privacy: What everyone needs to know. Oxford University Press, New York, NY (2017)

23. Freeguard, G., Sheppard, M., Davies, O.: Digital government during the coronavirus crisis. Tech. rep., Institute for Government, London, UK (2020)
24. Galič, M.: Surveillance and privacy in smart cities and living labs : Conceptualising privacy for public space. Optima Grafische Communicatie, Rotterdam (2019)
25. Goh, L.: The future is now: imagining university life post-covid. <https://www.universityworldnews.com/post.php?story=20210224140632590> (2021)
26. Goodman, L.A.: Snowball sampling. *The annals of mathematical statistics* **32**(1), 148–170 (1961)
27. Habib, H., Colnago, J., Gopalakrishnan, V., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L.F.: Away from prying eyes: Analyzing use and understanding of private browsing. In: Proceedings of the Fourteenth Symposium on Usable Privacy and Security. pp. 159–175. USENIX Association, Baltimore, MD (2018)
28. Hoolohan, C., Browne, A.L.: Design thinking for practice-based intervention: Co-producing the change points toolkit to unlock (un) sustainable practices. *Design Studies* **67**, 102–132 (2020). <https://doi.org/10.1016/j.destud.2019.12.002>
29. Information Commissioner’s Office: The ico’s updated regulatory approach in response to the coronavirus pandemic. <https://ico.org.uk/media/2617613/ico-regulatory-approach-during-coronavirus.pdf> (2021)
30. Ipsen, C., van Veldhoven, K., Kirchner, K., Hansen, J.P.: Six key advantages and disadvantages of working from home in europe during covid-19. *International Journal of Environmental Research and Public Health* **18**(4), 1826 (2021). <https://doi.org/10.3390/ijerph18041826>
31. Jameson, S., Richter, C., Taylor, L.: People’s strategies for perceived surveillance in amsterdam smart city. *Urban Geography* **40**(10), 1467–1484 (2019). <https://doi.org/10.1080/02723638.2019.1614369>
32. Jesson, J.K., Lacey, F.M.: How to do (or not to do) a critical literature review. *Pharmacy education* **6**(2), 139–148 (2006)
33. Kim, T., Barasz, K., John, L.K.: Why am i seeing this ad? the effect of ad transparency on ad effectiveness. *Journal of Consumer Affairs* **45**(5), 906–932 (2018). <https://doi.org/10.1093/jcr/ucy039>
34. Kiraly, O., Potenza, M.N., Stein, D.J., Kind, D.C., Hodgins, D.C., Saunders, J.B.: Preventing problematic internet use during the covid-19 pandemic: Consensus guidance. *Comprehensive Psychiatry* **100**, 152–180 (2020). <https://doi.org/10.1016/j.comppsy.2020.152180>
35. Koops, B.J., Galič, M.: Conceptualizing space and place: Lessons from geography for the debate on privacy in public. Edward Elgar Publishing, Cheltenham (2017)
36. Leszczynski, A.: Digital methods iii: The digital mundane. *Progress in Human Geography* **44**(6), 1194–1201 (2020). <https://doi.org/10.1177/0309132519888687>
37. Lewandowsky, S., Dennis, S., Perfors, A., Kashima, Y., White, J.P., Garrett, P., Little, J.R., Yesilada, M.: Public acceptance of privacy-encroaching policies to address the covid-19 pandemic in the united kingdom. *Plos one* **16**(1) (2021). <https://doi.org/10.1371/journal.pone.0245740>
38. Liu, W., Beltagui, A., Ye, S.: Accelerated innovation through repurposing: exaptation of design and manufacturing in response to covid-19. *R&D Management* (2021). <https://doi.org/10.1111/radm.12460>
39. Maalsen, S., Sadowski, J.: The smart home on fire: Amplifying and accelerating domestic surveillance. *Surveillance & Society* **17**(1/2), 118–124 (2019). <https://doi.org/10.24908/ss.v17i1/2.12925>
40. Margulis, S.T.: Conceptions of privacy: current status and next steps. *Journal of Social Issues* **33**(3), 5–21 (1977). <https://doi.org/10.1111/j.1540-4560.1977.tb01879.x>

41. Margulis, S.T.: Privacy as information management: A social psychological and environmental framework. Tech. rep., U.S. Department of Commerce, National Bureau of Standards, Washington, DC (1979)
42. Margulis, S.T.: Privacy as a social issue and behavioural concept. *Journal of Social Issues* **59**(2), 243–261 (2003)
43. Margulis, S.T.: Three theories of privacy: An overview. *Privacy Online* (2011)
44. Michalec, A.O., Hayes, E., Longhurst, J.: Building smart cities, the just way. a critical review of “smart” and “just” initiatives in bristol, uk. *Sustainable Cities and Society* **47** (2019). <https://doi.org/10.1016/j.scs.2019.101510>
45. Morton, A., Sasse, M.A.: Privacy is a process, not a pet: A theory for effective privacy practice. In: *Proceedings of the 2012 New Security Paradigms Workshop* (2012). <https://doi.org/10.1145/2413296.2413305>
46. Nability-Grover, T., Cheung, C.M.K., Thatcher, J.B.: Inside out and outside in: How the covid-19 pandemic affects self-disclosure on social media. *International Journal of Information Management* **55**, 102–188 (2020). <https://doi.org/10.1016/j.ijinfomgt.2020.102188>
47. National Cyber Security Centre: Home working: Preparign your organisation and staff. <https://www.ncsc.gov.uk/guidance/home-working> (2020)
48. Nissenbaum, H.: *Privacy in context: Technology, policy and the integrity of social life*. Stanford University Press, Redwood City, CA (2009)
49. Palmer, A.: Amazon sellers fined for price gouging hand sanitizer amid coronavirus pandemic. <https://www.cnn.com/2020/11/17/amazon-sellers-fined-for-coronavirus-price-gouging-hand-sanitizer.html> (2020)
50. Patton, M.Q.: Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work* **1**(3), 261–283 (2002). <https://doi.org/10.1177/1473325002001003636>
51. Reckwitz, A.: Toward a theory of social practices: A development in culturalist theorizing. *European journal of social theory* **5**(2), 243–263 (2002). <https://doi.org/10.1177/2F13684310222225432>
52. Regan, P.: *Legislating privacy: Technology, social values, and public policy*. University of North Carolina Press, Chapel Hill, NC (1995)
53. Sadowski, J., Bendor, R.: Selling smartness: Corporate narratives and the smart city as a sociotechnical imaginary. *Science, Technology, & Human Values* **44**(3), 540–563 (2019). <https://doi.org/10.1177/0162243918806061>
54. Sadowski, J., Strengers, Y., Kennedy, J.: More work for big mother: Revaluing care and control in smart homes. *Environment and Planning A: Economy and Space* (2021)
55. Schwandt, T.A.: *The SAGE dictionary of qualitative inquiry*. Sage, London (2007)
56. Seifert, A.: The digital exclusion of older adults during the covid-19 pandemic. *Journal of Gerontological Social Work* **63**(6-7), 674–676 (2020). <https://doi.org/10.1080/01634372.2020.1764687>
57. Shoeman, F.D.: *Philosophical dimensions of privacy: An anthology*. Cambridge University Press, Cambridge (1984)
58. Shove, E.: Changing human behaviour and lifestyle: A challenge for sustainable consumption. *The ecological economics of consumption* pp. 111–131 (2004), <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.7935&rep=rep1&type=pdf>
59. Shove, E.: Beyond the abc: climate change policy and theories of social change. *Environment and planning A* **42**(6), 1273–1285 (2010). <https://doi.org/10.1068/a42282>

60. Shove, E., Pantzar, M., Watson, M.: *The dynamics of social practice: Everyday life and how it changes*. Sage, London (2012)
61. Singh, J., Singh, J.: Covid-19 and its impact on society. *Electronic Research Journal of Social Sciences and Humanities* **2** (2020)
62. Slack Help Center: What is a channel? <https://slack.com/intl/en-gb/help/articles/360017938993> (2021)
63. Slupska, J.: Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review* **15**(1), 83–100 (2019)
64. Smith, H.J., Dinev, T., Xu, H.: Information privacy research: An interdisciplinary review. *MIS Quarterly* **35**(4), 989–1015 (2011). <https://doi.org/10.2307/41409970>
65. Solove, D.J.: *Understanding privacy*. Harvard University Press, Cambridge, MA (2008)
66. Sovacool, B.K., Hess, D.J.: Ordering theories: Typologies and conceptual frameworks for socio-technical change. *Social Studies of Science* **47**(5), 703–750 (2017). <https://doi.org/10.1177/0306312717709363>
67. Strengers, Y.: Peak electricity demand and social practice theories: Reframing the role of change agents in the energy sector. In: *The Global Challenge of Encouraging Sustainable Living*. Edward Elgar Publishing (2013)
68. Strengers, Y., Kennedy, J., Arcari, P., Nicholls, L., Gregg, M.: Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters. In: *Proceedings of the 2019 CHI conference on human factors in computing systems*. pp. 1–13 (2019). <https://doi.org/10.1145/3290605.3300875>
69. van de Waerdt, P.J.: Information asymmetries: recognizing the limits of the gdpr on the data-driven market. *Computer Law & Security Review* **38**, 105436 (2020). <https://doi.org/10.1016/j.clsr.2020.105436>
70. Vitak, J., Zimmer, M.: More than just privacy: Using contextual integrity to evaluate the long-term risks from covid-19 surveillance technologies. *Social Media & Society* **6**(3) (2020). <https://doi.org/10.1177/2056305120948250>
71. Wang, W., Sun, L., Lui, T., Lai, T.: The use of e-health during the covid-19 pandemic: a case study in China's Hubei province. *Health Sociology Review* pp. 1–17 (2021). <https://doi.org/10.1080/14461242.2021.1941184>
72. Warde, A.: Consumption and theories of practice. *Journal of Consumer Culture* **5**(2), 131–153 (2005). <https://doi.org/10.1177/1469540505053090>
73. Warren, S.D., Brandeis, L.D.: Right to privacy. *Harvard Law Review* **4**(5), 193 (1890). <https://doi.org/10.2307/1321160>
74. Watson, M., Browne, A., Evans, D., Foden, M., Hoolohan, C., Sharp, L.: Challenges and opportunities for re-framing resource use policy with practice theories: The change points approach. *Global Environmental Change* **62**, 102072 (2020). <https://doi.org/10.1016/j.gloenvcha.2020.102072>
75. Westin, A.F.: *Privacy and freedom*. Athenum, New York, NY (1968)
76. Wu, P.F., Vitak, J., Zimmer, M.T.: A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology* **71**(4), 485–490 (2020). <https://doi.org/10.1002/asi.24232>

A Interview Questions

A.1 Introduction

“The theme of this interview is information privacy. I am interested in the kinds of information that you choose to disclose while using internet technologies as well as your thoughts and feelings around the collection, use and dissemination of this data by third parties. I am especially interested in how the information that you share about yourself has changed during a global pandemic and whether any of your thoughts and feelings around the use of your data have been impacted by any conflicting priorities such as the need for social interaction, the need to access education or work or the need to support initiatives to aid public health.”

A.2 Information disclosure

1. What sort of internet tools do you regularly use?
2. What kind of information do you disclose on the internet?
 - Why do you choose to disclose this information? What factors impact your decision?
 - How does this compare to the data that the people around you disclose?
 - What are the consequences of not disclosing this data?
 - What are the consequences of disclosing this data?

A.3 Changes in information disclosure

1. Tell me about the change in the internet tools you use as a result of the pandemic?
2. Has this resulted in any change in the amount, or type, of information that you share?
 - Why do you feel this change has occurred?

A.4 General privacy practices

1. What sort of steps to you take to protect your data privacy?
 - Do you feel suitably protected by the actions you take?
 - What level of competency is required to perform these actions? i.e. what skills have you developed to perform these tasks and how easy/hard do you find them?
 - How did you become aware of this method? i.e. who introduced you to it, was it a social or educational setting?
2. What other further steps could you be taking to protect your privacy?
3. To what extent do you feel responsible for protecting your privacy?

A.5 The importance of privacy

1. To what extent do you feel information privacy is important in the current climate of covid-19?
 - Social interaction
 - To make a living
 - To access amenities
 - To protect public health
 - Are there any other further factors that you have had to prioritise over privacy in the current climate?

A.6 Internet tools for fighting COVID-19

1. Have you downloaded any apps that have been specifically developed to help fight COVID-19?

Whether this was to prevent the spread (e.g. NHS contact tracing) or to document symptoms for scientific research (e.g. ZOE Symptom Tracker).

 - What part did privacy play in informing this decision?
 - Do you feel these apps will sufficiently protect your information privacy?
 - How comfortable were you in inputting the data that the app asks for?

Would you happily have inputted this data into a service that is not attempting to fight a pandemic?
2. What level of privacy sacrifice would you be willing to make in order to aid a public health crisis?

A.7 Wrap-up

- Thank you again - your contribution will be invaluable
- I think I have everything I need here but would I be okay to contact you via email if I have any further questions?
- Is there anyone you can recommend who might be willing and able to talk to me over the next 2 weeks or so?

B Code Book

Code	Inclusion Statement	Examples
Accidental self-disclosure - occurrence	x accidentally discloses information about themselves that they did not intent to disclose	“I opened up a Zoom meeting and my nickname was still L-Dog”
Accidental self-disclosure - concern	x is concerned that they may accidentally disclose information about themselves that they did not mean to disclose	“The channels in Slack are so hard to use, I’m worried I am going to use it wrong”

Competency - awareness of threats	x expresses an awareness of privacy threats	"I know with all of these things that there is always the potential for information to get into the wrong hands"
Competency - business practices	x is aware of common business data practices	"I mean, Google collects all of these things about you anyway"
Competency - spatial bounds of internet	x expresses an understanding/lack of understanding of the spacial bounds of the internet	"I am careful not to post things that I don't want even one person not seeing as I know how far these things can get"
Competency - persistence of the internet	x expresses an understanding/lack of understanding of the temporal bounds of the internet	"I had no idea that they would still have this stuff from 10 year ago that I swear I deleted"
Contact tracing - misconceptions	x expresses a perception about contact tracing apps that is not true	"I don't want Boris seeing me go to the shop"
Contact tracing - perceptions	x expresses an opinion surrounding contact tracing	"Well we all know contact tracing hasn't worked quite like they intended"
Contact tracing - reasons	x expresses a reason for using contact tracing	"It is a social duty"
Contact tracing - usage	x gives supplementary information about their usage of contact tracing apps	"My Bluetooth is never switched on so I doubt it is doing anything"
Contextual integrity - maintenance	x expresses that they have no privacy concerns as the information flow is as they expected	"You come to expect to have to give your data to these things therefore it doesn't concern you"
Contextual integrity - violation	x expresses (often latently) that they have privacy concerns because the information flow is not as they expected	(latent) feelings of discomfort at the wrong people the recipient of a communication
Consumer choice	x exercises their data meaningfully as a consumer	"I deliberately click on the affiliate advertising of content creators that I like because they do provide this entertainment for free"
Device repurposing	x is using a device for a purpose for which it was not originally intended	"I having to use my personal phone to take work calls"
Escapism	x shares that they have turned to internet tools as an escape from their daily reality	"TikTok is a good distraction from everything, like a really unhealthy meditation method"

Friends and family data misuse - concern	x is concerned that friends and family might misuse their data	“a friend might screenshot and share it”
Home environment	x’s home environment is affecting their privacy practices	“I don’t have diversity of opinion here so I post more online”
Identity - junior staff member	x identifies as a junior staff member	“I am pretty junior compared to my co-workers”
Identity - poor computer literacy	x perceives themselves as not having a very high level of computer literacy	“You know me, I have no idea what goes on with computers”
Identity management - concern	x is concerned about maintaining their identity amongst connections	“I don’t want anyone to think I am untidy”
Inside-out - occurrence	x perceives/engages in disclosing information of particular topic that they would not normally disclose	“everyone has been posting about their vaccination status on there”
Involuntary disclosure - occurrence	x has disclosed information about themselves involuntarily e.g. because of coercion or obligation	“As part of work, I have to give out my personal mobile number to clients”
Loss of access - social	x expresses that they have lost access to their usual methods of socialisation	“We haven’t been able to go out and see anyone at the moment”
Loss of access - amenities	x expresses that they have lost access to their usual methods of amenities e.g. shopping and healthcare	“I am technically shielding so I haven’t just been able to pop to the shop”
New tools	x is using a new tool in the course of the COVID-19 pandemic	“I started using TikTok last summer”
Nothing to share	x expresses that they have nothing of note to share on social media	“We haven’t done anything is why I am not posting anything”
Opinion-based disclosure - occurrence	x is perceiving, or engaging in opinion-based disclosure	“It was strange with the US election because people were posting their opinions about it”
Opinion-based disclosure - perception	x provides a perception of opinion-based disclosure	“no-one wants to see that”
Other values	x expresses that there are other values they are more concerned about than privacy	“It is far more important to try and save lives”

Outside-in - occurrence	x perceives/engages in not disclosing a particular topic that they would normally be comfortable disclosing	"I don't want to post that my adult children are home ... this feels entitled"
Privacy of alternatives	x is aware that there are options with more privacy and this changes their attitude or action	"With the NHS app, there were ways to achieve the same result without collecting that level of data"
Privacy paradox - evidence	x shows a difference between their privacy concerns and privacy actions	"I am pretty concerned about it but I am not about to do anything about it"
Privacy paradox - explanation	x provides an (often latent) explanation for the privacy paradox	"It doesn't matter how concerned I am because what I do has no impact"
Privacy stigma - concern	x expresses that they are concerned they may experience privacy stigma, but have not actually experienced it	"I am pretty sure they would just tell me to suck it up"
Privacy stigma - occurrence	x expresses that they have experienced privacy stigma	"They told us not to bother complaining about it"
Proctoring practicalities	x expresses concern around the practicalities of proctoring ahead of privacy concerns	"From the sounds of it, you are not able to access water for hours on end"
Proctoring privacy	x expresses concern around the privacy of proctoring ahead of the practicalities	"A random person is just there watching me sitting an exam"
Pseudonym	x uses a pseudonym to protect their privacy	"I use my middle name as my surname on Facebook"
Surveillance - concern	x expresses concern regarding surveillance capabilities	"I don't like that lectures are able to take attendance and see who attends lectures"
Role of government	x expresses privacy concerns because of their perceived role of government	"I just don't think the government should have that role"
Social calculus	x makes a privacy decision based on the perceptions of others	"People want to be perceived as doing the right thing"
Societal benefit	x makes a privacy decision based on the good of someone other than themselves	"If we can save lives and prevent massive economic loss then that is good"
Support system - established	x has an established support system in place	"We haven't been alone, [neighbour] has been helping us out"
Symptom tracker - perceptions	x expresses an opinion about the ZOE Symptom Tracker	"I think it is such a good initiative"

Symptom tracker - reasons	x expresses a reason for using the ZOE Symptom Tracker	“It feels like I am proactively doing something that helps people”
Symptom tracker - usage	x gives supplementary information around how they use the ZOE symptom tracker	“I have been inputting my symptoms into it every day since about April”
Technology repurposing - occurrence	x is using a technology for a purpose which it was not originally intended	“Like everybody, I am now using Zoom for social stuff, as well as work stuff”
Technology repurposing - concern	x is (not) concerned about using a technology for a purpose which it was not originally intended	“Zoom for social is no different than Zoom for work for my privacy”
Tool disuse - action	because of privacy concerns, x stops using a tool	“I had to un-download the Google Play store app”
Tool use - business communication	x uses a tool for the purpose of business communication	“We tend to use Slack to communicate”
Tool use - VOIP	x uses a tool for the purpose of video communication	“I have been using Zoom for my meetings with clients”
Tool use - proctoring	x uses a tool for the purpose of exam proctoring	“We have all had to download a proctoring tool for our exams”
Trust	x makes a privacy-related decision based on trust of platform or information recipient	“It might make be a bit of a snob but I trust it because it is a university”
Unfriending - action	x takes privacy action to ‘unfriend’ their connections	“I had to unfriend my mum as she kept posting too many pictures of me and my brother”
Vocational privacy	x expresses privacy concerns or requirements as a results of their vocation	“I have to protect the privacy of my patients”
Work background - concern	x is concerned about their work background when they are working with their camera enabled	“I don’t like that my class-mates can see my bedroom”
Work background - action	x takes action to alter their work background because of privacy concerns	“I have moved my desk to give an empty wall behind me”
Work background - reasons	x provides a reason for the action/inaction they take in relation to their work background	“The process is already confusing enough already without having to think about a virtual background”
Work-life divide - decreased	x expresses that they feel that their work-life divide has decreased (may be latent)	“I feel like my work life and my home life are getting too close”

Table 2: Final code book

C Interview Question Formulation

This appendix illustrates how Social Practice Theory shaped the process of interview question formulation.

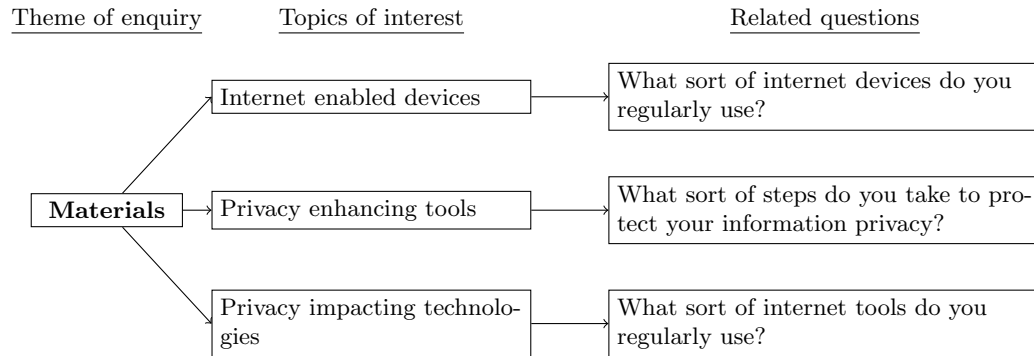


Fig. 1. Questions related to practice elements: Materials

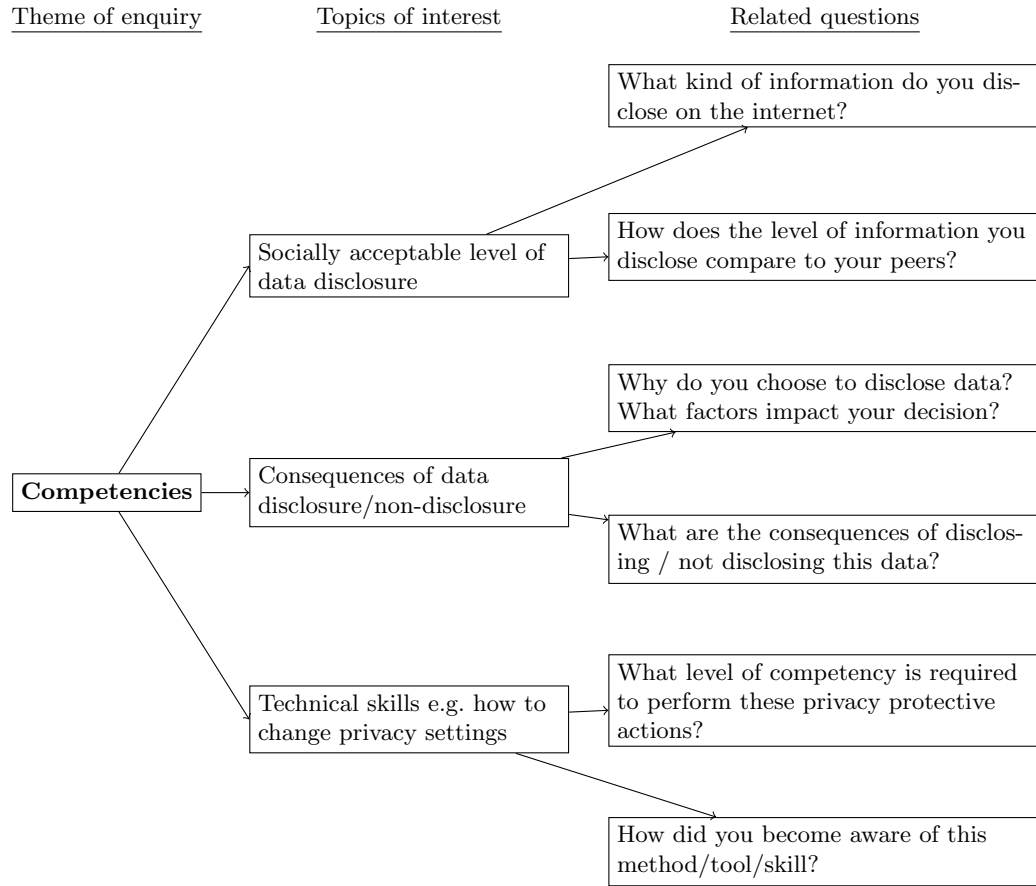


Fig. 2. Questions related to practice elements: Competencies

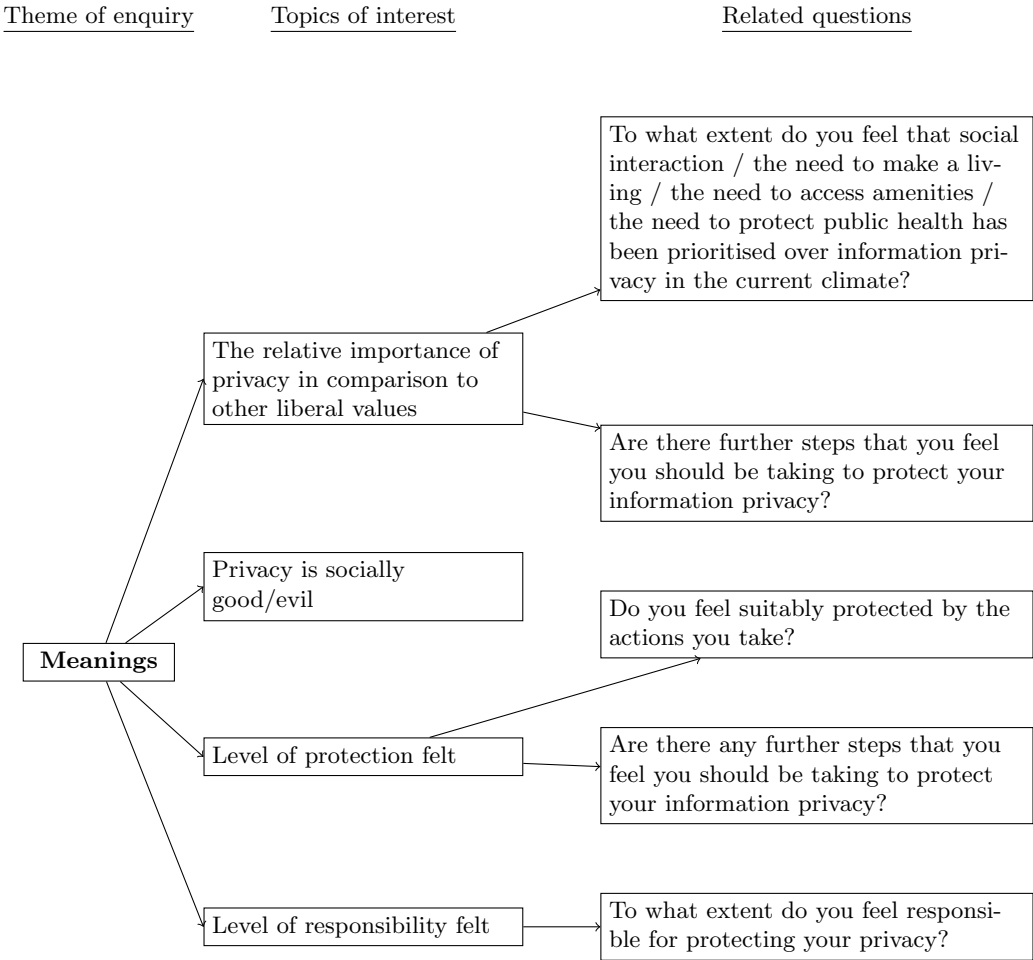


Fig. 3. Questions related to practice elements: Meanings

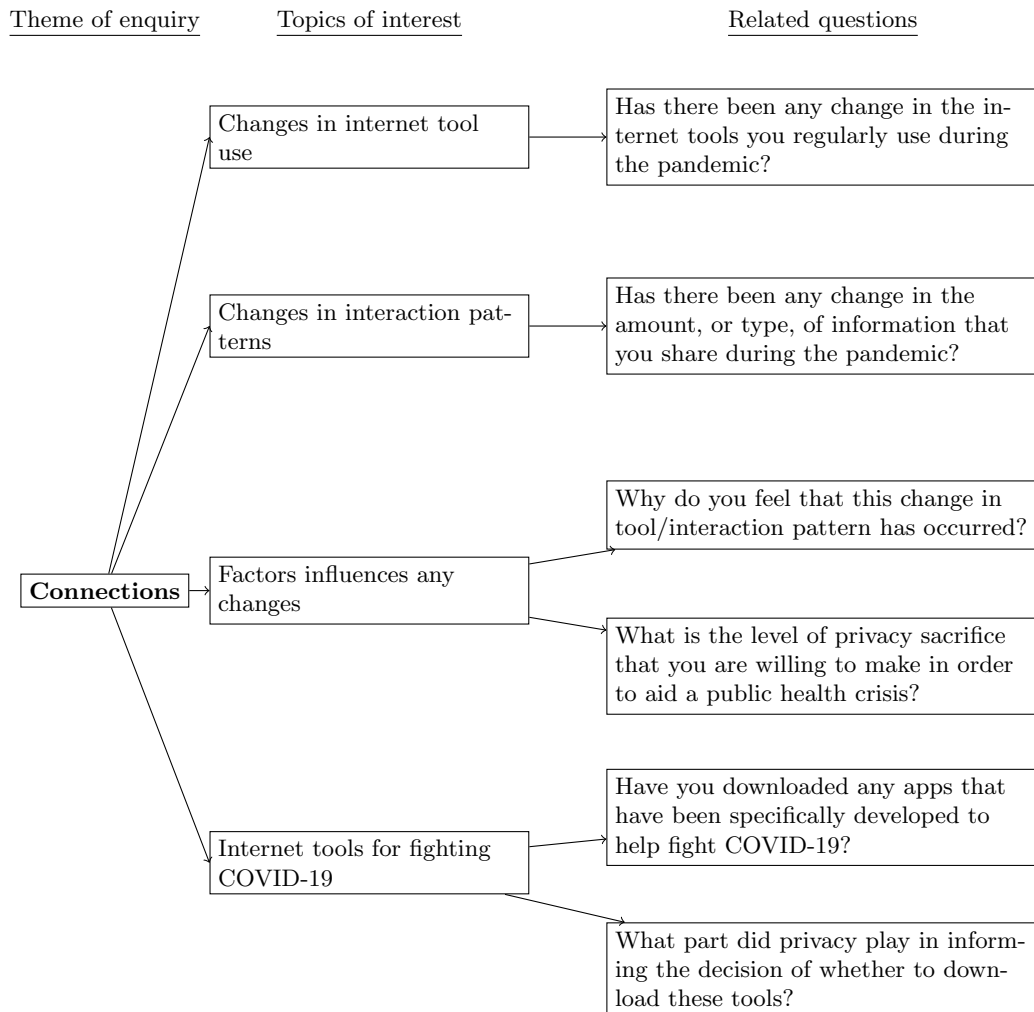


Fig. 4. Questions related to practice elements: Connections