


Please cite the Published Version

Nicol, Emma, Briggs, Jo , Moncur, Wendy, Htait, Amal, Carey, Daniel Paul, Azzopardi, Leif and Schafer, Burkhard (2022) Revealing cumulative risks in online personal information: a data narrative study. Proceedings of the ACM on Human-Computer Interaction, 6 (CSCW2). p. 323. ISSN 2573-0142

DOI: <https://doi.org/10.1145/3555214>

Publisher: Association for Computing Machinery (ACM)

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/632089/>

Additional Information: This is an Accepted Manuscript of an article which appeared in final form in Proceedings of the ACM on Human-Computer Interaction, Copyright © 2022 Owner/Author

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

Revealing Cumulative Risks in Online Personal Information: A Data Narrative Study

When pieces from an individual's personal information available online are connected over time and across multiple platforms, this more complete digital trace can give unintended insights into their life and opinions. In a data narrative interview study with 26 currently employed participants, we examined risks and harms to individuals and employers when others joined the dots between their online information. We discuss the themes of *visibility and self-disclosure*, *unintentional information leakage* and *digital privacy literacies* constructed from our analysis. We contribute insights not only into people's difficulties in recalling and conceptualising their digital traces but of subsequently envisioning how their online information may be combined, or (re)identified across their traces and address a current gap in research by showing that awareness is lacking around the potential for personal information to be correlated by and made coherent to/by others, posing risks to individuals, employers, and even the state. We touch on inequalities of privacy, freedom and legitimacy that exist for different groups with regard to what they make (or feel compelled to make) available online and we contribute to current methodological work on the use of sketching to support visual sense making in data narrative interviews. We conclude by discussing the need for interventions that support personal reflection on the potential visibility of combined digital traces to spotlight hidden vulnerabilities, and promote more proactive action about what is shared and not shared online.

CCS Concepts: • **Human-centered computing** → **Human computer interaction (HCI)**; **Empirical studies in HCI**; • **Security and privacy** → **Social aspects of security and privacy**;

Additional Key Words and Phrases: Human Computer Interaction, Research design, Cybersecurity, Personal data, Digital traces

ACM Reference Format:

. 2022. Revealing Cumulative Risks in Online Personal Information: A Data Narrative Study. In *Proceedings of CSCW '22: THE 25TH ACM CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK AND SOCIAL COMPUTING (CSCW '22)*. ACM, New York, NY, USA, 24 pages. <https://doi.org/xxxxxx>

1 INTRODUCTION

Our connections to diverse online services through multiple personal devices make it increasingly difficult to keep track of what we are disclosing about ourselves online via our digital traces. These traces include those that arise from people sharing their own personal information online, others sharing information about them, and via e.g., automated functions that make additional metadata public, such as disclosing one's location when posting on Instagram. Sharing may be intentional, unintentional or inadvertent. People are connecting digitally with others for professional and social reasons, via an increasing diversity of channels. Such diversity means that networks supporting interaction and collaboration with others are evolving in ways that are complex and difficult to mentally model. The challenge of understanding how one's data is being shared in and across these networks grows with this complexity.

A substantial body of research has examined how an individual's digital traces may be used to discover or infer information about them — their interests, livelihood, place of work, whether they are depressed or likely to self-harm, relationships, sexual orientation, political opinions, religion and other preferences — even when not explicitly disclosed [37, 43, 83]. Smartphone use alone can reveal much, based on information including accelerometer and GPS

Publication rights licensed to ACM. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the United States government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.

© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.

Manuscript submitted to ACM

53 data, app usage patterns, call logs and Bluetooth proximity [27]. Revelations include the phone user's identity, mood,
54 stress levels, personality, whether they are a parent, likely destination when travelling, whether they are sitting/walking
55 or running, and the quality of their sleep [27]. When combined over time and across multiple digital channels — e.g.,
56 Facebook, LinkedIn and Tinder — this array of digital traces can afford unintended insights into people's lives as private
57 individuals, employees, and citizens. Combined digital traces may also reveal unintended insights about employers, and
58 even about national security.

60 These insights are significant — from them, we can learn just how much we are revealing about ourselves online, not
61 just about our past and present, but also about our future: "...fragments of past (online) interactions or activities ...,
62 when correlated together, allow a preemption and prediction of future behaviors" [66, p250]. Insights are also relevant
63 to hostile actors — e.g., fraudsters — who can make use of coherent, combined digital traces to gain advantage over
64 their victims.

66 In this research we investigate:

- 68 • The everyday online information sharing practices of employed people, and their associated awareness of how
69 pieces of personal information — digital traces — can be connected over different online channels over time;
- 70 • To what extent people recognise how their connected traces are available to others, potentially to be explored
71 as a more coherent whole;
- 72 • What this more coherent whole could convey about an individual, including insights into their apparently
73 private self (e.g., behavior, values, habits etc.);
- 74 • How aware people are of the potential harms and hazards of how such insights could be used against them, and
75 by whom.

79 We took a holistic approach, acknowledging the interconnectedness of online practices [51, 82]; the networked
80 nature of online identity [52]; and use of multiple digital channels (e.g., social networking sites, IoT, apps), devices (e.g.,
81 personal smartphones, Wi-Fi-enabled devices at home, work computers), and behavioral patterns that are determined by
82 the affordances of particular digital technologies (e.g., GPS data of fitness apps) [28]. We conducted 26 semi-structured
83 interviews to (i) solicit insights into interviewees' digital ecosystems across multiple communication channels, sharing
84 networks and devices plus associated behavioral patterns and practices; (ii) explore co-constructed aspects of participants'
85 online identities across apparently discrete channels of information and; (iii) identify experiences and consequences
86 where combined digital traces revealed more than intended.

89 All participants in this study were residents of the United Kingdom (UK), and subject to the protection of the EU
90 General Data Protection Regulation (GDPR) in tandem with the UK Data Protection Act 2018 (DPA) [50]. However,
91 following the 2016 referendum at which the UK decided to leave the European Union, the GDPR stopped being directly
92 applicable. We were mindful of this uncertain context while conducting the study and we therefore acknowledge the
93 implications for our participants and findings in our discussion.

95 We first situate our study in the context of prior work on digital traces, cybersecurity, and the workplace, before
96 going on to outline our data narrative interview method, accounting for the necessary changes to its design during
97 Covid-19 related Lockdown conditions. We then present the results of our thematic analysis across three themes:
98 *visibility and self-disclosure*, *unintentional information leakage* and *digital privacy literacies*. We discuss issues around
99 soliciting people's recollections and understandings of their digital traces across networked space and time. Our
100 contribution comprises insights not only into people's difficulties in recalling and conceptualising their digital traces
101 but of subsequently envisioning how their information may be combined, or (re)identified across their traces. We also
102
103
104

105 contribute insights on the inequalities of privacy, freedom, and legitimacy that exist for different groups with regard
106 to what they make or feel compelled to make public online and the privileges that are enjoyed by some but not by
107 others. Finally, we make a methodological contribution on the use of sketching to support visual sense making in
108 the interviews, inviting new perspectives on researching personal online information interactions, and building on
109 previous studies in CSCW that used this method in other contexts. This set of interviews represents a step towards
110 our overarching research goal to identify the need for tools or other designed interventions that support not only
111 personal reflection on the potential visibility of combined digital traces, but that additionally support the curation of
112 one’s existing traces, retrospectively.
113
114

115 2 RELATED WORK 116

117 Our study takes a socio-technical approach to the cybersecurity risks emanating from people’s digital traces. We
118 interpret cybersecurity from a post-digital perspective, where “the protection of technology and information has
119 become so intermingled with the protection of people and society that distinguishing between the two is impossible.
120 ... in a post-digital society, technological security rests upon the protection of people, and vice versa” [21, p10]. Prior
121 work by Dunphy et al. [26] at the intersection of design and cybersecurity has focused on people and their experiences,
122 while government agencies such as the UK’s National Cyber Security Centre (NCSC) have now introduced cybersecurity
123 guidance “for anyone looking to develop security which works for organisations and for people” incorporating a design
124 orientation [58]. Our specific focus is on combined, intersecting digital traces, and we frame our work against this
125 backdrop, first defining digital traces for the purposes of this paper and explaining how they can be (mis)used, and the
126 digital literacies that affect people’s understanding of how they ‘look’ online.
127
128
129
130

131 2.1 Defining Digital Traces

132 Our digital traces are multi-dimensional. We leave traces of personal information across multiple digital platforms
133 and across time. Such traces are generated [66] before we are born, across the lifespan [63], and even post-mortem
134 [57]. Even in childhood, there is a multiplicity of apparently innocuous channels via which personal information is
135 often shared – for example through connected toys; children and parents posting on social media; biometrics used for
136 schools’ fingerprint charge accounts [80]. Brandtzaeg and Lüders [17, p2] highlight that it is “increasingly important to
137 understand how *time* is perceived in the context of a non-anonymous social media environment” (authors’ emphasis),
138 as digital traces over time can reveal much, not only about our current selves, but also about our past opinions, actions
139 and feelings.
140
141

142 Digital traces emanate from the central actor, using their real name and pseudonyms. They also emanate from a range
143 of other actors – e.g., health providers; employers (including through productivity tracking [9]); government agencies
144 (including public registers of companies) – serving to produce a co-constructed digital identity for individuals [79].
145 In addition, people’s personal information can surface through other channels, posted by friends and acquaintances,
146 and also by government sources (e.g., voter registers) and other organisations (e.g., that collate and create dossiers on
147 individuals).
148
149

150 While these traces are spread across multiple locations, with subsets of information shared with specific audiences,
151 boundaries between the platforms and audiences are known to be porous. Context collapse, “in which individuals
152 must meet the expectations of multiple and diverse audiences simultaneously” [17, p2] is a recognised phenomenon.
153 Embarrassing and harmful situations can arise through context collapse, when users try to navigate multiple, diverse
154 audiences on the same platform: they may accidentally blur borders between the public and the private, the professional
155
156

157 and the personal – leading to information leakage [23]. However, Costa [22, p3652] found that context collapse was
158 not a given, and was “a result of situated practices of social media usage within Western Anglophone contexts”. Her
159 Turkish participants ably navigated complex security settings to ensure that boundaries between online groups were
160 maintained.
161

162 **2.2 Use of combined digital traces**

163 There are tools available that enable individuals to make sense of their digital traces in certain contexts. For example,
164 quantified self, personal informatics, and life logging tools can give people a better understanding of their own behaviors,
165 through recording, measurement, visualization and publication of their own data [29, 45, 66, 71]. Coherently combined
166 traces – e.g. geolocation, step count, heart rate – can become material for conversation and expression of personal
167 identity, and/or to improve behavior or performance in a particular area, and form “highly personal accounts of (users)
168 pasts” [29, p518]. The utility of combined digital traces extends beyond the individual: exploitation by others can afford
169 unintended insights and privacy violations, potentially adversely affecting individuals, employers and organisational
170 security.
171

172 Approaches to exploiting digital traces may be manual or involve the use of specially-developed tools. ‘Lurkers’ –
173 especially adolescents – may trawl the social media feeds of friends and followers for updates and juicy titbits, joining
174 the dots between posts to work out more than was intended to be revealed ¹. More seriously, perpetrators of intimate
175 partner violence may go to great lengths online to track down their victims (survivors) through their digital traces
176 across multiple platforms, in order to continue their abusive behavior [35]. Examples of tools developed to harvest
177 digital traces include a Blockchain-based application that enabled people to establish others’ trustworthiness [84], and
178 a tool that combined online dating site posts with fitness tracker information to reveal where people lived, whether
179 they lived alone, and when they were at home or out exercising – information that was subsequently exploited by
180 stalkers [20]. Using Facebook profiles, Bachrach et al. [8] were able to infer people’s Big Five Personality traits. Other
181 initiatives have sought to predict from Twitter and Reddit posts whether people are depressed, suffering from anorexia,
182 or likely to self-harm [46]. On a larger scale, and beyond our current focus on an individual’s interpretation of combined
183 digital traces, automated Big Data approaches can use these same traces to assemble insights into people’s behavior and
184 to predict e.g., the likelihood of someone repaying a loan or developing diabetes [65], someone’s political leanings [62],
185 their propensity for criminal behavior [55], and their mental health [47].
186

187 Efforts to exploit digital traces can be facilitated via lax security and privacy settings and behaviors. A large scale
188 example of this lies in the lax security applied to social networking sites in Runet (the Russian Segment of the Internet),
189 leading to 30 million profiles becoming publicly available to download [41, p50]. The profiles included users’ personal
190 and intimate details such as “sexual orientation, sex frequency and preferences in sex”, along with “personal information
191 like weight, height, smoking habits, alcohol, drugs, body characteristics... dwelling type, marital status, and religion”.
192 While this information may have been disclosed to circulate within the particular context of e.g., a dating site, it became
193 more widely available, exposing people’s intimate details to a wider audience than was ever intended [41]. On a smaller
194 scale, when parents share posts and pictures of their children (“sharenting”) without consent, they add a dimension
195 to their childrens’ online identities that may be at odds with how their children wish to appear online, skewing their
196 digital traces [64]. Meanwhile sharing posts and photos about friends may unwittingly reveal private information about
197 them (e.g., details of companions or associates, locations, activities etc).
198
199
200
201
202
203
204
205

206
207 ¹<https://psycnet.apa.org/fulltext/2017-07146-004.pdf>
208

209 Even when people actively separate their digital identities across different online channels to organize their social
210 groups or to obfuscate aspects of their identity, their efforts can be undermined by re-identification, involving the
211 linking together of profiles and other information [36]. For example, the Personal Genome Project ² linked profiles to
212 online voter lists via e.g., birthdate, zip code — destroying the assumed anonymity of the profiles [76]; Facebook profile
213 images tagged with real names were used to re-identify people on other sites (e.g., Friendster, Match.com) that host
214 otherwise anonymous profiles [36].
215
216

217 **2.3 Employees, Employers and Organisations**

219 Social media content is used by up to 80 percent of employers and recruitment agencies as part of their assessment
220 of candidate suitability for a post [74]. Young and Quan-Haase [85] found that applicants' chances of acceptance for
221 advertised job positions could be adversely impacted by their openness online about e.g., health conditions or pregnancy.
222 Employees can face dismissal for their conduct on social networking sites, even when posting outside of working hours
223 [78]. Thornthwaite [78, p119] observes that social media is “blurring the legal distinction between employees' public
224 and private lives, increasing employer control over personal lives in ways reminiscent of traditional master–servant
225 relationships”, the effects of which are then tested in industrial tribunals, which increasingly challenge employers'
226 intrusive stance.
227
228

229 Employees' social media activities also have the potential to negatively impact on their employers by unintentionally
230 leaking sensitive information online — such as trade secrets, intellectual property and personal details of other employees.
231 This can represent a significant security risk to organisations “result(ing) in a loss of competitive advantage, loss of
232 reputation, and erosion of client trust” [4, p351]. Irresponsible posting can result in damage to employers that goes way
233 beyond their reputation. There have been instances of military personnel and their families discussing operations and
234 deployment details on social media, even posting pictures of ongoing operations [25]. In a recent case, staff living on a
235 UK nuclear submarine base exposed compromising information via their use of the Only Fans pornography-sharing
236 website [56]. Adversaries motivated to exploit such information can seek out service personnel or their family members
237 to blackmail them, or use the intelligence gathered to attack or infiltrate deployment locations.
238
239
240

241 **2.4 Digital Self and Contextual Privacy**

242 The work of boyd e.g., [13][14] [15] and boyd and Ellison [16] drew from Goffman's notions of impression management
243 [32] to articulate the necessary maintenance and updating of “front stage” digital selves and online identities, and
244 discrepancies between what one “gives” — in explicit displays of friends, interests and online representations — and
245 “gives off” as interpreted by others, and as amplified in networked publics [13][14]. boyd's early work with young
246 people also found that they cared deeply about online privacy, and recognised the value of both privacy and publicity,
247 understanding them as contextual and adjustable, the latter especially with regard to being socially present and acquiring
248 social status. Indeed, self-disclosure is a key factor in developing relationships and building trust in online environments,
249 much as it is in face-to-face contexts. This self-disclosure includes actions such as deliberately sharing selected personal
250 photographs [24], and represents a negotiation of privacy, with information often shared with selected (groups of)
251 online network members, rather than with all network members [53].
252
253

254 This crafted, contextually-situated privacy is subject to the pressures of normativity. When flows of information
255 adhere to entrenched norms, there are few concerns, whereas when violations of norms occur, protest and complaint
256
257
258

259 ²<https://www.personalgenomes.org/>

often result [60]. For example, a patient may be comfortable with healthcare providers sharing medical information with specialists, but very uncomfortable when the same data is shared with marketing companies (see also Bussone et al. [19]). When considering contextual privacy in workplace or organisational settings, we can look to the work of e.g., Ashenden [7]. This work found that employees who believed their employer was driven by the need to protect information thought risks to be overstated and colleagues overly cautious, whereas those who believed the organisation was driven by a need to optimise information use, thought security risks justified and colleagues' behavior risky. McDonald and Forte [54] have drawn attention to the limits of concepts such as contextual integrity and boundary regulation when thinking about privacy in Human Computer Interaction (HCI). They revealed conceptual gaps in current frameworks and have argued for considering vulnerability i.e. of particular groups of people as a core concept when thinking about privacy. Researchers in CSCW have highlighted serious issues with digitally-mediated identity management, with the effects often being pronounced for those considered vulnerable e.g., Simpson and Semaan's work on algorithmic identity investigated and confirmed concerns that the short video sharing application TikTok was suppressing the individual identities of LGBTQ+ users via algorithmic and human moderation [73]. Seberger et al. [70] showed how users navigate trade-offs involved in app use. Despite technical and regulatory mechanisms aimed at empowering users to manage their privacy, people have a sense of resignation around privacy due to the convenience offered by apps: there is a fine line between feeling empowered by technology and the discomfort of invasive app behavior. Users are often resigned to disclosing data even as they accept personal responsibility for their own privacy.

2.5 Data Leakage

People can often be surprised when they discover the personal data collection and distribution activities of apps that they use. Shklovski et al. [72] showed that people felt personal space had been violated in “creepy” ways by apps with the creepiness lying in the realization that apps were conduits for personal information and space to “leak” to unknown entities who had not explicitly been invited in. These authors link creepiness to notions of personal space and territoriality [5], and to contextual integrity [59]. People will formally agree to the information sharing undertaken by apps, and can rationalize their use of them when asked, putting any creepiness out of their minds. Nonetheless, the creepiness remains. [72] further suggest that there are harmful health consequences of this enduring creepiness while acknowledging that such creepy experiences may not always be negative and unwanted; and pose an interesting question as to whether such creepiness fades over time suggesting that as cultural norms change, so too will the conditions under which such creepy experiences are encountered, which has implications across the digital lifespan.

2.6 Digital Privacy Literacies

A person's ability to generate digital traces online does not imply the accompanying presence of digital privacy literacy, that is, an understanding of how information travels when shared online, and the associated risks. Digital privacy literacy is an area of education and practice often used in social justice and/or public education programmes, including those run by public libraries to help develop competencies in groups of people at particular risk, including those who rely on public library computers for personal digital communications and information practices, particularly those who are subject to social inequalities (see e.g., [2]). Digital privacy literacy can be considered distinct from the well-established, if rather broad area of *digital literacy* (e.g., [44]), which refers to an individual's multiple competencies, from having regular access to and basic functional operational skills (e.g., using a keyboard and mouse) along with being able to “read” and “write” clear information across a number of digital modes using these apparatus, including in textual, visual and wider forms of communication media [44]. Digital privacy literacy can be regarded as a subset of *data literacy*, and

313 is used to refer to a range of competencies around understanding and communicating with informational data, which
314 often relates to privacy and (personal) data, and goes towards enabling one's personal data self-care.

315 In the social sciences, the growing literature on critical data studies e.g., [42], includes [49] Lupton's notion of
316 the "lively" aspects of personal data, as they are added to, and (re)configured by human interpretation and corporate
317 segmentation/analyses. Lupton notes that personal data, as (partly) human, is typically represented visually and in
318 language as organic and material (e.g., flows, breadcrumbs) or "humanised" as e.g., footprints (p47). People's encounters
319 with the personal data that they generate via use of digital technologies presents them with challenges as to how to
320 interpret, control and make sense of these data. Lupton elsewhere [48] has argued that such data and their circulations
321 could be made more perceptible and interpretable using what she describes as three dimensional materialisations,
322 recognising that people's interactions with such re-presentations of personal data elicit visceral responses. There
323 are also new research areas around human data interaction that include designing frictions into user experiences of
324 technologies to promote critical reflection, e.g., prior to sharing information; and on interaction design's dark patterns,
325 which comprise e.g., targeted manipulation and confusing terms of service [34], widely adopted by industry to nudge
326 people into a particular course of action, including coercing people into disclosing personal data, often beyond that
327 necessary for the task in hand.
328
329
330
331

332 3 METHODOLOGY 333

334 We conducted an interview study using a data narrative approach [82] in order to understand the risks and consequences
335 of the digital traces that people leave online. This approach served to capture participants' descriptions of their data,
336 device use, channels and networks of communication, and data and information practices. Using this approach also
337 allowed us to capture the co-constructed aspects of a person's online identity, as well as enabling the investigation of
338 direct and observed experiences of, in this case, the cumulative implications of digital traces.
339
340

341 3.1 Interview Study 342

343 We conducted the study in May-July 2020. Due to the physical distancing requirements of the Covid-19 Lockdown in
344 place in the UK at the time of the study, we had to conduct interviews remotely via videoconferencing, which we took
345 care to pilot before the interviews. We engaged with participants in advance by sending information sheets by email.
346 Cognisant of the likely effects on data sharing that might arise due to the circumstances of the Lockdown, we added
347 questions to the interview schedule regarding changes to data-sharing habits and experiences, with the intention of
348 capturing the effects of self-isolation, homeworking and other Lockdown-related phenomena (Appendix A).
349
350

351 3.2 Participants 352

353 We recruited 26 adults (13 male, 12 female, one non-binary; age 20 – 59 years, median 37 years) to take part in the
354 study. All were based in the UK, active online and in full-time employment. We recruited participants by creating an
355 advertisement that was circulated via emails to contacts with access to mailing lists to be shared more widely, and
356 via social media, with the offer of a £20 shopping voucher for participation. We aimed to recruit participants from a
357 variety of employment roles and sectors and made sure there was roughly equal representation from employees in the
358 public (n=16) and private sectors (n=10) and that staff recruited represented all levels of seniority. Participants were
359 employed in sectors including healthcare, education, engineering, management, IT and hospitality and were drawn
360 from city, suburban, town and rural locations. 21 participants reported speaking English as their first language, four
361 spoke it as a second language and one was bilingual in English and another language. 13 had postgraduate qualifications,
362
363
364

10 were qualified to undergraduate level, two had qualifications from further educational studies and one had high school qualifications. When we asked about their level of technology skill (the interviewer read out the full definition of each category to each participant) they responded as follows: four said “Low/Low-Medium” indicating basic use of software, hardware and social media; 15 said “Medium” indicating confidence with using and integrating a variety of standard software packages over a number of platforms; seven said “Medium-High/High” including the use of specialised software and an ability to program. At the time of interview, 18 participants were working at home full time, five split their time between working at home and at their workplace, while three reported no home working.

3.3 Method

The first author conducted all interviews, with each lasting 60-90 minutes. In a short briefing, we invited participants to ask questions about the study based on their reading of the information sheet. They then provided consent verbally. We then asked participants to complete a technology questionnaire via a SurveyMonkey link, delivered via the Chat function of the videoconferencing software, or sent by email. We designed the questionnaire to capture participants’ self-reported use of technology including devices, communication channels, data storage and social media networks (Appendix B). In addition, the interviewer asked participants a short series of questions regarding their current employment, level of education, and their understanding of and confidence in using digital technology.

Interview questions were centred on the following areas and are detailed in Appendix A: (i) information about communications channels, apps, data storage/management systems, and devices used, including whether/how any of these were shared; (ii) everyday practices and behavior patterns around e.g., conducting searches, posting and other digital information sharing; (iii) participants’ awareness of the unanticipated potential for self-disclosure through digital traces and their associated level of concern; (iv) information management, security setting behaviors and Lockdown-related changes – especially regarding working from home; (v) we asked participants to envision a scenario where someone else had to write a book about them based only on their digital traces, and to think about what the resulting book would comprise. We finished by asking them to summarise their advice to others on optimising their information security. We tailored the questions, where appropriate, through answers provided in the technology questionnaire.

We supplemented the interview questions by asking the participants to hand-draw sketches of their digital eco-system on paper. Having participants sketch as part of interviews, has its roots in Cultural Probes [31] and has been used successfully within the Human Computer Interaction (HCI) and Computer Supported Cooperative Work communities in a number of study contexts. For example [40] asked participants to draw a map of their finances to understand how people track money. Building on work by e.g., Ryan et al. [68] on mapping interactive digital artefacts, Vertesi et al. [82] used the data narrative approach to promote people’s descriptions of how they manage their personal data. Drawing was used to facilitate more thorough conversations, to elicit grounded comments about data practices and examine conceptions of personal data space. Vertesi et al. [82] argue that drawing during interview allows the remembering of new stories, the discovery of forgotten elements, and the visual expression of relationships between devices and data. The drawings produced are not a test of a participant’s precision or recall with regard to their digital ecosystem, rather, they give structure to the interview process as tools with which to think [82]. Memory aspects aside, asking participants to engage with their personal information sharing in this way rather than, for example, simply talking about it or using their devices as the main support, exploits the power of defamiliarization described in work by e.g., [11] to invite participants to have a new perspective on familiar aspects of their lives.

In the current work, participants were asked to come to the session prepared with pen/pencil and paper. They were asked to sketch out their communications channels, devices, types of information shared/intended recipient(s), along

417 with whether usage was in a personal or professional capacity, and (separately) whether they were using a personal
418 or professional account. The process of drawing the sketches proceeded throughout the interviews with participants
419 adding to them as elements were remembered. Participants were also asked to identify and draw any links between
420 media, devices and the public or private aspects of shared information. Participants were later asked to photograph and
421 email the final sketched maps to the interviewer (21 sketches were returned from 26 participants). We have included two
422 example sketches in Appendix C to illustrate the variation in approach and reflecting the uniqueness of each individual
423 in the study and the personal nature of their digital ecosystem.
424

425 We made audio recordings with participant consent, and coded anonymised transcripts by performing thematic
426 analysis [18], using NVivo. Our analysis took a hybrid approach (see also [69]): existing concepts were used for deductive
427 coding while new concepts grounded on the empirical data from the interviews, contributed to the inductive coding.
428 The deductive coding included, for example, concepts from technology law literature on personal information such
429 as Right to Erasure and pseudonymous posting [67] and on the participants' desires or requirements for a tool to
430 manage their digital traces. The resulting coding list was iteratively refined in the light of the interview data, as new
431 codes emerged. One author did the early coding, undertaking frequent code review sessions with another author
432 to help remove potential biases. The list of preliminary codes was then distilled further into a set of refined codes
433 (Table 1 in Results) that corresponded with a high number of instances across the transcripts, or that captured novel
434 emerging design ideas or relevant practices. All authors were involved in three data sharing meetings and arrived at the
435 designations of the refined codes through discussion. Further iterative analysis and clustering resulted in the three final
436 themes: *visibility and self-disclosure*, *unintentional information leakage* and *digital privacy literacies*. From an original
437 list of six themes, *visibility and self-disclosure* arose from the combination of themes of visibility, self-disclosure and
438 identity curation, *unintentional information leakage* was one of the original themes, while themes of conceptions of
439 overview of own data and data concerns were combined into one as *digital privacy literacies*. Each theme is discussed in
440 turn below illustrated with pseudonymous quotes.
441

442 4 RESULTS

443 We now discuss each of our themes in turn (see Table 1 for details of the codes that comprise the themes), illustrating
444 points with verbatim quotes. While participants' ages are reported, all names have been changed and other identifying
445 information omitted to protect interviewees' privacy.
446

447 4.1 Visibility and Self-disclosure

448 *4.1.1 Curating an online profile.* Creation or maintenance of online identities was mentioned by many of our partici-
449 pants: ten spoke about creating or maintaining professional online profiles while five spoke about their curation of a
450 non-professional online identity. Attitudes to having a presence and being in/visible online had an age dimension. On
451 the whole, younger participants (18-25 years) were those who were more likely to speak about the vital importance of
452 having an online presence especially in enhancing, even enabling one's career. Xander, a recent graduate now working
453 for a student organisation, had a good understanding of how his online information was received and judged by others;
454 he had even been researching how sharing personal information online comprised a form of self-commodification:
455

456 *To be successful, whether it's on social media, just to get likes, or whether it's in a professional sense... you*
457 *are your brand and you need to sort of, I don't know, show that in every single way you do online, and so I*
458

469 *am just careful about what I post, whereas I know that some other people aren't, and it can look quite bad.*
 470 (Xander, 22)
 471

472 Meanwhile, five participants expressed awareness that online traces only ever provided a partial picture, albeit an
 473 authentic representation of someone, and as such invited interpretation. Una, a clerical assistant commented:
 474

475 *I think it's a true snippet of who I am. But I think that it is just a snippet, because I don't post about*
 476 *everything....I wouldn't be concerned. I think people make judgements no matter what you put out there,*
 477 *so they have a snippet of what it is! (Una, 21)*
 478

479 While not expressing particular concern, Una touched on the potential for inferences to be drawn from incomplete
 480 traces, and also on how some interests lend themselves more to being documented and shared, saying: "I play a musical
 481 instrument, but that is nowhere on my social media, and not many people know how musical I am... [but] they know
 482 I'm maybe quite sporty, but they don't see the musical side" (Una, 21). As part of his youth worker role, Calvin recruits
 483 others to work with the young people for whom he has safeguarding responsibilities on on whom he carries out
 484 informal background checks online – while also mindful of the limitations of these:
 485
 486

487 *One of the first things I do is a basic Facebook search of them...and sometimes that has... created a false*
 488 *narrative ... We had a student on placement, and her photos showed ...this quite ragey, party person. When*
 489 *I met her, they were completely lovely, and those photos didn't represent them fairly. (Calvin, 29)*
 490

491 One participant spoke from bitter personal experience about times when the visibility of information posted online by
 492 them had directly led to their prospects being seriously curtailed: Tom, a bakery supervisor, had been aggressively
 493
 494

495 Table 1. Code Book: themes developed from the interview data with details of the codes that comprise them
 496
 497

Theme	Code	No. Interviews	Occurrences
Visibility and Self-disclosure	Creating/maintaining a professional online profile	10	18
	Curating a non-professional online identity	5	13
	Life Events motivating online sharing	20	43
	World Events motivating online sharing	19	40
	Revealing one's location	10	22
	Pseudonymous posting	6	7
Unintentional Info Leakage	Context missing/partial picture	5	5
	Revealing too much about yourself	8	10
	Things posted by others about you	11	17
	Others revealing more than they intended to	17	23
	Leakage in domestic settings/IoT	4	4
	Leakage due to work/personal boundary blurring	2	4
Digital Privacy Literacies	Postings appropriated to other media e.g., broadcast	5	7
	Google-searching self	14	14
	One's online info being boring/of no interest to others	9	20
	Lack of agency/overwhelmed/resignation to fate	4	5
	Concerns about marketing	10	14
	Inappropriateness	6	9
	Fake news	7	9
Security measures taken	6	10	
Right to erasure	15	21	

521 confronted at interview with examples of jokes he had posted online. This left him feeling “humiliated” and his job
522 interview drew to an abrupt close (Tom, 20). Meanwhile Yan, a civil servant spoke of:
523

524 *...colleagues who had disciplinary hearings...you have to be cautious...on what you put out online, so if*
525 *somebody shares a post.. with ... swearing and questionable humour, that gets around the office....somebody*
526 *might be having a quiet word to someone. (Yan, 23)*
527

528 One interviewee reflected on living with an ongoing tension between feeling they had to promote their visibility online,
529 and protecting their own safety and that of their community. Zara, a third sector worker whose family had sought
530 asylum in the UK, commented that her family’s desire to be invisible online raised questions, including around their
531 legal status, which she perceived as damaging her current prospects:
532
533

534 *I have also met loads of people who were genuinely risking... running for their lives. And any information*
535 *that they put online digitally would be instantly sought out, so they stayed off any kind of digital, social*
536 *media, anything. But then they’re also met with the contrast of needing to put something out in order to*
537 *progress – I’m going to say in a Western country – but, well, that’s not exclusive to Westerners, but just to*
538 *put yourself on show, or otherwise people don’t think you’re legitimate. (Zara, 20)*
539
540

541 Helen, a helpline operator, described how wanting to stay offline had affected a loan application: “I had to put myself
542 back on the public [voting] register, because if you use credit at all, you can’t get it if you’re not on the public register...
543 you get... forced into actually having your name and address out there” (Helen, 56). These experiences demonstrate how
544 a visible online presence can become skewed to tell a particular story. They also give insights into how online privacy
545 can be a privilege, when some individuals must establish and maintain their online representation as a source of public
546 identification — for evaluation and validation by others.
547
548

549 **4.1.2 Motives for Self-disclosure.** As well as talking about the ways in which they disclosed personal information
550 online, participants also described what motivated them to do so. 20 participants described how life events motivated
551 them to increase the amount of information they posted and 19 participants described being motivated to respond to a
552 world event or cause by posting or responding to posts online. These actions revealed online what were otherwise
553 private aspects of themselves.
554
555

556 Regarding special life events, HR manager Anna’s (38) desire to lose weight prior to her wedding involved tracking
557 steps and recording her meals to calculate calorie consumption on her FitBit. In interview she discussed being uncon-
558 cerned about the privacy implications, progressing to the subscription version of the FitBit app to record her menstrual
559 cycle. In contrast, Xander, expressed alarm when a friend posted their university acceptance letter on social media —
560 publicly disclosing an application number, leading Xander to imagine this provoking: “someone sort of malevolent on
561 the other end of the computer that just wants to mess with people” (Xander, 22).
562

563 With regard to causes, when probed, two participants who had claimed to share little about themselves online
564 recalled making public contributions to petitions and fundraising pages, and, also, sharing their full name and location,
565 information that often persists online indefinitely. Queenie, a lab technician commented in interview: “I’ve signed
566 petitions... judging by emails that come in unsolicited, you realise that other people know you’re an animal lover”
567 (Queenie, 55). Xander had unwittingly revealed his address through location tracking after getting involved in a good
568 cause: “The sports club that I’m involved with did... a charity fundraiser, so I downloaded it to... track my runs... you
569 realise that the start and finish point is right outside your front door” (Xander, 22). Meanwhile Patrick, an engineer
570
571
572

573 was cognisant that causes he got involved in online and related affiliations and opinions would persist with possible
574 repercussions:
575

576 *I have some views which are commonly held and not as yet controversial — but I do wonder at some point*
577 *politically if they will become (so). I'm becoming more and more careful about what I post about things like*
578 *that.* (Patrick, 56)
579

580 It is worth noting here that it was younger participants (18-25 years) who most vividly described their public
581 expressions of support for certain causes in terms of obligation. Research assistant Rita had clearly tussled with
582 expressing anything other than her more usual apolitical online self: "I thought that I was doing a very, very bad thing,
583 because I was being very silent on the matter [of the Black Lives Matter (BLM) campaign]" (Rita, 25). Rita consequently
584 contributed to the campaign in her own way by promoting online book lists she had curated about racial injustice.
585

586 Participant responses often linked self-disclosure with wanting to share a particular personal event or to signal
587 allegiance with or opposition to a more universally significant concern. Participants recognised the risks of oversharing,
588 but also, as in posting in support of a social movement such as BLM, of under-sharing — for fear of being seen as
589 uncaring or unaware. Visibility and self-disclosure were perceived as tricky to navigate: even when preferring to
590 maintain a minimal online profile, current norms around recruitment, immigration applications and the financial service
591 industry, for example, often require personal information to be available online in order to assess credibility or eligibility.
592 Participants often implicitly recognised the need to tread a fine line regarding the volume and type of information to
593 put out there. We heard from the perspectives of both recruiters and the recruited, how the absence of certain types of
594 information threatened employment and wider social and professional prospects. This partial picture was recognised as
595 potentially damaging in specific contexts such as job seeking.
596
597
598
599

600 4.2 Unintentional Information Leakage

601 Various forms of self-disclosure can stem from information leakage. Participants mostly talked about unintentional
602 information leakage in respect of their personal (i.e., non-work) information sharing, but leakage due to work/personal
603 boundary blurring was also reported by two participants. Third sector workers Zara and Flora had both resorted to using
604 their personal Facebook logins to set up Facebook accounts for work, having tried and failed to set up dedicated work
605 profiles. This led to their mixing information sources across professional and private accounts, and their professional
606 identities encroaching onto the personal: "It's really difficult to keep a personal Facebook, I think, if your workplace is
607 using Facebook a lot for the way they work" (Flora, 54).
608
609

610 Four interviewees reflected on their experiences of information leakage in their domestic lives. Such leakage could
611 be intimate, if also unintentional and/or somewhat creepy, though some were more relaxed about this than others. Will
612 (24) said he was unconcerned about any potential implications of sharing his passwords with his girlfriend. Meanwhile,
613 teacher Linzi (31) expressed her unease at her realisation that she had been inadvertently sharing details of her plans and
614 contacts with her partner via her calendar, due to device synching. On reflection, she said that while she had nothing
615 to hide, in different circumstances — such as in relationships involving domestic violence and controlling behaviours
616 — this could have been hugely problematic. Another interviewee (Queenie, 55) expressed obvious discomfort during
617 interview when recalling her discovery that her partner could view her Internet searches, including those she had
618 conducted to check particular spellings.
619
620

621 A further instance of information leakage in a domestic setting was described by designer Ben, who recalled instances
622 of inadvertent cross-device leakage. His Smart TV would spontaneously display his neighbour's private smart phone
623
624

625 information: "the TV switched itself on... someone [in the adjoining property] was playing on their phone or something...
626 and if they've clicked a Share button... it sometimes comes through to my TV in the middle of a show" (Ben, 49).
627 These information leakages mostly occurred due to insecure account settings. However, 11 interviewees recounted
628 how things posted online about them by others either unthinkingly or, due to more deliberately malicious actions,
629 were also sources of unintentional information leakage. Healthcare worker Will described how his mother's misplaced
630 pride had potentially serious consequences: "I said (to her) I wanted to join... one of the intelligence agencies. She...
631 posted up, 'My son wants to become a spy, how does he do it?'" (Will, 24). While Will joked, saying this was "a little
632 bit counter-productive" for undercover work, he went on to recount how his mother had also posted details of his
633 confidential military achievements and training exercises on Facebook, including the nature and location of the training.
634 This leakage violated military protocols and created a security risk.
635

636
637 Instances of postings either by participants or people known to them, that had then been appropriated to other
638 media, were reported by five participants. Conversations believed to be private had been recorded and/or more widely
639 (re)shared in a very different, typically much later context, e.g.:

640
641 *A friend of mine... was called out on Twitter for things that he'd said in a private group chat six years*
642 *ago, and... reported to his place of study. It's all cleared up, but it still sort of hit home... people can take*
643 *anything you say and change it to however they see it... I guess if there's any shred of doubt, it can be...*
644 *disastrous.*(Xander, 22)
645
646

647 Delivery driver Vinny (24) found one of his old Tweets embedded in a newspaper article several years after the article's
648 publication. He had concerns about assumptions people might make about his beliefs when seeing the tweet out of
649 context: "it was talking about...outdated cultural stereotypes...and I was wondering why my name was involved in this
650 [article he'd found]" (Vinny 24).
651

652 In contrast to more narrow understandings of data leakage that link it to the use of insufficiently secure settings, our
653 participants reported threats that arose in many other ways. Such threats were apparent through the actions of others,
654 via the re-appropriation of content intended for a specific audience, into new locations and contexts. This revealed the
655 information to a wider public — often alongside personally-identifying, or socio-politically significant information.
656 This might be done with the intent of causing reputational damage, but even in the absence of malicious intent, such
657 combinations of digital traces can lead to revelations, and the associated lack of control that individuals have can
658 be problematic and/or distressing. Our participants' responses also show that the proliferation of Internet of Things
659 (IoT) devices has created new vectors for information leakage. Personal and specifically domestic contexts are where
660 they reported the majority of such experiences, perhaps due in part to the Lockdown context, but also because these
661 instances were those that were the most immediate, identifiable and relatable. Two female participants in particular
662 talked of recently discovering routes via which partners had sight of what had previously been private information,
663 and of their raised awareness, and associated concern.
664
665
666
667

668 4.3 Digital Privacy Literacies

669 The interviews were revealing with regard to participants' digital privacy literacy, their knowledge and understanding
670 of the nature and potential of coherent digital traces, and of their control and personal agency over those traces.
671 Overwhelmingly, participants were aware that there was a great deal of publicly available information online about
672 them. 14 participants explicitly mentioned that they knew this from having previously conducted a Google search on
673 themselves. Jenny, a local government officer, had been disturbed to discover some information related to a company
674
675
676

677 with whom she'd long ago been involved: "it had my full name and address and date of birth, and I was like, 'Whoah!'"
 678 (Jenny, 43) Despite this, none of those who reported having searched for themselves on Google was able to describe with
 679 confidence or accuracy the range of publicly or semi-publicly (for instance, a Facebook account) visible information
 680 across their various online accounts. For those participants who said they had never Googled themselves, when offered
 681 the opportunity to check what was visible online during the interview, they were invariably surprised by the level
 682 of detail about them that was public. Further, slightly more than half (14) of the participants said they had what they
 683 regarded as stringent approaches to information sharing, deletion and account security. For example Olly, an electronic
 684 engineer, recounted one of his practices and the motivation behind it: "I tend to disable search history...my bigger
 685 fear is I am an immigrant into this country... so I think that if I search for something because it was in the news, can
 686 it be connected to me...by mistake?" (Olly, 40). However, this was at odds with some of participants' other answers
 687 during interview. For example, when asked how they would advise a friend with the same digital services as them what
 688 security measures should be taken to secure their information, in the case of all but 6 participants, their answers tended
 689 to be very general and provided few specific recommendations, indicating that they had relatively low levels of privacy
 690 literacy and a lack of awareness around their own information's potential for being compromised.
 691

692 As referenced in the wider results, participants did, on the whole, have a good sense of the long-lasting persistence
 693 of their information, once it was online. However, envisaging the potential effects of connecting apparently discrete
 694 aspects of their online information coherently proved more challenging even with access to their various accounts
 695 and having their sketches to hand. Understandably then, participants struggled to comment on where potential risks
 696 or possible consequences lay where others might connect the same dots into coherent digital traces to potentially
 697 use against them. Where matters of concern were expressed, these related to interviewees being aware of inviting
 698 unwelcome marketing (10 participants), and being targeted by advertised goods, particularly if these were of no personal
 699 interest to them.
 700

701 We found it striking that nine of the participants regarded themselves and the personal information they had shared
 702 online as being of no likely interest to others. Ivor, a writer and teacher, was aware that a great deal of his personal
 703 information was available but was bemused that there could be any interest in it:
 704

705 *They would know where I live. They know who I know, they know who I interact with a lot, they know*
 706 *what I work as, they know what my interests are... They could easily work out any political, spiritual, other*
 707 *viewpoints. They would know what I don't like, they would know what I do like, and not just in terms of*
 708 *products. As I say, I'm quite a boring individual, so none of it would be particularly shocking, and it would*
 709 *struggle to get a PG [UK film classification Parental Guidance: for children 8+] certificate, but at the back*
 710 *of my mind, it's 'why do you want to know all this? Why do you want to harvest all this about everyone*
 711 *and everything?'* (Ivor, 59)
 712
 713
 714
 715
 716
 717

718 This self-identification as "boring", a term used specifically by five participants, was a factor in some interviewees'
 719 lack of motivation around deleting superfluous personal information circulating online. Four further participants used
 720 language such as "dull" or "uninteresting" to describe their postings.
 721

722 In line with the literature, four participants expressed a lack of agency, overwhelm or resignation [10, 38], or
 723 feeling unable to manage and where necessary remove information [61]. Flora, for example, conveyed a sense of being
 724 overwhelmed by her online clutter or, at least, with finding sufficient time to deal with it; the task was clearly not a
 725 priority: "I would take one look at it and go, 'Oh, my God!' and walk away: I've got far too much to do to untangle this
 726 mess" (Flora, 54). Helen meanwhile, mentioned her sense of resignation to fate when asked to make a suggestion for a
 727
 728

729 designed tool or service that could help. She found it difficult to conceptualise and dismissed the notion as she would be
730 unlikely to use one: "I'm not sure what I'd want from it. I think in some ways, I've kind of accepted that the horse has
731 bolted!" (Helen, 56). Another participant shared a compelling first hand experience to support their thinking that any
732 remedial action could only ever be of limited use, and the benefits were unlikely to outweigh the substantial detriment
733 of living in online obscurity:
734

735 *I did have a stalker... I sort of removed everything that I used to have [online], and I just existed in the dark*
736 *for a long time. But it wasn't dark enough, because she did actually come to [my workplace]... so at that*
737 *point I realised there was just no point in being dark on all of these tools, becauseif they want to find*
738 *you, they will. (Matt, 44)*
739
740

741 Participants across all age groups understood how time and a potentially changed future context of a posting affected
742 its significance and 15 participants talked about their right to erase such digital traces. Notably, those in the 18-25 years
743 age group were more likely than older participants to express a desire to delete the digital traces of their younger selves,
744 as these no longer represented the person they perceived themselves to be. Xander, 22 had recently deleted everything
745 on Facebook posted in the years pre-university, while Zara, 20 had increased her privacy settings to prevent others
746 from seeing her childhood postings. As Vinny, a delivery driver explained of the online material most concerning him:
747 "I'd probably delete the stuff from most of my school days... I've forgotten a lot of the stuff I posted back then, but...
748 some of it might be potentially embarrassing" (Vinny 24).
749

750 In summary, participants showed an awareness that they had left digital traces but could not be accurate about
751 how visible their online information was: those who looked were surprised when confronted with the reality. Even
752 with the support of sketching, the majority did not or could not show how their devices and information channels
753 were interconnected. All participants had a sense of the persistence of online information but only rarely did they
754 acknowledge the potential for connections to be made and compromises to arise. Even those who believed themselves
755 vigilant in their approach to personal information sharing could not explain beyond the most basic guidance, how one
756 would secure devices and channels to minimise risks from cumulative revelation. In general, participants lacked agency
757 to undertake remedial action to their digital traces out of a sense of it being too late, not possible to do, or it not being
758 necessary as their traces were "boring" and therefore posed little risk to them. Younger participants were more likely to
759 have actively removed content, often to delete elements of childhood online activity as they moved into adulthood.
760

761 5 DISCUSSION AND CONCLUSION

762 This research focused on employed people's everyday online information sharing practices and their associated levels
763 of awareness of how pieces of personal information — their digital traces — can interconnect over different online
764 channels and media over time. We wanted to find out to what extent people recognised how these connected traces
765 are available to others, to be explored as a more coherent whole; what this coherent whole could convey about them,
766 including their apparently private self (e.g., behaviours, values, routines etc.); and where and to what extent they were
767 aware of hazards and potential harms of how this could be used against them, and by whom. Through thematic analysis
768 of the outcomes of 26 interviews, we uncovered themes of *visibility and self-disclosure*, *unintentional information leakage*,
769 and *digital privacy literacies*.
770

771 *Visibility and self-disclosure* was heavily influenced by necessity and obligation, with some participants feeling
772 compelled to have an online presence when job seeking. This is consistent with Berkelaar and Buzzanell's findings
773 [12, p84] that employers increasingly expect potential staff to maintain digital career capital to enable employers to
774

781 “construct and evaluate professional and/or workplace identities”. Participants also identified that online visibility could
 782 help to build legitimacy as citizens, and to comply with perceived social norms — for example, by publicly expressing a
 783 stance around current events such as BLM. Choosing *not* to be visible and *not* to disclose information about oneself can
 784 be seen as a privilege, afforded to those who are established members of society and not seeking work. This is especially
 785 pertinent for those whose safety may be jeopardised by online visibility — such as survivors of domestic or other abuse,
 786 and asylum seekers — yet who feel compelled to be visible due to the adverse impact that invisibility could have on
 787 their chances of getting a job, or gaining legitimacy as citizens and members of social groups [21]; also see [75].
 788
 789

790 *Unintentional information leakage* occurred as a result of the actions of others, who shared participants’ information to
 791 unforeseen audiences and at times causing un/intentional shame or other harm. This could be particularly uncomfortable
 792 when the information shared was from long-forgotten posts, or was taken out of context. While participants had a
 793 good understanding of the persistent nature of aspects of their traces, they found it difficult to recall what they had
 794 previously posted across multiple channels and hence where potential vulnerabilities might lie. Yet it is not at all
 795 surprising that participants struggled to remember past posts when remembering involves “cognitive processing of
 796 knowledge from the past, through a repetitive process of reconstruction” [81, p371]. Given the volume of information
 797 commonly shared online, remembering everything that one has posted presents an intractable cognitive processing
 798 burden that links to our third theme of *digital privacy literacy*. While processes of remembering can be supported by a
 799 range of internal and external cues including those that are technological such as Facebook “On This Day” reminders,
 800 things always get irretrievably forgotten [81]. Although options exist to have content removed from the Internet or at
 801 least not show up in search results — e.g., the Right To Erasure³ — there is no easy mechanism through which to erase
 802 aspects of one’s past history online, or to remove comments made over years that could be misinterpreted or show
 803 one in a bad light if later taken out of context. Multiple respondents rationalised that their online information was
 804 “boring” and of no interest to others. They also referred to being unable to summon the required time, effort and/or
 805 practical digital privacy competencies to erase aspects of their past history online. This is understandable, when such
 806 curation increasingly involves sophisticated multidisciplinary skills and knowledge spanning digital, technical, legal,
 807 and socio-cultural competencies. For example, an individual who is seeking public election might want to check back
 808 through their past history online for any information that could be taken out of context and wrongly interpreted as
 809 expressing socially unacceptable views. Of course, this is also open to misuse, with individuals who genuinely hold
 810 socially unacceptable views cleaning up their online profiles to obfuscate their true opinions.
 811
 812
 813
 814
 815

816 Our study was conducted at a time when the legal context of the UK was an uncertain one. Materially, little has
 817 changed for UK citizens with regard to GDPR since the UK left the EU, as the UK enacted the UK-GDPR in 2020. However
 818 there is an ongoing high-profile political and legislative debate as to whether the UK should diverge more aggressively
 819 from the European framework, which is seen in some quarters as unnecessarily burdensome and overprotective [3].
 820 All these changes took place, and were publicly discussed, while the interviews took place. This posed some legal and
 821 ethical challenges for the research: knowing that the GDPR would cease to be applicable shortly after the interviews
 822 were completed, what legal assurance could be given to the participants? It raised also questions for the substantive
 823 part of the research: discussions surrounding post-Brexit data protection in the news will have created more awareness
 824 of data protection questions, and may also have contributed to an even stronger feeling of uncertainty and vulnerability.
 825 Disclosing data about oneself in the UK during 2019, the year prior to this study, also meant that it was at least not
 826
 827
 828
 829
 830

831 ³UK Information Commissioner’s Office (ICO, 2017: 49)
 832

certain what legal protection would apply to it in a few months' time, which given the permanence of digital traces poses a significant difficulty.

5.1 Limitations and Future Work

A key limitation of our work is that while our participants were able to conceptualise aspects of the implications of personal information sharing in interview, they consistently struggled to conceptualise the entirety or whole picture of their accumulated digital traces across multiple channels and across time, and potential knock-on effects and risks. We acknowledge that the data narrative approach was not sufficient to achieve this and in this context, we identify the following pressing future work:

- Demonstrate to individuals in everyday terms – perhaps by using other narrative approaches, including scenarios – the potential use by another agent of seemingly harmless pieces of personal information posted across disconnected digital traces.
- Go beyond “awareness nudges” by promoting reflection *before* sharing, to enable people to make informed choices about the information that they add to their cumulative digital traces.
- Some participants conveyed anxiety around their old posts being re-discovered, despite them not having clear recall of their contents, amplifying their perceived impotence and lack of knowledge about how to go about removing offending information. We see an opportunity to enable people to efficiently curate the material that they have posted in the past online, without having to trawl through every single post or delete an account wholesale.
- A further opportunity to reduce unintended information leakage lies in integrating prompted password change as part of standard installation for owners of domestic internet-enabled/ IoT devices, combined with information about inherent risks of devices and how to mitigate against these, to protect domestic privacy.

Last but not least, there is a critical need to address digital privacy literacy, including digital privacy gaps. This aligns with ongoing efforts towards ensuring social justice within the HCI e.g., [75], and CSCW [77] design and wider research communities. Talhouk et al.'s CSCW work [77] around the digitisation of food aid intended for Syrian refugees in Lebanon found that due to refugees' “low technological literacies”, their “experiences of engaging with food aid” were severely impoverished and ability to “identify and report the misuse of the technologies by other stakeholders and intermediaries” (p133) curtailed, amplifying the already present power asymmetries experienced by those groups.

While interviewees had a good understanding of the persistent nature of their traces, they found it difficult during interviews to recall what they had previously posted. Remembering, from the Latin – *rememorari* – or “call to mind”, involves cognitive processing of knowledge from the past, “through a repetitive process of reconstruction” [81, p371]. Yet people face challenges in making connections between something visible, and its meaning – and, to paraphrase Rancière [1]– across heterogeneous spaces and times. Rancière also refers to “the power of art in its ability to represent what is absent or unrepresentable – and that when they are represented they infer power” (ibid). He, along with others, discusses memories as works of fiction – reconstructions as opposed to re-presentations or later reproductions. While processes of remembering can be supported by a range of internal and external cues – things always get irretrievably forgotten [81]. There is only ever a partial picture, or re-presentation.

Our work offers understandings around personal information and what it collectively comprises [39], including the inferences that others can draw. It aims to promote personal agency around management of this information. As future work, we will use the findings reported here to inform the design of an online tool. The digital user interface of this

885 tool, as well as how it curates, contextualises, and relates information to people, will be informed by the qualitative
 886 outcomes of design workshops. The tool will allow people to explore the risks and consequences surrounding their
 887 own online data-sharing activities and the digital traces they leave behind. We are mindful of Elsdon et al.'s proposition
 888 that “design should seek to support people in making account of their data, and guard against the assumption that
 889 more, or “better”, data will be able to do this for them”[29]. Our current design work is also mindful of so-called “moral
 890 economies” that are produced as a result of practices and activities around personal data, which are laden with affect,
 891 cultural expectation, and responsibility [82]. Design, we argue, is central to promoting sense-making and digital privacy
 892 literacies in this context. Even the provision of designed tools is a form of design activism, introducing new frictions
 893 into online activity to provide context to, reflection on and guidance for, our information-sharing decisions [6, 33],
 894 and/or where necessary, helping to develop counter-narratives [30].
 895
 896
 897

898 ACKNOWLEDGMENTS

899 We acknowledge the contributions of our project partners and time and effort of our participants.
 900
 901

902 REFERENCES

- 903
 904 [1] 2007. Art & Research : Jacques Rancière and Indisciplinarity. <http://www.artandresearch.org.uk/v2n1/jrinterview.html>
 905 [2] 2015. Data Privacy Project – Initiatives to inform and support libraries and librarians. <https://dataprivacyproject.org/>
 906 [3] 2021. Data: a new direction - GOV.UK. <https://www.gov.uk/government/consultations/data-a-new-direction>
 907 [4] Nurul Nuha Abdul Molok, Atif Ahmad, and Shanton Chang. 2018. A case analysis of securing organisations against information leakage through
 908 online social networking. *International Journal of Information Management* 43 (12 2018), 351–356. <https://doi.org/10.1016/j.ijinfomgt.2018.08.013>
 909 [5] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975). <https://eric.ed.gov/?id=ed131515>
 910 [6] James Ash, Ben Anderson, Rachel Gordon, and Paul Langley. 2018. Digital interface design and power: Friction, threshold, transition. *Environment*
 911 *and Planning D: Society and Space* 36, 6 (2018), 1136–1153. <https://doi.org/10.1177/0263775818767426>
 912 [7] Debi Ashenden. 2018. In their own words: employee attitudes towards information security. *Information & Computer Security* 26, 3 (7 2018),
 913 327–337. <https://doi.org/10.1108/ICS-04-2018-0042>
 914 [8] Yoram Bachrach, Michal Kosinski, Thore Graepel, Pushmeet Kohli, and David Stillwell. 2012. FacebookPersonality_michal_29_04_12.pdf. (2012).
 915 <https://doi.org/10.1145/2380718.2380722>
 916 [9] Sara Bannerman. 2019. Relational privacy and the networked governance of the self. *Information Communication and Society* 22, 14 (12 2019),
 917 2187–2202. <https://doi.org/10.1080/1369118X.2018.1478982>
 918 [10] Susanne Barth and Menno D.T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual
 919 online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
 920 [11] Genevieve Bell, Mark Blythe, and Phoebe Sengers. 2005. Making by making strange. *ACM Transactions on Computer-Human Interaction (TOCHI)* 12,
 921 2 (6 2005), 149–173. <https://doi.org/10.1145/1067860.1067862>
 922 [12] Brenda L. Berkelaar and Patrice M. Buzzanell. 2015. Online Employment Screening and Digital Career Capital. *Management Communication*
 923 *Quarterly* 29, 1 (2 2015), 84–113. <https://doi.org/10.1177/0893318914554657>
 924 [13] DM Boyd. 2008. *Taken out of context: American teen sociality in networked publics*. Ph.D. Dissertation. [https://search.proquest.com/openview/](https://search.proquest.com/openview/9cc930ef134daf46c17434d2992e8251/1?pq-origsite=gscholar&cbl=18750)
 925 [9cc930ef134daf46c17434d2992e8251/1?pq-origsite=gscholar&cbl=18750](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1518924)
 926 [14] Danah Boyd. 2009. Why youth (heart) social network sites: The role of networked publics in teenage social life. *papers.ssrn.com* (2009). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1518924
 927 [15] Danah Boyd. 2010. 'Public Default Private When Necessary'. boyd - Google Scholar. available:[http://dmlcentral.net/blog/danah-boyd/public-](http://dmlcentral.net/blog/danah-boyd/public-default-private-when-necessary)
 928 [default-private-when-necessary](http://dmlcentral.net/blog/danah-boyd/public-default-private-when-necessary)
 929 [16] DM Boyd and NB Ellison. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer-mediated Communication* 13, 1 (10
 930 2007), 210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
 931 [17] Petter Bae Brandtzaeg and Marika Lüders. 2018. Time Collapse in Social Media: Extending the Context Collapse. *Social Media + Society* 4, 1 (1 2018),
 932 205630511876334. <https://doi.org/10.1177/2056305118763349>
 933 [18] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
 934 [19] Adrian Bussone, Bakita Kasadha, Simone Stumpf, Abigail C. Durrant, Shema Tariq, Jo Gibbs, Karen C. Lloyd, and Jon Bird. 2020. Trust, Identity,
 935 Privacy, and Security Considerations for Designing a Peer Data Sharing Platform Between People Living With HIV. *Proceedings of the ACM on*
 936 *Human-Computer Interaction* 4, CSCW2 (10 2020), 27. <https://doi.org/10.1145/3415244>

- 937 [20] Hongliang Chen, Christopher E. Beaudoin, and Traci Hong. 2016. Protecting oneself online: The effects of negative privacy experiences on privacy
938 protective behaviors. *Journalism and Mass Communication Quarterly* 93, 2 (2016), 409–429. <https://doi.org/10.1177/1077699016640224>
- 939 [21] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude P.R. Heath. 2020. Too Much Information: Questioning Security in a Post-Digital Society.
940 In *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery, New York, NY, USA, 1–14. <https://doi.org/10.1145/3313831.3376214>
- 941 [22] Elisabetta Costa. 2018. Affordances-in-practice: An ethnographic critique of social media logic and context collapse. *New media & society* 20, 10 (10
942 2018), 3641–3656. <https://doi.org/10.1177/1461444818756290>
- 943 [23] Jenny L. Davis and Nathan Jurgenson. 2014. Context collapse: Theorizing context collusions and collisions. *Information Communication and Society*
944 17, 4 (2014), 476–485. <https://doi.org/10.1080/1369118X.2014.888458>
- 945 [24] Kathryn Dindia. 2000. Sex Differences in Self-Disclosure, Reciprocity of reciprocity of self-disclosure and liking: Three meta-analyses reviewed. In
946 *Balancing the Secrets of Private Disclosures*. Routledge, 37–52. [https://doi.org/10.4324/9781410604606-10/SEX-IFFERENCES-SELF-ISCLOSURE-
947 ECIPROCTY](https://doi.org/10.4324/9781410604606-10/SEX-IFFERENCES-SELF-ISCLOSURE-ECIPROCTY)
- 948 [25] Judson C. Dressler, Christopher Bronk, and Daniel S. Wallach. 2015. *Exploiting military OpSec through open-source vulnerabilities*. Vol. 2015-Decem.
949 IEEE. 450–458 pages. <https://doi.org/10.1109/MLCOM.2015.7357484>
- 950 [26] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014.
951 Understanding the experience-centeredness of privacy and security technologies. In *ACM International Conference Proceeding Series*, Vol. 15-18-
September-2014. Association for Computing Machinery, New York, New York, USA, 83–93. <https://doi.org/10.1145/2683467.2683475>
- 952 [27] David Ellis, Lukasz Piwekis, and Adam Joinson. 2016. The future of wearable technology – Centre for Research and Evidence on Security Threats.
953 <https://crestresearch.ac.uk/comment/the-future-of-wearable-technology/>
- 954 [28] David A. Ellis, Brittany I. Davidson, Heather Shaw, and Kristoffer Geyer. 2019. Do smartphone usage scales predict behavior? *International Journal*
955 *of Human Computer Studies* 130 (10 2019), 86–92. <https://doi.org/10.1016/j.ijhcs.2019.05.004>
- 956 [29] Chris Eldsen, David S. Kirk, and Abigail C. Durrant. 2016. A Quantified Past: Toward Design for Remembering With Personal Informatics.
957 *Human-Computer Interaction* 31, 6 (11 2016), 518–557. <https://doi.org/10.1080/07370024.2015.1093422>
- 958 [30] Alastair Fuad-Luke. 2013. *Design activism: beautiful strangeness for a sustainable world*. Routledge.
- 959 [31] Bill Gaver, Tony Dunn, and Elena Pacenti. 1999. Design: Cultural probes. *Interactions* 6, 1 (1 1999), 21–29. <https://doi.org/10.1145/291224.291235>
- 960 [32] Erving Goffman. 1959. *The Presentation of Self in Everyday Life*. [https://books.google.co.uk/books?hl=en&lr=&id=THAZT5uT-IC&oi=fnd&pg=
961 PA120&ots=IuGdfILkoa&sig=D4qf0QBOVwXTiGoRVHUYwbr7Mik&redir_esc=y#v=onepage&q&f=false](https://books.google.co.uk/books?hl=en&lr=&id=THAZT5uT-IC&oi=fnd&pg=PA120&ots=IuGdfILkoa&sig=D4qf0QBOVwXTiGoRVHUYwbr7Mik&redir_esc=y#v=onepage&q&f=false)
- 962 [33] Eric Gordon and Gabriel Mugar. 2020. *Meaningful Inefficiencies*. Oxford University Press.
- 963 [34] Colin Gray and Shruthi Sai Chivukula. 2019. When does manipulation turn a design 'dark'? *Interactions* 27, 1 (12 2019), 96–96. [https://doi.org/10.
964 1145/3375016](https://doi.org/10.1145/3375016)
- 965 [35] Aikaterini Grimani, Anna Gavine, and Wendy Moncur. 2020. An evidence synthesis of covert online strategies regarding intimate partner violence.
Trauma, Violence, & Abuse (2020). <https://doi.org/10.1016/j.drugpo.2019.102621>
- 966 [36] Ralph Gross, Alessandro Acquisti, and H. John Heinz. 2005. *Information revelation and privacy in online social networks*. Technical Report. 71–80
967 pages. <https://doi.org/10.1145/1102199.1102214>
- 968 [37] Oliver L. Haimson, Jed R. Brubaker, Lynn Dombrowski, and Gillian R. Hayes. 2016. Digital footprints and changing networks during online
969 identity transitions. In *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery, 2895–2907.
<https://doi.org/10.1145/2858036.2858136>
- 970 [38] Eszter Hargittai and Alice Marwick. 2016. "What can i really do?" Explaining the privacy paradox with online apathy. *International Journal of*
971 *Communication* 10 (2016), 3737–3757. <https://doi.org/10.5167/uzh-148157>
- 972 [39] Trevor Hogan. 2015. Tangible data, a phenomenology of human-data relations. In *TEI 2015 - Proceedings of the 9th International Conference on*
973 *Tangible, Embedded, and Embodied Interaction*. Association for Computing Machinery, Inc, 425–428. <https://doi.org/10.1145/2677199.269160>
- 974 [40] Joseph 'Jofish' Kaye, Mary McCuiston, Rebecca Gulotta, and David A Shamma. 2014. Money Talks: Tracking Personal Finances. In *Proceedings of*
975 *the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA. (2014), 521–530.
<https://doi.org/10.1145/2556288.2556975>
- 976 [41] Slava Kisilevich and Florian Mansmann. 2010. *Analysis of privacy in online social networks of Runet*. Association for Computing Machinery. 46–55
977 pages. <https://doi.org/10.1145/1854099.1854112>
- 978 [42] Rob Kitchin and Tracey P. Lauriault. 2015. Small data in the era of big data. *GeoJournal* 80, 4 (8 2015), 463–475. [https://doi.org/10.1007/s10708-014-
979 9601-7](https://doi.org/10.1007/s10708-014-9601-7)
- 980 [43] Hanna Krasnova, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online social networks: Why we disclose. *Journal of*
981 *Information Technology* 25, 2 (6 2010), 109–125. <https://doi.org/10.1057/jit.2010.6>
- 982 [44] Gunther Kress. 2003. Literacy in the New Media Age - Gunther R. Kress - Google Books. [https://books.google.co.uk/books?hl=en&lr=&id=
983 2vaNeafOoiYC&oi=fnd&pg=PP17&dq=gunther+kress+media&ots=Uwjel_v8Mb&sig=1MF-h0rPc5I4ZiM2bbTcurjebbl#v=onepage&q=gunther%
984 20kress%20media&f=false](https://books.google.co.uk/books?hl=en&lr=&id=2vaNeafOoiYC&oi=fnd&pg=PP17&dq=gunther+kress+media&ots=Uwjel_v8Mb&sig=1MF-h0rPc5I4ZiM2bbTcurjebbl#v=onepage&q=gunther%20kress%20media&f=false)
- 985 [45] Ian Li, Anind Dey, and Jodi Forlizzi. 2010. *A Stage-Based Model of Personal Informatics Systems*. <http://daytum.com>
- 986 [46] David E. Losada, Fabio Crestani, and Javier Parapar. 2018. Overview of eRisk 2018: Early Risk Prediction on the Internet (extended lab overview).
987 *CEUR Workshop Proceedings* 2125 (2018).
- 988

- 989 [47] David E. Losada, Fabio Crestani, and Javier Parapar. 2019. Overview of eRisk 2019 Early Risk Prediction on the Internet. *Lecture Notes in Computer*
990 *Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11696 LNCS, September (2019), 340–357.
991 https://doi.org/10.1007/978-3-030-28577-7_{ }27
- 992 [48] Deborah Lupton. 2017. Feeling your data: Touch and making sense of personal digital data. <https://doi.org/10.1177/1461444817717515> 19, 10 (7 2017),
993 1599–1614.
- 994 [49] Deborah Lupton. 2019. *Data selves: more-than-human perspectives*. John Wiley and Sons Inc. 154 pages.
- 995 [50] Orla Lynskey. 2015. *The foundations of EU data protection law*. <https://books.google.com/books?hl=en&lr=&id=jCXYCgAAQBAJ&oi=fnd&pg=PP1&dq=Lynskey,+Orla.+The+foundations+of+EU+data+protection+law.+Oxford+University+Press,+2015.&ots=iXfY7KwAd&sig=Hz7XDNKqkyAnKWbAM7sIVCIGr-M>
- 997 [51] Mirca Madianou and Daniel Miller. 2012. Polymedia: Towards a new theory of digital media in interpersonal communication. *International Journal*
998 *of Cultural Studies* (8 2012). <https://doi.org/10.1177/1367877912452486>
- 999 [52] Alice E Marwick and danah boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 7 (11 2014),
1000 1051–1067. <https://doi.org/10.1177/1461444814543995>
- 1001 [53] Alice E Marwick and danah boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 7 (11 2014),
1002 1051–1067. <https://doi.org/10.1177/1461444814543995>
- 1003 [54] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. (4 2020), 1–14. <https://doi.org/10.1145/3313831.3376167>
- 1004 [55] Albert Meijer and Martijn Wessels. 2019. Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration* 42,
1005 12 (9 2019), 1031–1039. <https://doi.org/10.1080/01900692.2019.1575664>
- 1006 [56] Metro. 2021. Navy officer 'filmed X-rated video at Faslane nuclear base' | Metro News. <https://metro.co.uk/2021/02/08/navy-officer-filmed-x-rated-video-at-faslane-nuclear-base-14039731/>
- 1007 [57] Wendy Moncur. 2016. Living digitally. In *Memory in the Twenty-First Century: New Critical Perspectives from the Arts, Humanities, and Sciences*.
1008 Palgrave Macmillan UK, 108–112. https://doi.org/10.1057/9781137520586_{ }13
- 1009 [58] NCSC. 2018. The cyber threat to UK business 2017-2018 report. <https://www.ncsc.gov.uk/information/the-cyber-threat-to-uk-business-2017-2018-report>
- 1010 [59] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. <https://dl.acm.org/doi/10.5555/1822585>
- 1011 [60] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (10 2011), 32–48. https://doi.org/10.1162/DAED_{ }A_{ }00113
- 1012 [61] Jonathan A. Obar. 2020. Sunlight alone is not a disinfectant: Consent and the futility of opening Big Data black boxes (without assistance). *Big Data*
1013 *and Society* 7, 1 (2020). <https://doi.org/10.1177/2053951720935615>
- 1014 [62] Open Rights Group. [n.d.]. Who do they think you are? | Open Rights Group. <https://www.openrightsgroup.org/campaign/who-do-they-think-you-are/>
- 1015 [63] Kathryn M. Orzech, Wendy Moncur, Abigail Durrant, and Diego Trujillo-Pisanty. 2018. Opportunities and challenges of the digital lifespan: views
1016 of service providers and citizens in the UK. *Information Communication and Society* (2018). <https://doi.org/10.1080/1369118X.2016.1257043>
- 1017 [64] Gaëlle Ouvrein and Karen Verswijvel. 2019. Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences
1018 with sharenting against the background of their own impression management. *Children and Youth Services Review* 99 (4 2019), 319–327. <https://doi.org/10.1016/j.childyouth.2019.02.011>
- 1019 [65] Alex Pentland. 2012. Reinventing society in the wake of big data. https://www.edge.org/conversation/alex_sandy_pentland-reinventing-society-in-the-wake-of-big-data
- 1020 [66] Tyler Reigeluth. 2014. Why data is not enough: Digital traces as control of self and self-control. *Surveillance and Society* 12, 2 (5 2014), 243–254.
1021 <https://doi.org/10.24908/ss.v12i2.4741>
- 1022 [67] Jeffrey Rosen. 2011. The Right to Be Forgotten. *Stanford Law Review Online* 64 (2011). <https://heinonline.org/HOL/Page?handle=hein.journals/slro64&id=89&div=17&collection=journals>
- 1023 [68] William Ryan, Martin Siegel, Erik Stolterman, Tonya Thompson, Heekyoung Jung, and William R. Hazlewood. 2009. Device Ecology Mapper: A
1024 tool for studying users' ecosystems of interactive artifacts. *Conference on Human Factors in Computing Systems - Proceedings* (2009), 4327–4332.
1025 <https://doi.org/10.1145/1520340.1520661>
- 1026 [69] Corina Sas and Irni Eliana Khairuddin. 2017. Design for trust: An exploration of the challenges and opportunities of bitcoin users. *Conference on*
1027 *Human Factors in Computing Systems - Proceedings* 2017-May (5 2017), 6499–6510. <https://doi.org/10.1145/3025453.3025886>
- 1028 [70] John S. Seberger, Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. Empowering resignation there's an app for that.
1029 *Conference on Human Factors in Computing Systems - Proceedings* (5 2021). <https://doi.org/10.1145/3411764.3445293>
- 1030 [71] Abigail J. Sellen and Steve Whittaker. 2010. Beyond total capture: A constructive critique of lifelogging. *Commun. ACM* 53, 5 (5 2010), 70–77.
1031 <https://doi.org/10.1145/1735223.1735243>
- 1032 [72] Irina Shklovski, Scott D Mainwaring, Halla Hrunn Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space:
1033 Perceptions of Privacy and Mobile App Use. (2014). <https://doi.org/10.1145/2556288.2557421>
- 1034 [73] Ellen Simpson and Bryan Semaan. 2021. For You, or For "You"? *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (1 2021), 1–34.
1035 <https://doi.org/10.1145/3432951>
- 1036
1037
1038
1039
1040

- 1041 [74] Robert Sprague. 2011. Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of*
1042 *Louisville Law Review* 50 (2011).
- 1043 [75] Angelika Strohmayer, Jenn Clamen, and Mary Laing. 2019. Technologies for social justice lessons from sex workers on the front lines. In
1044 *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery, New York, NY, USA, 1–14. <https://doi.org/10.1145/3290605.3300882>
- 1045 [76] Latanya Sweeney, Akua Abu, and Julia Winn. 2013. Identifying Participants in the Personal Genome Project by Name (A Re-identification
1046 Experiment). *SSRN Electronic Journal* (2013), 1–4. <https://doi.org/10.2139/ssrn.2257732>
- 1047 [77] Reem Talhouk, Lizzie Coles-Kemp, Rikke Bjerg Jensen, Madeline Balaam, Andrew Garbett, Hala Ghattas, Vera Araujo-Soares, Balsam Ahmad, and
1048 Kyle Montague. 2020. Food Aid Technology: The Experience of a Syrian Refugee Community in Coping with Food Insecurity. *Proceedings of the*
1049 *ACM on Human-Computer Interaction* 4, CSCW2 (10 2020). <https://doi.org/10.1145/3415205>
- 1050 [78] Louise Thornthwaite. 2018. Social media and dismissal: Towards a reasonable expectation of privacy? *Journal of Industrial Relations* 60, 1 (2 2018),
1051 119–136. <https://doi.org/10.1177/0022185617723380>
- 1052 [79] Zeynep Tufekci. 2008. GROOMING, GOSSIP, FACEBOOK AND MYSFACE. *Information, Communication & Society* (2008). [https://doi.org/10.1080/](https://doi.org/10.1080/13691180801999050)
1053 [13691180801999050](https://doi.org/10.1080/13691180801999050)
- 1054 [80] UK Children’s Commissioner. 2018. *Who knows what about me?* Technical Report. [https://www.childrenscommissioner.gov.uk/digital/who-knows-](https://www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/)
1055 [what-about-me/](https://www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/)
- 1056 [81] Elise van den Hoven. 2014. A future-proof past: Designing for remembering experiences. *Memory Studies* 7, 3 (7 2014), 370–384. <https://doi.org/10.1177/1750698014530625>
- 1057 [82] Janet Vertesi, Jofish Kaye, Samantha N Jarosewski, Vera D Khovanskaya, and Jenna Song. 2016. Data Narratives: Uncovering tensions in personal
1058 data management. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. Association
1059 for Computing Machinery, San Francisco, California, USA, 478–490. <https://doi.org/10.1145/2818048.2820017>
- 1060 [83] Ning Xia, Han Hee Song, Yong Liao, Marios Iliofotou, Antonio Nucci, Zhi Li Zhang, and Aleksandar Kuzmanovic. 2013. *Mosaic: Quantifying privacy*
1061 *leakage in mobile networks*. Vol. 43. 279–290 pages. <https://doi.org/10.1145/2534169.2486008>
- 1062 [84] Yifan Yang, Daniel Cooper, John Collomosse, Catalin Dragan, Mark Manulis, Jo Briggs, Jamie Steane, Arthi Manohar, Wendy Moncur, and Helen
1063 Jones. 2020. TAPESTRY: A De-centralized Service for Trusted Interaction Online. *IEEE Transactions on Services Computing* (2020). <https://doi.org/10.1109/TSC.2020.2993081>
- 1064 [85] Alyson L. Young and Anabel Quan-Haase. 2009. Information revelation and internet privacy concerns on social network sites. (2009), 265.
1065 <https://doi.org/10.1145/1556460.1556499>
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092

1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144

6 APPENDICES
A INTERVIEW QUESTIONS

Table 2. Interview Questions with Changes in Response to Lockdown/ Working From Home

Question	Original(Y/N)	Amended (Am)?
What communication channels do you use?	Y	Am
What Apps and Sites (e.g Twitter, match.com, Strava) do you use?	Y	Am
What data management services do you use (e.g. iCloud, Box)?	Y	Am
Devices used (e.g. mobile, Fitbit, NEST, IoT)	Y	Am - sharing?
Do you share devices with anyone?	Y	Am - emphasis
Behavioural patterns/practices (e.g. search history)	Y	Am
What do you post? Who it is visible to?	Y	Am
Types of information posted, Why/how do you hide data	Y	Am
Instances where information posted revealed more than intended	Y	Am
Concerns about types of revelation	Y	Am
What are your digital hygiene practices		
- to ensure privacy/reputation mgmt?	Y	Am
Account sharing and associated posting responsibilities	Y	Am
Given an overview of your data, what could be found out?	Y	Unchanged
Do you work in public/private sector? What level? How big is org?	N	Added
Are you working from home during Lockdown? Is this new?	N	Added
Did your employer advise on data management during Lockdown?	N	Added
Who lives at home with you? Any bandwidth issues?	N	Added
What advice would you give to someone with the same eco-system as you, to be secure?	N	Added

B SURVEY OUTCOMES OVERVIEW

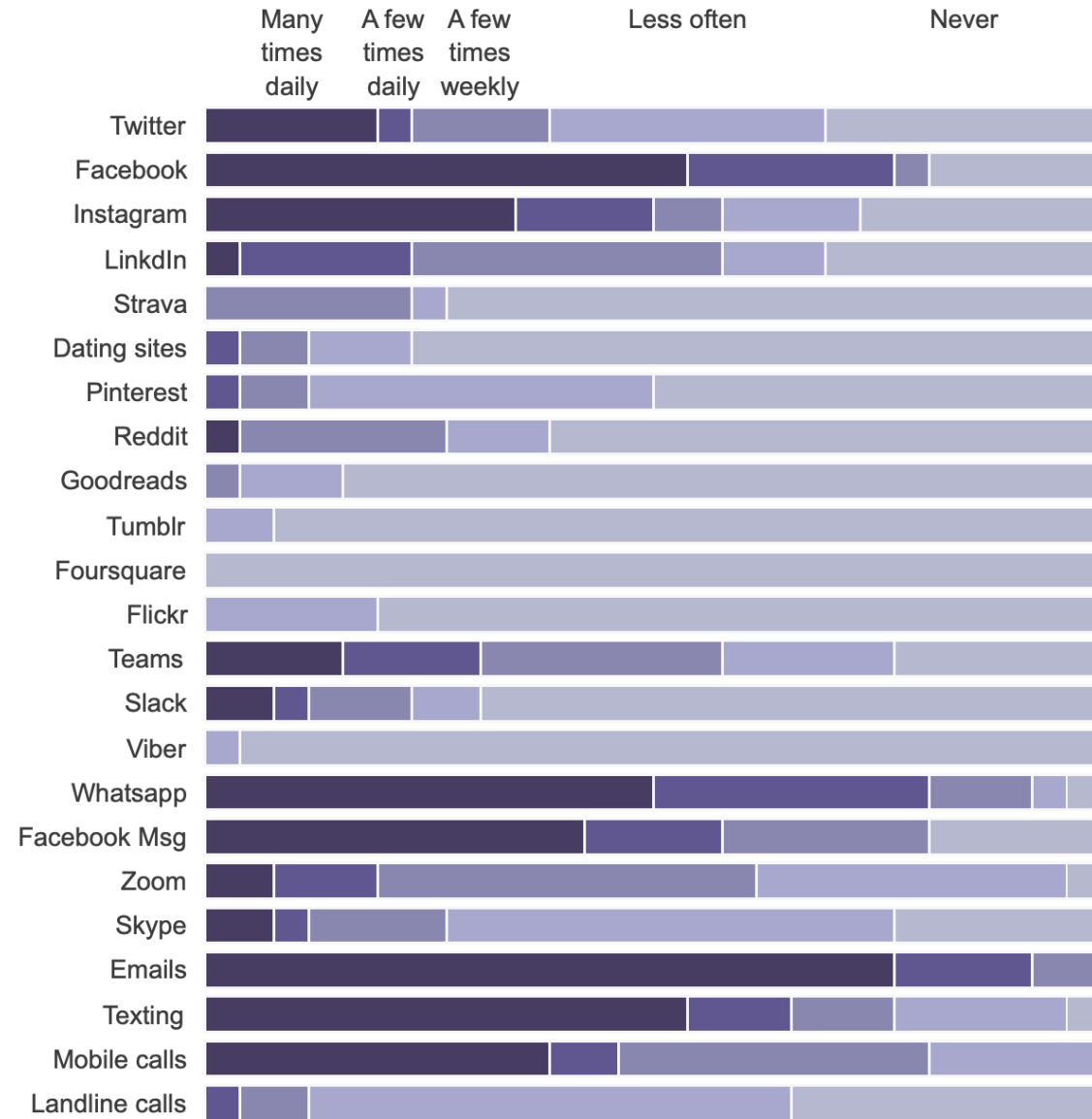


Fig. 1. Participant Responses to Technology Questionnaire.

C PARTICIPANT SKETCHES

1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248

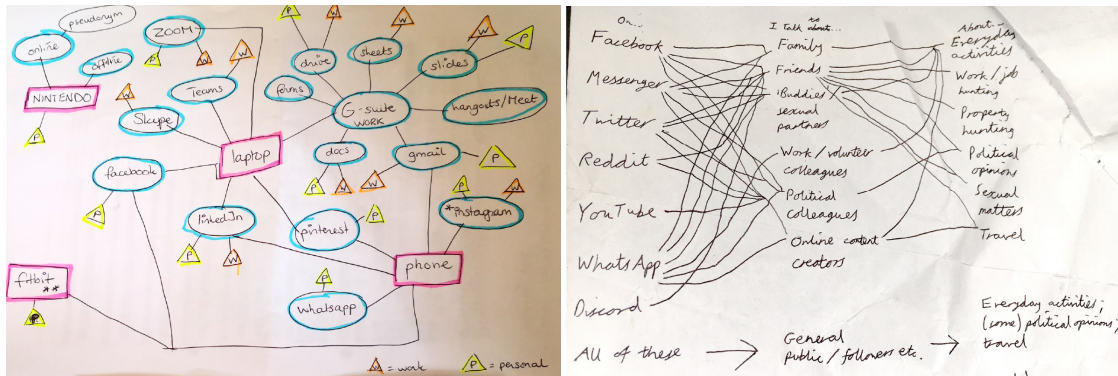


Fig. 2. Two drawings created by participants, Vinny, 24 (right) and Denise, 32 (left) during interview to represent the online platforms they used and the types of information shared. Both participants indicated interconnections, drawing lines between platforms to convey information flows. We received sketches from 21 participants documenting their devices and apps, often along with the various relationships these enabled, in a mapping or table arrangement. The sketches supported and added depth to interview conversations and the drawing of the sketches often triggered participants to remember additional details