Digital Security Narratives in the Time of COVID-19: A Case for Kindness

Lizzie Coles-Kemp and Peter A. Hall

Abstract The COVID-19 pandemic has shined a light on the digital divide and its implications in a digital-first society. In the UK, where our research is focused, parts of society still lack the infrastructure and/or basic skills needed to access essential online services like health, welfare, food, housing and education. During the pandemic, these services became digital by necessity, forcing many people to seek help through informal networks such as community hubs. Based on our focus groups and interviews with voluntary and third sector organisations in the UK, we make a case in this chapter for a kinder, more holistic approach to the accessibility of essential online services, based on the hypothesis that such an approach creates the types of spaces in which the benefits of such services can be more safely realised.

Keywords Care · Digital divide · Digital inclusion · Kindness · Privacy · Welfare · Service design · Holistic and usable security

1 Introduction

As essential services moved online by necessity during the COVID-19 pandemic, access to education, health, welfare, food and housing services became dependent on access to the internet. In the UK, where 1.5 million households have no internet access, and an estimated 10 million people lack the basic foundational skills needed to access online services, one common reason cited for low digital engagement is concern about privacy and security [1]. In this chapter we argue that the design of online systems, the security logics that shape their access and the sociomaterial assemblages around them have the effect—intended or not—of excluding populations.

L. Coles-Kemp
Information Security Group, Royal Holloway University of London, Egham TW20 0EX, UK

P. A. Hall (✉)
Graphic Design, University of the Arts London, 45-65 Peckham Rd, London SE5 8UF, UK
e-mail: p.hall@arts.ac.uk

N. Martins et al. (eds.), *Perspectives on Design and Digital Communication III*,
Springer Series in Design and Innovation 24,
https://doi.org/10.1007/978-3-031-06809-6_8

Rather than frame this problem with a discussion of assistive technologies and inclusive design, we start this chapter with a case study drawn from primary research, which we then consider in terms of alternative security and service design narratives. This approach, based on the COVID-19 support experiences of a community group in North East England, is driven by a suspicion that conventional framings of security and accessibility privilege solutions based on incremental technological improvements rather than a more holistic response. We argue that new driving narratives are needed that account for the relational ways in which people in their day-to-day lives conceive of digital security, to supplement the dominant narratives of a *negative* security where a "referent object" (property, data, the state) is presented as needing protection, usually through technological means. An alternative narrative of a *positive, enabling* image of security, drawn from the field of International Relations, is not premised on protecting a referent object but on "making something possible"; in this position, security has "the property of a relationship" (McSweeney 1999, cited in [2], p. 778). We identify analogous approaches in sociology and urbanism, where the security of a city is reimagined less in terms of protective measures and more in terms of invisible or unnoticed acts of "kindness"—such as repair and care—that are fundamental to the maintenance of everyday urban life [3]. Our case study is taken from a focus group and a follow-up interview with Pallion Action Group in the North-East of England, one of many community organizations that have stepped up during the pandemic to provide support to those on the wrong side of the digital divide.

2 Framing: A Case Study

Our work is framed in the COVID-19 pandemic experiences of voluntary and third sector organisations up and down the UK who found themselves as the first and last line of support for vulnerable and underserved individuals and groups trying to adjust to day-to-day existence shaped by physical isolation, extreme uncertainty and digital-only access to everyday support. As part of a study of assisted digital access funded by the UK's Research Institute for Sociotechnical Cyber Security,[1] we invited voluntary and third sector organisations to take part in a series of focus groups held over Zoom to discuss how such groups were supporting the digital access needs of their community. Inspired by these focus groups, we took the experiences of Pallion Action Group, one of the community groups that took part in this study and followed up by interviewing the manager of that group (Karen Noble) to form a picture of how they have supported their community members with digital assistance from March 2020 to present day. Direct quotes from the focus group and follow-up interview are presented in this section. We set out these experiences to frame our subsequent argument for a kinder, more humanistic, and relational form of digital security.

[1] https://www.riscs.org.uk/digital-responsibility/.

Pallion Action Group provides monetary, debt and welfare advice and support to vulnerable groups. Pallion is one of the most deprived areas of Sunderland and the community organisation has been providing support in the areas of welfare access, household finance and employment training since its start. As part of this programme of work, it has been providing digital skills training and support for digital access. Pallion is a suburb and electoral ward in West Sunderland in North East England. Since its founding in 2005 as a residents' group, Pallion Action Group has changed its focus from supporting primarily youth services to becoming a community hub, initiating activities to build support networks in the Pallion area. During the pandemic, Pallion Action Group's assistance with services such as providing activity packs for families, collecting prescriptions and shopping for self-isolating and housebound residents, and supporting people with accessing online services has increased, prompting the local council to recognise its work and that of other community hubs with further funding.

Overall, the group has reported a significant increase in the number of people accessing its services—3000 new signees (individuals and households) since the start of the pandemic—as well as a broadening in the range of people seeking help during the pandemic, and in the kinds of services provided. Whereas prior to the first lockdown and shift to digital-only services, the typical visitor to Pallion Action Group was an older person needing assistance with online services who was "*scared to touch a button or …who just didn't do digital things*," [4] the pandemic prompted younger people to seek help: "*kids who were supposed to be [school]working from home, who didn't have the digital equipment or they didn't have Internet access. Then we had parents who didn't have the digital skills to help the kids get online…so I think our first issue was about trying to get people to understand what digital equipment was and what was best for them. We had to go back to basics for a lot of people.*" [4].

The pandemic saw a shift from digital by default to digital by necessity for many essential and statutory everyday services in welfare, health, finance, food and education. Whereas pre-pandemic, those needing to access the services essential to providing household income (such as housing support and access to benefits) could make claims in person, digital by necessity meant that community hubs such as Pallion Action Group were called upon to devise a way to support claimants with no internet access, such as filling forms over the phone: this sometimes meant an advisor going through the form fields with the claimant, typing their responses, printing out the form with an indication of where it needed to be signed, and then posting it to the claimant or arranging for it to be picked up. Those seeking help with this kind of support, for example in making Universal Credit claims (monthly Government payments to help people with living costs), can have a high level of trust with the assisting organization, a trust built up over time based on reputation and familiarity of known individuals in the hub: "*If you didn't have your computer access, you couldn't warrant Universal Credit claims and that puts you at risk of not being able to get paid. So there was a lot of confusion around that. And the amount of people who followed up and said, can I give you my login details?*" [4].

Such assistance is not merely helping the individual with managing the bureaucracy of the service but also offering emotional support and empathetic support. This is because the pandemic created a stressful environment in which household resources were severely constrained, job security was threatened, and household dynamics were severely disrupted. For the households that Pallion Action Group support, this took an emotional and mental health toll as well as placing a financial burden. The complexities of accessing online services and the challenges of coping with wholesale change to the ways that services essential to wellbeing were provided were experienced against this backdrop of heightened pressures.

At the same time, the pandemic has put a severe strain on the ways in which an organisation can offer assistance for each individual and the wider community because much of the support now has to be provided over the telephone or via the web. Pallion Action Group therefore had to work out how deliver digital skills and support as part of a wider set of services intended to work with the *whole person*, not just their administrative needs. In the original focus group Noble stated: "*So, we got funding to get tablets for people; and on there we have put quizzes, surveys about the impact of COVID, and mindfulness and meditation activities, photography competition with prizes; also we've put guides about how to get on Zoom and other things.*"

This *whole person* approach is one that addresses the human security needs of the individual, placing support for digital access in the wider context of the safety and security of the individual and their families. In the focus group, the following story was related, regarding meeting an older person struggling with shopping during the pandemic: "I *had a gut feeling about [this] one lady who sounded down; all of the usual things have been taken away by COVID, she had no social circle left, she was just left to vegetate; and the agencies knew about this, but nothing was done… Age Concern [were] charging £15 per hour to go shopping; which is why we got involved.*" This was part of a wider pattern, it was said, of increased isolation and desperation which the organisation was attempting to combat through initiatives such as the one described above: "*A common story is older and more vulnerable very isolated people, no contact, no devices, this really sticks with me; in the first instance we are arranging to drop off a prescription; [they say] "you're the first person I've spoken to in ages"; she wanted to just go next-door and mix with people, and didn't care about the consequences—amounted to suicidal feelings; during the pandemic we've noticed a lot more suicidal people, over 70 especially.*" Securing the whole person is underscored by the way that Pallion Action Group places as much importance on mindfulness and yoga sessions as it does on e-safety training and skills development. From Pallion Action Group's point of view, both contribute to the safety and security of the individual.

3 Security Narratives and the Digital Divide

The Pallion case challenges how we conceptualise digital security and what it means for an individual to be digitally secure. From the perspective of Pallion Action Group, digital security is a combination of caring for the wellbeing of people and ensuring that data and access is technically secured. As the different dimensions of the digital divide reflect, access to technology is contingent on physical access to security technology and the availability of the underpinning technical and data infrastructure. Regardless of whether an individual independently accesses a digital service or requires help, the technological controls used to regulate access need to be usable, accessible and inclusive if the digital divide is to be bridged. Such controls typically include authentication processes that deploy a username and password, digital identifiers that link data to a specific individual, and permissions to access particular fields in an online form. However, as the example shows, for many marginalised and underserved groups it is not enough to develop an individual's practical skills in securely accessing digital services and resources. Pallion Action Group's pandemic experiences show how alongside the technical security of access control to secure an individual, the emotional wellbeing of an individual must also be attended to. Emotional wellbeing is primarily achieved through acts of care that take place through human relationships creating a relational form of security. Contrary to popular misconceptions that "acts of care" suggests warm feelings, "do-gooder" behaviour, and subjective, unquantifiable aspects of security, we venture that it can be reconceived and recognised as an essential aspect of system maintenance that should be woven into any framework and policy that sets out principles of digital security. This argument builds on nascent scholarship in this area [5, 6].

The COVID-19 pandemic foregrounded digital inequalities and the ways in which those without access to digital devices and services are disbenefited in the most fundamental of ways when a society shifts from being digital by default to digital by necessity. Digital exclusion is a multifaceted concept and is typically considered from three perspectives [7]:

- Physical access to digital devices.
- Skills to navigate the digital world.
- Inequalities of access.

The move to digital by necessity emphasised the importance of technology and its security being accessible for all. During the pandemic, all age groups have seen an increase in the need to access essential services online [8], but there are still parts of society that have remained digitally excluded, resulting in an increased risk of COVID-19 infection and an increase in social and economic isolation. Accessibility issues play a role in this picture of digital exclusion: economic cost, lack of digital skills and fear of online harms are all cited as reasons for digital exclusion during the COVID-19 lockdowns [1, 9]. Moreover, the availability of digital services has also been an issue and regional variations in quality of Internet access have been highlighted during the lockdowns [9]. COVID-19 has also revealed that trust in technology and institutions plays an important part in questions of accessibility. Within some sectors of society, there has been a marked degradation of trust between communities and the state during the pandemic [10]. This, in turn, can result in digital inclusion itself being regarded as a potential harm.

Traditional security analysis focuses on state-centered concerns [11] as the site of where security is done. Security logics, or the reasoning that underpins security strategies, can broadly be divided in to positive and negative forms of security [12] where positive forms of security enable people to live free from fear of attack and negative forms of security protect people from threat and harms [2]. Doty [12] argues that the dominant security logic is a negative security logic that is typically one of exclusion which depends upon an understanding of self and other that is framed by a notion of territory. Doty identifies three main security logics: national security logic, societal security logic and human security logic. *National security logic* is a traditional security logic focused on the protection of the state against existential threats. It is negative in the sense that security is perceived as protection against external threats to the national/state territory. *Societal security logic* foregrounds identity politics and society as a site of security but recognises the dependency of societal security on the security of the state. *Human security logic* is a human and individual-centred conceptualisation of security. It is a positive security logic where security is perceived as a desired good which enables access to a good life. It is a logic of inclusion, which transcends state boundaries and supports pluralistic conceptions of identity.

Much of the focus in the traditional canon of security thinking is on the doing of security [13] and the doing of security is often performed through security technologies ranging from military weapons to passwords and file permissions [14]. The dominant narrative and messages around technological security predominantly reflect negative forms of security [14] where the focus of such technologies is to protect the technology and the data from adversaries performing attacks via technical means. However, the picture of digital access that Pallion Action Group provides us shows how safe and secure access to digital services is not simply about using tools and technologies for protection. Supporting secure access to essential digital services requires an attentiveness to the tensions, emotions and cultural understandings that are woven around such access. This is very much a human security logic where security is a desirable way of being that should be available.

Security scholar Paul Roe has argued that responses to protecting entities such as a state or society need to be a combination of positive and negative security for individuals and societies to live securely [2]. Whilst the dominant narrative around security technologies is predominantly one of negative security, digital security technologies are particularly malleable and are often able to support both positive and negative security positions. This malleability can be seen in the way that such technologies can be appropriated and re-configured to respond to different threat models [15]. For example, a technology that monitors location might be used as a stalking device [16–18] or as a physical security protection mechanism [19]. Privacy and security technologies can also be configured and practised to protect against adversaries that were not envisaged at the design stage. For example, [20] describe how throwaway email addresses and anonymous apps are used to provide protection to abused women from family members. It could be argued that such re-configuration and diverging appropriations of security technologies are a form of "design in use" which describes the re-assembly and re-configuration of technology once it is deployed [21]. It could therefore be argued that it is in the assembly and re-assembly of security technologies that the positive or negative security position of the technology is often enacted. Pallion Action Group's approach to community support with its focus on human security reflects this blended positive and negative security position. The support that Pallion Action Group provides in assisting an individual's digital access takes the following forms:

- adapting support to enable the individual to realise the benefits of digital service access (positive security),
- providing a listening ear, to focus on a person's overall wellbeing and provide empathetic support (positive security) and
- supporting the digital set-up of protection controls to protect against digital threats (negative security).

As such, Pallion Action Group's approach requires confronting the intersections between technology and inequality, and is built on an understanding of security roles and responsibilities that could be interpreted as a form of social contract [22].

4 Limits of Common HCI and Service Design Approaches

The blended logics of positive security provide a perplexing problem for the design of online services, from the development of their user interfaces to their security design. Typically, a design approach might map out a typical user journey, identifying points of friction in, for example, a user's efforts to claim housing benefits, the contributing factors to those points of friction, and where improvements to a service design, user interface or security design might be introduced to address the problems identified. Yet, conventional design approaches struggle to deal with the multiple disciplinary perspectives at play in these situations (e.g. see Vines et al. on the "ageing" user [23]). Novel assistive technologies, for example, can support specific users facing specific challenges when they have been identified, but not when the users in need have not been identified or have not come forward seeking help. Sociologists (e.g. [24]) have used the phrase "care avoidance" to describe the issue of people in need of support who do not come forward, and "care paralysis", where service providers and professionals find reason not to get involved with "disagreeable" clients.

Another common method employed in design approaches is to construct personas—fictional characters based on target users of the service—and hypothetical scenarios that capture the design problems identified. Introduced by Alan Cooper in 1999, personas are considered a good way to represent real, relatable user needs, to measure the effectiveness of a design, to inform better design decisions and for multidisciplinary teams to communicate with each other [25]. The limitations and pitfalls of a personas-based approach, however, include their tendency to overlook people who do not conform to the picture of the "typical" user such as those with disabilities and other challenges. At the same time, if a persona is purposely constructed to represent a particular challenge, it can give designers a false sense of understanding their users. A more general limitation of the persona method is that it "creates an extra layer of interpretation between users and developers and thus can create a greater distance" [26]. While a person's inability to access online services might not be due to a limitation in resource or capability, the assumption of particular competencies or capabilities built into user interfaces and service design is clearly one of the most pressing design flaws in the current design of online services.

More fundamentally, personas tend toward an individualised conception of a problem space, whereas online services such as health, welfare, education are fundamentally relational. Cipolla and Manzini [27] have argued for a particular kind of service configuration that is relational. Drawing from philosopher Martin Buber's conception of a distinction between "I-Thou" encounters (between two holistic beings) and "I-It" encounters (between a person and an object or a representation of a person), they argue that relational services follow a circular interactional model that where benefits are reciprocally produced:

> Relational services are defined here as those deeply based on interpersonal interactions, particularly favouring "I-Thou" encounters. They are challenging the standard way of conceiving and offering services. [27, p. 3]

By way of example, Cipolla and Manzini contrast the standard school bus service with a "Walking Bus" relational service. The standard service is conceived as a mechanical operation, wherein the driver can perform his function on an anonymous basis, and can be substituted by another driver with the same technical skills, and where any interpersonal output (e.g. friendship with users) is not seen as an essential part of the operation. The relational service, designed to encourage children to walk to school with a group following predefined routes under supervision of adults (generally pensioners on a voluntary basis) is strongly based on the relational qualities produced between the participants—such that the participants cannot easily be replaced [27, p. 3].

In the Pallion examples encountered in our primary research, the trust engendered in the community by a community hub is not transactional, and does not seem to be replicable in I-it encounters between human and software; it is rather based on the relational qualities produced between the participants. The "care avoidance" instance above, for example, is specifically addressed by the broader relational quality of trust engendered by a community hub well-established in its geographical area, where a person in need of help is typically identified by a concerned neighbour. Pallion Action Group pro-actively encourages this kind of positive security with the use of the phrase "don't wait till you're in crisis" on its Facebook page. "*We know our community inside out and there's a lot of word of mouth and a lot of people have had help from here, so I usually get a people who either message me or send us an email or a Facebook message saying "so and so I'm really worried about them"*" [4].

It is clear that the positive security examples provided by our research present a relational rather than standard model of service design: while specific points of friction might be identified and addressed with improvements in the user experience such as verification-by-phone, or even theoretical innovations to authenticate trusted third parties (for example [28, 29]), the positive security framework facilitates a more holistic reconceptualization of what we mean by security.

5 A Case for Kindness: Understanding Needs in Context

Analogous approaches to positive security can be found in discourse on cities. The sociologists Hall and Smith [3] argue that the routine but often invisible ways in which people are maintaining the city–the "looking after, helping out, cleaning, fixing up" [3, p. 3]—might be reconceived as a "politics of urban kindness" (p. 5). Extending the concept of repair and maintenance to the care and welfare of people, Hall and Smith find analogous examples of the constant upkeep required to maintain the complex machinic order of the city in "minor acts of social repair" from marriage guidance to outreach services, youth mentoring and support groups: an "infrastructure of kindness" (p. 11). This position builds on the ideas of Nigel Thrift, who has argued that cities are responsive to catastrophe in part because they are constantly adding "new circuits of adaptability" [30, p. 202]. One manifestation of these circuits is the "hum of continuous repair and maintenance" from the noise of pneumatic drills to the knock on the door of a repairman to the emergency services cleaning up small but sustained disasters [30, p. 202]

To align the politics of urban kindness with positive security requires that we consider the support work of voluntary and third sector organisations as integral to the design of online services, not an aberration, or workaround. The response to COVID-19, as with a city's response to a natural disaster or other catastrophe, depended not just on digital infrastructures, but the "circuits of adaptability" of social support networks. This in turn requires that the design process also consider the integral role of "minor acts of social repair" and urban kindness in the so-called user journey typically modelled in the design process. To incorporate, for example, a "user's" phone call to a community hub that results in a completed form being mailed back to them for signing and posting suggests a broader, more holistic account of the user experience than a conventional account.

The post-war design of cities was considerably influenced by Jane Jacobs [31] book *The Death and Life of Great American Cities*, which argued in a chapter on safety and security that the public peace is not primarily kept by the police but by an "intricate, almost unconscious network of voluntary controls and standards" kept and enforced by the people who live and work on a street [31, p. 32]. Drawing from her own observations and city crime statistics, Jacobs posited that safe city neighbourhoods had three main qualities: (1) a clear demarcation between public and private, (2) "eyes upon the street," meaning not surveillance cameras or police patrols but the watchful eyes of its residents, business owners, regulars; and (3) streets must be populated fairly continuously, both to increase the number of eyes on the street to give those street watchers something to look at. The street watchers, Jacobs argued, were not looking out for crimes to report, but were engaged in a form of observation that is there to protect the values of the community as decided by the community. “You can’t make people watch streets they do not want to watch” (p. 36). “A lively street always has both its users and pure watchers” (p. 37). Jacobs helped to move city planning away from a separatist approach to city building, and helped bring about the mixed use, more pedestrian friendly spaces that began softening the neighbourhoods annexed by highways and high rises in the 1960s and 1970s.

In a similar way to the minor acts of social repair that keep a community in good order, Jacobs’s “eyes on the street” enact a positive security that enacts a shared value system and even pre-empts breakage. The “word of mouth” scenario described above, whereby a visitor to the community hub confides that they are worried about a neighbour, prevents a potentially greater crisis and enacts a sense of *shared,* ontological security. Roe defines ontological security as “the maintenance of the day-to-day routines that provide us with a sense of who we are and how we relate to others” [2, p. 778]. This can extend to the ambient sounds that we often associate with a sense of bustling or shared spaces. Thrift’s “hum of continuous repair and maintenance” in this sense supports an ontological security that is situated in the everyday routines of people. An example might be the elderly woman who keeps the television on low volume all day to imbue her home with a sense of ontological security.

The aim here is not to varnish, or Romanticise acts of social repair or urban kindness. The “values of a community” are, of course, negotiated by communities, and will include less-than-law-abiding values as well as frequent contraventions of those values, as in the numerous examples of pandemic-era scams that emerged in focus groups with Pallion Action Group. Values and a sense of order are precariously maintained, even with unwritten codes such as that which condones fraudulent Universal Credit claims but not stealing from one’s grandfather, the proverbial “honour amongst thieves” [4]. Hall and Smith also note that keeping things and people well looked after is a political activity as much as it is practical, and this is not a simple politics when “repair” is imposed rather than reciprocal. Rather than present a Romanticised account of kindness as a form of positive security, we argue that narratives driving the design of online services need to take into account these essential but often invisible aspects of system maintenance.

In closing, it is illustrative to identify some of the characteristics of a more dominant narrative of digital security by looking at the current website for the UK Government’s National Cyber Security Centre (NCSC), which presents guidelines and practical steps for individuals and families as part of its broader information section. In defining cyber security, the NCSC clarifies that its “core function” is to protect devices (smartphones, laptops, tablets and computers), services and the personal information stored on them. To improve the cyber security of individuals and families, the NCSC recommends [32] an array of technological solutions: strong passwords, stored in a browser, two-factor authentication, updated devices and frequently backed-up data.

While these are familiar and sound guidelines, they fall short of the security guidance needed in the scenarios presented in our research with community hubs and underserved people. For example, recommending that a family updates its devices presumes they have the financial resources to purchase new devices, and/or the cognitive capacity and sufficient time to negotiate an upgrade of the operating systems on their devices. Backing up data and two-factor authentication similarly depend on sufficient resources to fund cloud storage (or a back-up drive) and the time and cognitive capacity to undertake what are relatively complex tasks.

To revisit the findings of the social change charity cited in our introduction, an estimated 10 million people lack the basic foundational skills needed to access online services [1]. Recognising this, through the Research Institute of Sociotechnical Cyber Security [33], NCSC has supported and taken part in research programmes related to digital responsibility and accessible and inclusive forms of security to better understand the security dimensions of the digital divide.

6 Conclusion: A Case for Kinder Narratives of Digital Security

In this chapter we have drawn from a case study and a literature review to build a case for a more holistic understanding of digital security in the wake of the COVID-19 pandemic. Academics, community practitioners and policymakers must now work together to co-develop the next generation of security guidance that produces safer forms of digital inclusion for both people and technology.

As part of this co-production effort, our case for kindness is a case for inclusiveness and more holistic narratives of digital security, as illustrated by the positive security approaches brought up in our research. To move security forward and better address the disproportionate impact of COVID-19 across the digital divide, we recommend that the narratives driving the design of online systems and the security measures consider the following:

- People who are unable to access online services because they lack appropriate infrastructure
- People who lack sufficient skills and know-how to manage sequences of online tasks
- How trust relations are built, sustained and improved to help people seek and secure support in accessing online services
- The role of voluntary and third sector organizations in building trust and supporting peoples’ access to online services
- Digital literacy within those voluntary and third sector organizations and more generally among those providing informal or formal assisted access to online services.

Such a call to action requires a broader perspective on how access to digital services takes place. At its core, this call to action is asking for our understanding of responsibility for secure digital access to be re-examined—and to conceptualise secure digital access as a form of public good.

Acknowledgements We would like to thank Pallion Action Group and Karen Noble for their participation and generous contributions to this study. Lizzie Coles-Kemp's participation in this study is funded by EPSRC grant EP/N02561X/1 and has been supported by the RISCS Digital Responsibility Fellowship (2020–2022). We would also like to thank Dr. Nick Robinson for his work to set-up the original programme of focus groups.

References

1. Good Things Foundation (2021) A new manifesto for digital inclusion. https://www.goodthingsfoundation.org/insights/new-manifesto-digital-inclusion/
2. Roe P (2008) The "value" of positive security. Rev Int Stud 34:777–794
3. Hall T, Smith RJ (2015) Care and repair and the politics of urban kindness. Sociology 49(1):3–18
4. Noble K (15 Feb 2022) Personal interview with Peter hall
5. Kocksch L, Korn M, Poller A, Wagenknecht S (2018) Caring for IT security: accountabilities, moralities, and oscillations in IT security practices. Proc ACM Hum-Comput Inter 2(CSCW): 1–20
6. Morris A, Coles-Kemp L, Jones W (July 2020) Digitalised welfare: systems for both seeing and working with mess. In: 12th ACM conference on web science companion, pp 26–31
7. Van Dijk J (2020) The network society. Sage, London
8. Age UK (2021) Digital inclusion and older people—how have things changed in a Covid-19 world? Online briefing paper. https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/active-communities/digital-inclusion-in-the-pandemic-final-march-2021.pdf
9. Yates S (2020) COVID-19 and digital exclusion: insights and implications for the Liverpool city region. Policy brief. https://www.liverpool.ac.uk/media/livacuk/publicpolicyamppractice/covid-19/Policy,Brief,031.pdf
10. House of Lords Select Committee on COVID 19, UK Parliament (2021) Select committee on COVID-19. Corrected oral evidence: living online. https://committees.parliament.uk/oralevidence/1736/pdf/
11. McDonald M (2008) Securitization and the construction of security. Eur J Int Rel 14(4):563–587
12. Doty RL (1998) Immigration and the politics of security. Secur Stud 8(2–3):71–93
13. Smith GM (2005) Into cerberus' lair: bringing the idea of security to light. British J Polit Int Relat 7(4):485–507
14. Coles-Kemp L (2020) Inclusive security: digital security meets web science. Found Trends® Web Sci 7(2): 88–241
15. Kazansky B (2021) It depends on your threat model: the anticipatory dimensions of resistance to data-driven surveillance. Big Data Soc 8(1):2053951720985557
16. Coles-Kemp L, Ashenden D (2017) An everyday story of country folk' online? The marginalisation of the internet and social media in the Archers. In: Custard, culverts and cake. Emerald Publishing Limited
17. Tseng E, Sabet M, Bellini R, Sodhi HK, Ristenpart T, Dell N (2022) Care infrastructures for digital security in intimate partner violence. CHI'22. https://emtseng.me/assets/Tseng-2022-CHI-Care-Infrastructures-Digital-Privacy-IPV.pdf

18. Freed D, Palmer J, Minchala D, Levy K, Ristenpart T, Dell N (April 2018) A stalker's paradise, how intimate partner abusers exploit technology. In: Proceedings of the 2018 CHI conference on human factors in computing systems, pp 1–13
19. Matthews T, O'Leary K, Turner A, Sleeper M, Woelfer JP, Shelton M, Manthorne C, Churchill EF, Consolvo S (May 2017) Stories from survivors: privacy & security practices when coping with intimate partner abuse. In: Proceedings of the 2017 CHI conference on human factors in computing systems, pp 2189–2201
20. Naseem M, Younas F, Mustafa M (2020) Designing digital safe spaces for peer support and connectivity in patriarchal contexts. Proc ACM Hum-Comput Inter 4(CSCW2):1–24
21. Ehn P (2008) Participation in design things. PDC '08: proceedings of the tenth conference on participatory design, Bloomington, Indiana, 30 September–4 October 2008. ACM Press, New York, pp 92–101
22. Coles-Kemp L, Ashenden DM, O'Hara K (2018) Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. Polit Gov 6(2):41–48
23. Vines J, Pritchard G, Wright P, Olivier P, Brittain K (2015) An age-old problem: examining the discourses of ageing in HCI and strategies for future research. ACM Trans Comput-Hum Inter (TOCHI) 22(1):1–27
24. Schout G, de Jong G, Zeelen J (2011) Beyond care avoidance and care paralysis: theorizing public mental health care. Sociology 45(4):665–681
25. Qiany S (2020) A personas guideline, from what they are to how to use. UX collective, Sept 23, 2020. https://uxdesign.cc/while-we-are-talking-about-personas-what-exactly-are-we-talking-525a645eb61a
26. Fuglerud KS, Schulz T, Janson AL, Moen A (2020) Co-creating persona scenarios with diverse users enriching inclusive design. In: Antona M, Stephanidis C (eds) Universal access in human-computer interaction. Design approaches and supporting technologies. HCII 2020. Lect Notes Comput Sci, vol 12188. Springer, Cham. https://doi.org/10.1007/978-3-030-49282-3_4
27. Cipolla C, Manzini E (March 2009) Relational services. Knowl, Technol, Policy
28. Barros Pena B, Kursar B, Clarke RE, Alpin K, Holkar M, Vines J (2021) Pick someone who can kick your ass-moneywork in financial third party access. Proc ACM Hum-Comput Inter 4(CSCW3):1–28
29. Dunphy P, Monk A, Vines J, Blythe M, Olivier P (2014) Designing for spontaneous and secure delegation in digital payments. Interact Comput 26(5):417–432
30. Thrift N (2008) Non-representational theory. Routledge, London and New York
31. Jacobs J (1961) The death and life of great American cities. Vintage, New York
32. NCSC (2022) https://www.ncsc.gov.uk/section/information-for/individuals-families
33. Research Institute for Sociotechnical Cyber Security (2022) https://www.riscs.org.uk/digital-responsibility/