Some users are still the enemy

Partha Das Chowdhury, Lucy Davies, and Kopo Marvin Ramokapane

University of Bristol

Abstract. Usable security helped security engineers imagine humans through explicit understanding of individual cognitive *budgets*, their workflows, behavioural realities, so on and so forth. We expand the conceptualisation of humans, and assert that security mechanisms should not only consider what individuals *can*, but should equally prioritise (if not more) what individuals *value*. To that end we propose Amartya Sen's Capability Approach framework to capture individual *beings*, and *doings*; and conceptually evolve *basic cyber capabilities* for migrant sex workers, for exposition.

1 Introduction

Individuals should be able to *securely* participate in a digital society in a manner that they *can*, and *value*. Adam & Sasse's seminal work has provoked a significant body of work to bring humans to the centre of systems design through systematic explorations of human deprivations, abilities, and their situated realities, and how mechanisms that *look secure on paper will fail in practice* without these considerations [3]. We argue that prior research has largely focused on developing the element of *can* participate, but relatively less on the question of the matter of *value*. We draw upon Amartya Sen and formulate a working definition of *value* as

> Individuals are not passive beings waiting for benefaction, but active agents with beings, and doings of their own. Consequently, the freedom to choose, and the ability to act in a manner consistent to that choice, are central to a valued participation in community life [35].

Such a conceptualization of *value* draws from several intellectual traditions such as morals [9], economics [42], social choice theory [36], and justice [37][1]. While

[1] We do not posit *value* in absolute disregarding equity, responsibility and social choice. For example, the freedom to discriminate, or propagate hate online might be valued by some individuals and organizations. Conceptualization of value through capability and agency, draws upon Aristotle's flourishing, Adam Smith's emphasis on moral sentiments of people, Kant's assertion that individuals can choose on principle and the distinct roles of *niti* (law) & *nyay* (manifest justice) in Indian jurisprudence. We adhere to reasoned public participation to define *valued participation.*

they provide a evaluative lens of *capability* & *agency* as value; Sasse's body of work empirically demonstrates that discounting human cognitive diversity, and individual dispositions, in turn, shrinks real opportunities for humans at the end of the system [4,33,32,8].

Motivating Example: Consider the example of a UK police officer who posted sexual content for sale via the subscription platform, OnlyFans [1]. The discovery of this by his employers forced him to resign or face being fired. Additionally, he has been added to a list that bars his future employment in law enforcement or policing [6]. In a related incident, a physics teacher selling her virtual services as a sex worker via the same subscription based platform, lost her job following protests by parents and pupils [7]. The school confirmed that the teacher satisfactorily performed her professional responsibilities as a teacher. The teacher, in turn, explained that she had engaged in sex work as a means of supplementing her income. In both cases, individuals exercised their agency to participate in digital society in a manner they valued, within the bounds of the law. Yet their engagement with a legitimate online platform resulted in significant professional and personal sanctions.

Sex work is legal in the UK, though soliciting is not. Neither of our motivating examples report solicitation as the reason behind *terminating* the employment of the said individuals. While the United Nations and the European Commissioner of Human Rights acknowledge the discrimination commonly faced by sex workers [20], there are significant gaps in technical and regulatory interventions to protect this marginalized group from being othered, discriminated against, or intentionally harmed. In both examples given, the mired relationship between society and sex work culminated in two individuals losing their occupation, dignity, and privacy. Their short and long-term economic and social wellbeing is profoundly impacted through their interaction with technology systems, and the said interactions are neither illicit nor reprehensible. Such manifest outcomes raise a foundational concern for systems design; current approaches inadequately account for the plurality of valued human activities, particularly when those activities intersect with moralized or stigmatized domains.

Human centred security work such as Sasse's [3,2,46] brought humans to the centre of systems design, however this centring was largely instrumental, focussed on *security outcomes* and not so much or not at all, on the need for individuals to pursue the life they *value*. For example, refugee resettlement systems have historically prioritised hard security outcomes and discounted the needs for refugees to be in touch with their families [22]. Such privileging of security outcomes, in turn, narrowed the imagination of humans primarily in terms of their *can* such as skills, cognition, comprehension, and ability. Capturing *can* methodologically translated into a quantitative ordering of preferences based on interactions of various combinations of skills, cognitions, and abilities with technology in essence promoting a utilitarian[2] focus on usability and performance optimisation [15,40,44]. Such approaches have advanced our understanding of

[2] In economics, *utility* has been viewed as preference ordering – the satisfaction derived by an individual from an increased share of a good and its evaluation [34].

what users *can* do but have left comparatively underexamined the question of what users *value* doing, and how systems might support, rather than constrain, those valued forms of participation.

We invoke Sasse's emphasis on individual agency [24], diverse cognitive realities [21] to argue that utilitarian usability while influential and often well-intentioned, has methodological shortcomings. Utilitarianism cannot capture the needs, *valued interactions*, and lived realities of individuals, consequently, shrinking real opportunities for individuals. When systems rely on utilitarian assumptions, they systematically discount the heterogeneous and sometimes socially marginal forms of value that matter to real users. Systems that discount *valued* interactions of users who exist on the margins of social norms, often fail to meet their legitimate security as well as usability expectations; for example, sex workers were conscious of digital risks such as facing bans from non-sex-work platforms, content theft from sex-work-specific platforms, and digitally mediated context-collapse, where an individual's work persona and private life experience a forced collision due to algorithmic design [28].

In this paper, we will explore the current state of the inclusion of sex workers in human centred security research, drawing upon Das Chowdhury et al. [12] to situate *capability approach* as a methodological foundation to capture both what diverse individuals *can*, and they *value*. We then apply the framework to evolve a list of *basic capabilities* for migrant sex workers for exposition; such capabilities will inform systems design that supports, rather than constrains, migrant sex workers to participate in the labor market with dignity and security. We take the core philosophy of Sasse's work and push user-centricity to a new paradigm.

2 State of play

Cybersecurity provisioning, traditionally, decides a security policy and then implements mechanisms to match the policies. Such paradigms inherently assume that humans can manage their own security, e.g., choosing strong passwords, applying patches, and spotting phishing messages. Human centred security research has effectively challenged such unfair and pervasive responsibilization, and unravelled diverse individual realities in order to make them focal variables in systems provisioning exercises. Recent research exploring unfair expectations and responsibilization in cyber security systematically coded the role of usable security over the last few decades in highlighting individual realities of cognition, comprehension, skills, knowledge and behavioural influences [14]. We used their methodology to explore the state of play regarding the inclusion of sex workers in the field. To begin this, we examined citations of two seminal papers which effectively launched the field: "*Users are not the Enemy*" [3] and "*Why Johnny Can't Encrypt*" [46]. These had been cited 2559 and 2047 times, respectively, on 8th July 2025. Our aim is not to exhaustively map all cybersecurity research involving sex workers, but to examine their presence within the influential intellectual lineage shaped by these two foundational works.

Table 1. PRISMA Search

	Users are not the enemy	**Why Johnny can't encrypt**
References	2559 papers	2047 papers
Search within citing articles for term "sex work"	167 papers	118 papers
Accessibility exclusion: Exclude not able to access, not in English and/or duplicates	145 papers	108 papers
Content exclusion: Exclude no mention of "sex work," irrelevant mention and/or non-studies	1 paper	3 papers
Included	**1**	**3**

Inclusion: We reviewed papers that had cited one of the two seminal papers and retained those that: (a) reported on empirical user studies, (b) used the term "sex work", and (c) had been published in a reputable HCI journal (e.g., TOCHI, Computers & Security, IEEE S&P) or conference (e.g., SOUPS, USENIX, CHI, CSCW, WWW, EuroUSEC). This process resulted in 4 papers where "*Users are Not the Enemy*" [3] yielded 1 relevant paper and "*Why Johnny Can't Encrypt*" [46] yielded 3. We did not restrict our search to a time period.

Exclusion: We excluded papers without a user study, those that were not peer reviewed, those that did not mention *sex work*, and those we could not access or that were duplicates. Our dataset is available[3] for the community.

Across the papers identified within this citation network, a consistent pattern emerged: sex workers rarely appear as a primary user group in usable security research. They are referenced incidentally, most often as examples of avenues of users who may warrant future attention, perhaps considered the edgiest of edge cases, suggesting that within this influential lineage of work, they have not been treated as central or representative users.

Kapoor et al.lists sex workers as an example of an 'at-risk population' but they did not engage with this group with in their study, and nor explicitly mentioned them in the recommendations for future work (though platform workers are) [23]. Slupska et al.discussed participatory threat modelling, where the researchers asked workshop participants to *define their own cybersecurity threats*, decentering the 'average user' narrative. Though they were not specifically aiming to co-produce with sex workers, one participant coincidentally had previously engaged in the sex industry and noted that her concerns about her digital privacy were often met with a response of "well you can't expect privacy when you've done that sort of work" [41]. Their findings strongly counter any notion of 'average' through their feminist cybersecurity approach, providing a valuable jumping-off point for further research in this area. Gibson et al.focused on AI 'nudification' applications [19]. Interestingly, their paper used the sex work industry as a positive example of how consent could be validated and age verified. They noted though that the mechanisms for performing this type

[3] https://github.com/parthadc9/Festschrift.git

of verification involve *inherent privacy trade-offs* through the maintenance of a variety of *sensitive identity information*. However, their research found that none of the 20 nudification applications they encountered attempted such verification. Mader et al.investigated Apple's Lockdown Mode, a security hardening setting for iOS. Once again, sex workers are only referenced in the *high-risk users*category, described as those who face an elevated likelihood of a digital attack and/or would experience disproportionate harm from such an attack. Here too, sex workers are acknowledged only abstractly, without empirical engagement or design implications [26].

What is the rationale for their lack of inclusion? There is the understanding of sex workers as a hard-to-reach population [5] but there are also those who work in the sex industry who are interested in contributing to research, such as the Beyond the Gaze project that surveyed 641 sex workers and held 62 semi-structured interviews [43] and McDonald et al.'s paper that had 65 survey responses with 29 interviews [28]. Furthermore, it is equally important not to overlook the ever-burgeoning cohort of academics who are, or have previously been, engaged in sex work, their efforts highlights the availability of expertise from within the community itself. Our investigations highlight a persistent gap in usable security research in capturing the needs of sex workers in ways that foreground the lives they value and the forms of participation they seek to sustain. We draw from [12] to situate Amartya Sen's *capability approach* to systematically capture individual needs, their *valued* interactions, and environmental circumstances. This proposed expansion to the repertoire of human-centred security methodologies, contributes to Sasse's emphasis on building security mechanisms that aligns with users' needs and their mental models.

3 Capability Approach

Amartya Sen outlined the foundations of *capability approach* while critiquing utilitarian and Rawlsian approaches to welfare [39]. This was presented as framework of thought, there by consciously avoiding giving it an epistemological status of 'The' *capability approach*. Individual freedom and human diversity are at the core of any operationalization of this framework. *Capability approach* has two principal elements:

- **Capability:** The opportunities individuals have and the influence of their environment on this.
- **Functioning:** The beings and doings that constitute the qualities of the life an individual wants to live.

Freedom is at the core of *functioning*; this means individuals can choose between multiple possible sets of activities (doings), and *capabilities* evaluate the genuine opportunities available to realise those choices. The framework recognises that mere possession of resources cannot empower individuals to achieve a *functioning*. For example, provisioning a bicycle cannot enable all individuals to achieve the *functioning* of mobility, only those individuals with *capabilities*

such as able physique and adequate roads. Individuals without these will require different forms of support to be mobile with dignity. In the case of sex workers, an example is the legalisation and regulation of sex work in Germany through *Das Prostituiertenschutzgesetz* [10]. This requires legal registration, intended to achieve a *functioning* of safety. However, this assumes *capabilities* such as proof of residency and ability to attend in-person registration. Those who cannot, such as migrants without settled status, are then forced into an underground form of sex-work, risking both client abuse and legal prosecution.

A critical subset of *capabilities* is formulated as ***basic capabilities***:

> *"Basic capability means the freedom to do certain basic things, for example the ability to read and write is a* ***basic capability*** *in certain jurisdictions. They can help 'in deciding on a cut-off point for the purpose of assessing poverty and deprivation' "* [38, p.109].

Delineating a set of *capabilities* as *basic capabilities* makes them focal variables for provisioning. Martha Nussbaum advocated for a universal list of *basic capabilities* while Sen argued for a more contextual list [27,29]. An example of a *basic capability* for individuals with appropriate eye sight is to be able use their eyes to safely cross busy roads. A recognition of this led to the provisioning of zebra crossings with or without push buttons to stop traffic. By extension, similar defaults in cybersecurity mechanisms would enable disadvantaged groups to perform security tasks; for example, one or more age related impairments can act as barriers in applying tasks as multi factor authentication, setting up back ups or configuring updates [18]. Making such barriers, focal variables would ensure elderly individuals are able to set up multi-factor authentication. For sex workers, a basic capability could be to exercise control over their environment through disclosure of their legal name only when they deem necessary. However, algorithmic enabled context collapse can link their work and personal identities together unintentionally. The provision of a mechanism to create truly separate digital identities without requiring separate devices would enable them to achieve this basic capability.

Capability approach based assessment of individual opportunities should be situated at the policy layer [13], in line with the role of regulators in ensuring public safety such as National Highway Transportation Safety Administration (NHTSA) in providing crash-worthiness information, which was followed in Europe by the 'Product Liability Directive' [25]. There are examples of policy interventions to prevent tech-mediated harms; privacy is enshrined in the The Universal Declaration of Human Rights (Article 12), European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). On the other hand, recent concerted campaign by civil society organisations successfully thwarted attempts to dilute the privacy guarantees provided by end to end encrypted messaging applications [30].

4 Case Illustration: Capturing the needs of migrant sex workers

To illustrate the applicability of capability approach, we draw from the Beyond The Gaze project [43]; they combined interviews and surveys with sex workers and with experienced support workers. A key finding of the study was the diversity of types of sex work [17]. The study highlights the barriers that sex workers from disadvantaged groups face; for example migrant sex workers are unable to register with one of the biggest platforms due to their stringent verification process. Platforms exacerbate privacy risks of migrant sex workers. Consequently, they are unable to participate in the market. We draw from feminist studies to conceptually explore *basic capabilities* for migrant sex workers to be able to participate in a digital economy. To that end, we build upon Robeyns' work on selection of relevant *capabilities* in the context of gender inequalities [31].

Barriers faced by migrant sex workers Platforms require all sex workers to register in a privacy intrusive manner that becomes more dangerous for migrant sex workers. For example, the study in [17] reveals a migrant sex worker was required to prove that they are in the U.K. by *clicking a picture in a street holding a newspaper*. There are also fears of immigration risks which in turn determines their access to financial services and their ability to get paid. The vulnerabilities are due to structural reasons; for example, sex work is often conflated with trafficking for migrants. Sex workers can be treated as victims or even traffickers, compounding their exploitation. Consequently, they are further pushed to the margins, and intrusive data collection practices by platforms increases and reproduce the risk for migrant sex workers.

4.1 Capability Approach Based Policy Formulations

In our example, we consider sex work as a desired *functioning* for migrant sex workers. This entails delineation of *basic capabilities* for a minimally adequate participation in the market.

Enumeration of basic capabilities A list of *basic capabilities* is evolved through participation and discussion. Reflecting on the example at hand, a list of *basic capabilities* for participation in the market can be as:

- Should be able to work in a digital labour market they *value*.
- Should be able to securely access such markets.
- Should be able to get paid without infringing their right to a private life.
- Should be protected from violence of any sort.
- Should have access to due process laid down by law.

Whilst these capabilities resonate with our moral intuition, they should be evolved in a methodically sound manner. To that end, we adhere with Sen's formulation of a contextual list refined using the criterion proposed by Robeyns in [31] as:

- **Criterion of explicit formulation:** This criterion specifies that any list should not reflect blatant majoritarianism even within a particular demography. For our example, linguistic minorities among migrant sex workers might not have the numbers to make them an effective lobbying group. Consequently, their language requirements might be lost in majoritarian articulation [45,11]. Looking at our example list, linguistic minority sex workers might not have secure access to labour market, unions or legal representation.
- **Criterion of sensitivity to context:** The previous criterion will ensure that every voice is heard, while this criterion mandates that the incumbent list should reflect their distinct situated realities. For example, the stigmatisation experienced by sexual minorities in certain jurisdictions [16]; this means a list should capture the intersectional context of migrant, and sexual minority sex workers. That will have a direct bearing on being able to be protected from violence of any sort, and other *capabilities*.
- **Criterion of different levels of generality:** This criterion specifies drawing up a general *ideal list* which is then moderated based on political feasibility— *feasible list*. Referring back to our example of linguistic minorities, the *ideal list* can aim to accommodate many languages, while technical and infrastructural constraints might allow implementation of the *feasible list*. However, drawing up the *ideal list* ensures continuous expansion of *capabilities* and in turn, expansion of opportunities for migrant sex workers to participate in the labour market.
- **Criterion of exhaustion and non-reduction:** A list of *basic capabilities* should be granular to the extent that no one element of the list should be reducible to another. For instance, if we bring in our motivating scenario of the teacher and the example *capabilities*, then this would mean multiple distinct labour markets are reflected, or for that matter, the ability to securely access digital markets should not be subsumed under the *capability* to access digital labour markets.

5 Conclusion

Adams & Sasse rightly defied convention when stating *Users Are Not The Enemy*; this paper makes the argument that some users however still are. We make two constructive claims in this paper. The first is that systems that fail empower individuals to participate in a digital society in a manner they *can* and they *value* do a disservice to both legitimate security, and usability expectations of their user. Consequences of a narrow conceptualisation of *the user* can be devastating on individual lives and liberties, even in fairly democratic societies. To that end, we present the *capability approach* framework to capture individual needs, interactions they *value* and their environmental realities to advance the work of usable security from Sasse. We use the framework for a conceptual exploration of *basic capabilities* for migrant sex workers. Our work can go a long way to define the moral norms embedded in systems and in turn the legacy of a

digital-first society. A secure Internet for all - including those made obscure by the blinkers of moral norms and sanctimony - is as much a moral need as it is a requirement for collective resilience against cyber harms.

Acknowledgments. The research is funded through grants EP/Y035313/1, EP/W025361/1, and EP/V011189/1.

References

1. Onlyfans, https://onlyfans.com/
2. Acar, Y., Fahl, S., Mazurek, M.L.: You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In: 2016 IEEE Cybersecurity Development (SecDev). pp. 3–8 (2016)
3. Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999)
4. Adams, A., Sasse, M.A., Lunt, P.: Making passwords secure and usable. In: People and computers XII: proceedings of HCI'97, pp. 1–19. Springer (1997)
5. Barros, A.O., Dias, S.F., Martins, M.R.O.: Hard-to-reach populations of men who have sex with men and sex workers: a systematic review on sampling methods. Systematic Reviews (2015)
6. BBC: Officer barred from policing over OnlyFans profile (2025), https://www.bbc.co.uk/news/articles/c62n0z0g622o?app-referrer=search
7. BBC: Teacher struck off after pupils saw her explicit OnlyFans page (2025), https://www.bbc.co.uk/news/articles/c8xgnxe2lvgo
8. Beautment, A., Sasse, A., Wonham, M.: The compliance budget: managing security behavious in organisations. In: Proceedings of the 2008 New Security Paradigns Workshop. NSPW (2008)
9. Bentham, J.: An introduction to the principles of morals and legislation, eds. The collected works of Jeremy Bentham. University of London/The Athlone Press, London (1970)
10. Bundesministerium für Bildung, F., Senioren, F., Jugend: Prostituiertenschutzgesetz, https://www.bmbfsfj.bund.de/bmbfsfj/themen/gleichstellung/frauen-vor-gewalt-schuetzen/prostituiertenschutzgesetz
11. Bourdieu, P.: Language and symbolic power. Harvard University Press (1991)
12. Chowdhury, P.D., Hernández, A.D., Ramokapane, M., Rashid, A.: From utility to capability: A new paradigm to conceptualize and develop inclusive pets. In: New Security Paradigms Workshop. Association for Computing Machinery (ACM) (2022)
13. Chowdhury, P.D., Renaud, K.: Advocating a policy push toward inclusive and secure "digital-first" societies. IEEE Security & Privacy (2024)
14. Chowdhury, P.D., Renaud, K., Ott, I.: Would 'secure'users lead to secure commons? surprisingly not!: A framework to evaluate effective power and collective outcomes in cybersecurity. In: New Security Paradigms Workshop 2025 (NSPW 2025). Association for Computing Machinery (ACM) (2025)
15. Coopamootoo, K.P.: Usage patterns of privacy-enhancing technologies. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. pp. 1371–1390 (2020)

16. Cui, Y., Yamashita, N., Liu, M., Lee, Y.C.: "So close, yet so far": Exploring sexual-minority women's relationship-building via online dating in china. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. pp. 1–15 (2022)
17. Cunningham, S., Sanders, T., Scoular, J., Campbell, R., Pitcher, J., Hill, K., Valentine-Chase, M., Melissa, C., Aydin, Y., Hamer, R.: Behind the screen: Commercial sex, digital spaces and working online. Technology in society **53**, 47–54 (2018)
18. Das Chowdhury, P., Renaud, K.: 'Ought' should not assume 'Can'. Basic capabilities in cybersecurity to ground sen's capability approach. In: Proceedings of the 2023 New Security Paradigms Workshop. pp. 76–91. ACM, Spain (2023)
19. Gibson, C., Olszewski, D., Brigham, N.G., Crowder, A., Butler, K.R.B., Traynor, P., Redmiles, E.M., Kohno, T.: Analyzing the ai nudification application ecosystem. arXiv (2024)
20. Human Rights Comment: Protecting the human rights of sex workers (2025), https://www.coe.int/en/web/commissioner/blog/2024/-/asset_publisher/aa3hyyf8wKBn/content/protecting-the-human-rights-of-sex-workers
21. Inglesant, P.G., Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In: Proceedings of the sigchi conference on human factors in computing systems. pp. 383–392 (2010)
22. Jensen, R.B., Coles-Kemp, L., Talhouk, R.: When the civic turn turns digital: Designing safe and secure refugee resettlement. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–14 (2020)
23. Kapoor, S., Sun, M., Wang, M., Jazwinska, K., Watkins, E.A.: Weaving privacy and power: On the privacy practices of labor organizers in the u.s. technology industry. ACM Hum.-Comput. Interact. 6, CSCW2 (2022)
24. Kirlappos, I., Sasse, M.A.: What usable security really means: Trusting and engaging users. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 69–78. Springer (2014)
25. Leverett, E., Clayton, R., Anderson, R.: Standardisation and certification of the 'internet of things'. In: Proceedings of WEIS. vol. 2017. University of Cambridge (2017)
26. Mader, B., Eichenmuller, C., Pugliese, G., Eckhardt, D., Benenson, Z.: I blame apple in part for my false expectations: An autoethnographic study of apple's lockdown mode in ios. arXiv (2024)
27. Martha, N.: Nature, function, and capability: Aristotle on political distribution. Oxford Studies in Ancient Philosophy pp. 145–184 (1988)
28. McDonald, A., Barwulor, C., Mazurek, M.L., Schaub, F., Redmiles, E.M.: "it's stressful having all these phones": Investigating sex workers' safety goals, risks, and practices online. In: Proceedings of the 30th USENIX Security Symposium. USENIX (2021)
29. Nussbaum, M.C.: Women and Human Development: The Capabilities Approach. The Seeley Lectures, Cambridge University Press (2000)
30. Peersman, C., Llanos, J.T., May-Chahal, C., McConville, R., Chowdhury, P.D., De Cristofaro, E.: Towards a framework for evaluating csam prevention and detection tools in the context of end-to-end encryption environments: A case study (2023)
31. Robeyns, I.: Sen's capability approach and gender inequality: Selecting relevant capabilities. Feminist Economics **9**(2-3), 61–92 (2003)

32. Ruba Abu-Salma, M., Sasse, A., Bonneau, J., Danilova, A., Naiakshina, A., Smith, M.: Obstacles to the adoption of secure communication tools. In: 2017 IEEE Symposium on Security and Privacy (SP). IEEE (2017)
33. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal **19**(3), 122–131 (2001)
34. Sen, A.: Utility: ideas and terminology. Economics & Philosophy **7**(2), 277–283 (1991)
35. Sen, A.: The political economy of targeting (1992), keynote Address In D. van de Walle and K. Nead, eds., Public Spending and the Poor (Washington, DC, World Bank 1995).
36. Sen, A.: The formulation of rational choice. American Economic Review **84**(2), 385–90 (1994)
37. Sen, A.: The Idea Of Justice. Penguin (2009)
38. Sen, A.K.: The Standard of Living. Tanner Lectures in Human Values, Cambridge: Cambridge University Press (1976)
39. Sen, A.K.: Equality of what? In: McMurrin S Tanner Lectures on Human Values, vol. 1. Cambridge: Cambridge University Press, 1987, Cambridge, UK (1979), reprinted in John Rawls and Charles Fried and Amartya Sen and Thomas C Schelling. Sterling M. McMurrin (Ed), Liberty, Equality and Law
40. Sharevski, F., Zeidieh, A.: Assessing suspicious emails with banner warnings among blind and low-vision users in realistic settings. In: 33rd USENIX Security Symposium (USENIX Security 24). pp. 2083–2100 (2024)
41. Slupska, J., Dawson Duckworth, S.D., Ma, L., Neff, G.: Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In: extended abstracts of the 2021 CHI conference on human factors in computing systems. pp. 1–6 (2021)
42. Smith, A.: An Inquiry into the Nature and Causes of the Wealth of Nations. W. Strahan and T. Cadell, London (1776), reprinted in R.H. Campbell and A.S. Skinner (eds.), The Glasgow Edition of the Works and Correspondence of Adam Smith, Vols. II and III. Oxford: Oxford University Press, 1976.
43. Teela Sanders, Jane Scoular, Rosie Campbell, Jane Pitcher, Stewart Cunningham: Beyond the Gaze: Summary Briefing on Internet Sex Work (2018), https://www.beyond-the-gaze.com/wp-content/uploads/2018/01/BtGbriefingsummaryoverview.pdf
44. Vemou, K., Karyda, M.: A classification of factors influencing low adoption of PETs among SNS users. In: Furnell, S., Lambrinoudakis, C., Lopez, J. (eds.) Trust, Privacy, and Security in Digital Business. pp. 74–84. Lecture Notes in Computer Science, Springer
45. West, S.M.: Data capitalism: Redefining the logics of surveillance and privacy. Business & society **58**(1), 20–41 (2019)
46. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of PGP 5.0. In: USENIX security symposium. vol. 348, pp. 169–184 (1999)