# From Utility to Capability: A New Paradigm to Conceptualize and Develop Inclusive PETs

Partha Das Chowdhury
partha.daschowdhury@bristol.ac.uk
Department of Computer Science
University of Bristol
United Kingdom

Andrés Domínguez Hernández
andres.dominguez@bristol.ac.uk
Department of Computer Science
University of Bristol
United Kingdom

Kopo M. Ramokapane
marvin.ramokapane@bristol.ac.uk
Department of Computer Science
University of Bristol
United Kingdom

Awais Rashid
awais.rashid@bristol.ac.uk
Department of Computer Science
University of Bristol
United Kingdom

## ABSTRACT

The wider adoption of Privacy Enhancing Technologies (PETs) has relied on usability studies – which focus mainly on an assessment of how a specified group of users interface, in particular contexts, with the technical properties of a system. While human-centred efforts in usability aim to achieve important technical improvements and drive technology adoption, a focus on the usability of PETs alone is not enough. PETs development and adoption requires a broadening of focus to adequately capture the specific needs of individuals, particularly of vulnerable individuals and/or individuals in marginalized populations. We argue for a departure, from the utilitarian evaluation of surface features aimed at maximizing adoption, towards a bottom-up evaluation of what real opportunities humans have to use a particular system. We delineate a new paradigm for the way PETs are conceived and developed. To that end, we propose that Amartya Sen's *capability approach* offers a foundation for the comprehensive evaluation of the opportunities individuals have based on their personal and environmental circumstances which can, in turn, inform the evolution of PETs. This includes considerations of vulnerability, age, education, physical and mental ability, language barriers, gender, access to technology, freedom from oppression among many important contextual factors.

**ACM Reference Format:**
Partha Das Chowdhury, Andrés Domínguez Hernández, Kopo M. Ramokapane, and Awais Rashid. 2022. From Utility to Capability: A New Paradigm to Conceptualize and Develop Inclusive PETs. In *New Security Paradigms Workshop (NSPW '22), October 24–27, 2022, North Conway, NH, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3584318.3584323


*NSPW '22, October 24–27, 2022, North Conway, NH, USA*

ACM ISBN 978-1-4503-9866-4/22/10…$15.00
https://doi.org/10.1145/3584318.3584323

## 1 INTRODUCTION

While privacy has been recognised as a fundamental right, there has been debate as to whether technical and regulatory interventions adequately allow everyone, irrespective of their circumstances, to exercise this right [45]. This is tied to the fundamental question of how privacy protection mechanisms are conceived, or the assumptions considered, when designing and building such mechanisms. For instance, PETs have often seen the *human* at the other end of systems as some passive *user* [121]. This notion (of PETs) does not usually account for people's diverse interactions (or lack of) with technology and their vulnerabilities, short or long-term social, political, and economic circumstances. Neither does it grapple with the multiple ways people can be re-identified, profiled and harmed. However, not reflecting on human's diverse realities while developing such systems, may not only hinder adoption due to technical misfit but may be unintentionally harmful [1].

The Human Computer Interaction (HCI) and usable security communities have made a strong case for putting humans at the heart of systems design [6, 33, 99] through cross-pollination with the social sciences and experimentation with participatory and co-design methods. Other fields, for example, security economics, have also made considerable progress in widening the discussions surrounding the end users [4, 5, 79]. While these efforts are recognized in other areas of technological development, the research community behind PETs has remained mostly concerned with corrective mechanisms and questions of usability [29, 96, 121]. For example, Coopamootoo conducted a study to understand the use of privacy methods and highlighted that *ease of use* is one of the important barriers behind low adoption of advanced PETs [29]. But focusing on low adoption and *ease of use* as the main problems, suggests the answer to better PETs is to improve the surface features of their use [96]. When we go beyond the frame of usability, we see other diagnoses of the inadequacy of PETs such as Vemou et al., who identify that PETs are not adequately sensitive to diverse cultures [121].

The pervasive digitization of society requires everyone to engage with digital services, but it also poses the risk of harm as a result of data collection and aggregation, whether or not this is transparent to users. We argue that there is a need to expand the focus of PETs in order to account for the diverse relationships with technology

and realities of age, education, dis/abilities, vulnerability, gender, race, class, marginalized individuals, migrants, and socio-political situations [106]. This is important to avoid harm, exclusion and negative impact on participation in the digital economy by vulnerable individuals. Equitable access to protection mechanisms will enable individuals to enjoy basic protections and human rights – particularly important for vulnerable people. For example, migrants should be able access healthcare without being exposed to data misuse and exploitation.

We contribute to this area by not only discussing the limitations of current approaches to building PETs but also proposing a foundation upon which designers and researchers can build PETs for everyone. Drawing on the work of Amartya Sen [100], we posit that a *capability approach*[1] based evolution of PETs will enable individuals to achieve privacy in a manner they are able to, and they deem valuable. The *capability approach* brings an evaluative space to systematically assess individuals' opportunities to live a private life by putting their freedom of choice at the heart of that assessment. If we view PETs as a tool or service that enables the functioning of a private life, then merely possessing the service will not enable the functioning. There are other key factors such as skill, intelligence, physical ability, as well as social, economic and political circumstances. Exercising privacy, like any social good, would be dependent on these factors and circumstances [104] [2].

A *capability approach* asks what information is necessary to make an evaluative judgment of personal, social, economic and political circumstances for the provision of PETs for diverse social groups and marginalized sections in particular. Such an evaluation aims to inform the building of systems that are appropriate for the particular group. Further, a capability-based provisioning of PETs benefits from capturing the diversity of stakeholders' expectations of any defined system [26, 90]. This notion is a departure from the resource (only) based view, which assumes that having PETs will allow everyone to have a private life [96]. The specific relevance of the capability-based provisioning of PETs can be further enforced by the observed diversity in expectations from and commitments of various stakeholders of any defined system [26, 90]. We outline an interdisciplinary research agenda based on our proposition and invite empirical and methodological dialogue toward conceptualizing and developing more inclusive and human-centric PETs.

## 2 INTERROGATING HUMAN CENTRICITY: THE NEED TO MOVE FROM UTILITY TO CAPABILITY

Individuals should be able to use PETs in a manner that they *can* and that they *value* – intrinsic to this *can* and *value* is human diversity. Human diversity is the fundamental reason we propose *capability approach* as a foundation on which to build PETs – it adequately accounts for diverse human capabilities as well as choice. While the *capability approach* would evaluate individuals in diverse personal and environmental situations to point to the opportunities they have, it will do so against the minimum basic protections that every individual should have – for example, protection against unauthorized information disclosure. Evolution of the list of minimum basic protections as well as evaluation of diverse capabilities in enjoying those protections are integral components of the *capability approach* framework. This two pronged approach is a shift from the traditional utilitarian[3] usability evaluations of system surface features with respect to a priori defined users.

Evaluation of capabilities will capture information on the discrimination and deprivation of vulnerable individuals. The need to capture this is being acknowledged in the literature: McDonald et al. argues that standardizing and advantaged lenses can impair conceptualizations of identities and the privacy needs of vulnerable people, therefore, urges that the HCI community go beyond individuals' perception of risk to consider other conditions (e.g., power structures) that perpetuate the privacy needs of individuals [69]; Wong et al. surveyed prominent literature to understand how systems design is considered with regard to privacy in HCI. They advance the view that in order to realize privacy beyond *solving, supporting and informing*, the privacy by design community must acknowledge privacy systems as socio-technical systems [125]; McDonald et al. describe the shortcomings in commonly used privacy theories in the HCI literature which do not capture individuals who do not adhere to commonly accepted norms or expectations about users. It is challenging to thoroughly capture information about vulnerabilities through the evaluation of surface features. Because of this, some authors argue for moving from norms compliance (c.f. Nissenbaum's contextual integrity [77]) to human vulnerabilities – drawing from, and building upon, feminist, queer-Marxist, and intersectional approaches to inform system design [70].

There have been notable attempts to improve usability by attuning design to the plural lived experiences of users. For example, Hertzum [54] argues for treating usability as a 'sensitizing concept' rather than a predefined concept. This approach invites system designers to consider alternative variants –'images'– of usability such as *universal usability, situational usability, perceived usability, hedonistic usability, organizational usability* and *cultural usability* [53]. Another example is value sensitive design [42, 51], which offers a framework for bringing in social and ethical considerations. Sensitizing design to lived experiences and moral values are powerful in the abstraction they offer to align systems use with situated, emotional and subjective experiences. The argument we make here is that for these powerful abstractions to be effective there needs to be methodological capturing of individuals and their circumstances. Utilitarian logic of systems design, however well-meaning, cannot completely capture adequate information required to design inclusive systems. Sen, in his seminal work on equality, questions the ability of *utility* to capture the concept of "needs" [104][4]. To be sure, this is not to say that usability is irrelevant nor that higher adoption necessarily implies more inclusive systems (as conceptualized in this paper). We propose that to be inclusive –as in not

[1] Amartya Sen articulated the *capability approach* first in Tanner lectures on Human Values, delivered at Stanford University in 1979. Available on Tanner Lectures website, reprinted in John Rawls et al., Liberty, Equality and Law (Cambridge: Cambridge University Press, 1987)

[2] For example, transport as a social good is understood and used differently by different people. For someone without legs, a standard bicycle can never be an effective means of transport, and offering a cycle would be inadequate, to say the least [31].

[3] 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 [102].

[4] Moreover, in *An Introduction to the Principles of Morals and Legislation*, Bentham also highlights the inadequacy of the word *utility* in conveying *interests* and *circumstances* [18]

discriminatory or exclusionary– systems design should refrain from privileging usability and give independent consideration to capabilities [30, 91].

Independent consideration of capabilities means being sensitive to the social practices of individuals in difficult situations–for example refugees with diverse social practices, as well as their relationship with technology that captures their information. Rikke Bjerg et al. engaged over 89 refugees in the process of settling in a new country using a digital re-settlement process. In their paper, the authors lament the HCI community's focus on usability of platforms for provisioning information to migrants – arguing that the centering on surface technical features 'exacerbates the existing barriers in the re-settlement process'.

The *Capability approach* can be used to make interpersonal comparisons of welfare to understand the comparative practical consequences of systems on individuals. Endeavors (like usability images and value sensitive design) to make PETs sensitive need an assessment of the distributive implications of technology. Coles-Kemp et al. conducted a study with 132 *newcomers* seeking resettlement in a new country, employing Ribot and Peluso's [92] theory of access to examine the experiences of participants with digital communications and interactions. They report that, although the HCI community emphasized fit for use and reducing cognitive load, the realization of benefit has not been comprehensively addressed. Systems designed for people in precarious situations should foreground considerations of realization and enablement rather than protection of the system [27]. The assessment of realization of benefit is tied to distributive considerations of justice.

While we argue for moving beyond the utilitarian bias, we do not discount the presence of other factors that negatively affect the adequacy of privacy protection. While the data extraction incentives [70], and utilitarian approaches of technology evaluation [58] are prominent barriers at the supply side, there are also well-known constraints at the demand side such as privacy literacy [48] and accessibility [91]. The successful adoption of PETs has been found to depend not only on factors linked with technical fitness but also on users' understanding of benefits and risks, and the access-ability of their intended users [49, 91]. For example, previous work has shown that individual perception of risks are critical factors in the adoption of privacy protection technology [14], which is further exacerbated by the value individuals are willing to trade for risks they do not perceive or cannot assess [7, 10]. These observed diversities in risk evaluation and awareness often lead to blanket assertions like individuals do not value privacy leading to "victim blaming" [3, 15]. Sen emphasizes the fundamental role these observed diversities play in assessing the capability of individuals [103]. Thus, recognition of diversities in risk perception, awareness and privacy literacy should also be incorporated in to the evaluation of opportunities.

In fine, there is wide recognition in the literature that the mere possession of a tool is not enough for individuals to benefit from the tool – it depends on their health, education, circumstance and other dispositions. An adequate assessment of these dispositions determine the opportunities that individuals have – we propose *capability approach* as the framework to conduct this assessment for building effective PETs. This will allow us to build PETs based on opportunities.

**Significance.** Usability is concerned with how individuals interact with surface features and information provisioning (goods). This has shortcomings since humans differ in their health, ability, education and/or can be in vulnerable situations, displaced from their homes and/or living under oppressive regimes. This diversity of circumstance can have a constraining impact on marginalized and/or vulnerable individuals with respect to their use of technology and eventually exclude them. Therefore, there is a need for more adequate approaches to capture human diversities, deprivations, preferences and design systems.

## 3 CONSEQUENCES OF DISCOUNTING INDIVIDUAL REALITIES

Conventional privacy protections have not not been sufficiently sensitive to the personal, and social circumstances of people. The prevailing view of *privacy as confidentiality* focuses exclusively on protecting data which is considered personal or sensitive, with the assumption that users will have adequate skills to protect their data [47]. While we acknowledge the research towards engineering confidentiality [46], this view needs to be expanded to account for the myriad ways in which people's privacy may be compromised through other means of identification.

One might for instance draw attention to the growing ethical concerns over the use of people's digital traces, including seemingly innocuous data, for purposes of behaviour prediction and nudging, cross-referencing, profiling and policing [21, 119]. In the next subsections, we outline some of the consequences of discounting individual realities manifesting in adverse behaviours and harms linked with the use of information systems.

### 3.1 Information Overload and Asymmetries

Citizens are confronted on a daily basis with myriad data transactions with information systems, yet very little is known about what goes on in the background or what exactly are the quid pro quos of such transactions. How data is collected, transmitted and processed by information systems has remained largely concealed [25]. The way this has been dealt with has been primarily via consent mechanisms and the publication of complex privacy policies. Yet such measures are insufficient given that concerns with the negative consequences of data sharing with commercial and governmental entities can lead people to find workarounds or experience adverse reactions including fear, reticence and feelings of resignation about participating in online activities [36, 87]. We elaborate some of these here.

*Resignation.* A widespread assumption among service providers is that individuals irrespective of their circumstances, will be able to process complex legal jargon [17] and take an informed decision. But shifting the burden of obtaining informed consent to citizens is at odds with adequately empowering them to take control [12, 39]. In fact, this has led to a regime of misinformed and often coercive consent [74]. Clear evidence of this is in the proliferation of purposefully misleading consent controls or *dark patterns* [4, 64]. Such asymmetrical relations engender different adverse behaviours and

feelings of resignation among users. Previous research has shown that there are disconnects between the stated privacy policies and the controls that are used to implement them [13]. Even if a trained individual is able to navigate through complex policies, there might not be adequate controls to enable the functioning of a private life. Service providers take advantage of people's need to access online services and their inability to process the complexities. Contrary to the criticized view of the privacy paradox (see Section 3.3), users have little choice than to accept obscure terms and conditions in exchange for online services either because the risks are not well understood or they are overburdened with information [111].

*Lying.* Requiring the possession of credentials as an obligatory point of passage for the provision of online services might lead to a situation where those who would not posses them or want to remain private, are incentivized to lie. Ramokapane et al. outline the use of lying to access services online [89]. Page et al. analysed survey data from 1532 participants and report the individuals who tend to lie more "have increased boundary preservation concerns as well as increased privacy concerns" [83]. Lying to protect sensitive information and to avoid discrimination has been reported by Van Kleek et al. in their investigation of reasons behind lying behavior online [120]. One can debate around the reason individuals resort to lying [97], but our concern is that many users perceive that the only effective means for them to preserve their privacy and/or dignity online is to lie rather than proper regulatory or technical protections.

*Reticence and fear.* In the last decade, there has been increasing public awareness of the ubiquity of surveillance enabled by the huge amounts of data held by commercial actors (notably social media platforms) and the use of biometrics and face recognition technologies by governments. Numerous studies have evidenced the diverse and *chilling effects* manifesting in practices of self-censorship, self-restraint or change of behaviours online such as limiting sharing of pictures or other information on social media [40, 66]. Humbert et al. conducted a survey on the interdependent privacy risks of individuals by the activities of their friends. Their findings highlight the impact of irresponsible online behavior of individuals on their friends or family who do or do not directly use technology [56]. These reactions limit the function of individuals because they might lose out on the benefits of participating in the digital economy or are afraid of expressing themselves freely.

**Gaps.** An assessment of the abilities of individuals with diverse social and educational backgrounds to process complex technologies, legal documents and/or respond to ubiquitous connected devices, is missing in the evolution of PETs. The extant environment makes it difficult for many to achieve the *functioning* of a private life.

## 3.2 Misplaced expectations about users

The idea of provisioning of PETs is often seen as a special benefaction for individuals, about whom several assumptions are made. Prevalent thinking among developers is toward *fixing* the user. This is true in the way application developers perceive their users and how API providers perceive application developers (intermediate users). For both instances, the diktat is that users should behave in a particular manner else they are threats to the system. A mundane example is the futility of the expectation that users' would heed to SSL certificate warnings even though the over-use of warning messages has been criticised in that they can be counterproductive, thus defeating the purpose they were meant to serve [98].

*The impact on users and non-users.* The field of science and technology studies, and notably feminist scholarship, has been long concerned with how users are configured based on detached and self-referential models by developers (who commonly belong to privileged groups) [35, 82]. Systems are typically built on tendentious assumptions driven by the point of view of said developers on what is *right* for the user. This has led to inadequate generalizations manifesting in problems of misalignment (e.g. gendered technology) or exclusion on the basis of race, age, dis/abilities or other traits [35, 82]. In the context of PETs, a prevalent assumption has been that users should be responsible for their own privacy which could be enhanced by means of anonymity, encryption and secure channels of communication [47]. Users are thus imagined as possessing the right set of knowledge, skills and resources to find and make use of PETs. However, there might be a disconnect between developers' *idealized* assumptions about users and the very specific needs and identities of people at the other end of systems. This is particularly sensitive for those in high-risk, marginalized or vulnerable situations such as whistle blowers, victims of domestic violence, protesters or refugees [22, 61]. Another issue with predefined ideas of use is that developers may be biased towards those expected to interface with technology while being blind to a vast number of non-users (such as the elderly or disconnected), who may not directly interact with online systems but whose data may well be collected by various information systems [84]. Indeed, the frame of 'threats' is primarily concerned with the realm of the web or browser; it neglects the risk of being surveilled by other means such as sensors and IoT devices when such exposure leads to profiling, identification, discrimination and other dangers [34, 110]. With the advent of big data, several ethical issues have come to the fore around the use of peoples' digital traces and statistical prediction for the automation of decisions related to access welfare, employment and public services, credit scoring [16, 95].

An analogy can be made between (threat) modelling thinking and the contractarian model of jurisprudence. Immanuel Kant and Rousseau proposed norms and legal institutions that would effectively compel citizens either to conform, or be outlaws. This approach is geared towards ensuring the survivability of the institutions rather than the wellbeing of the citizens they are meant to serve [107]. In a similar way, the evaluation of systems based on norms operationalization and reductive models about complex human behaviour is usually aimed at fine tuning features that ensure the intended use of systems rather than on what real opportunities individuals have to use these systems [58]. For privacy systems design, privacy policy is decided first, and the mechanisms to implement said policy are decided later. Anyone whose behavior deviates from the specifications of the systems designer is blamed [70]. The protocol designer rarely provides reasons for their expectation of a particular allowed behavior. The problem with these assumptions

is that they make systems rigid and unpleasant to use [32]. HCI research over the last two decades has argued strongly against *blaming* and *fixing* the individual towards being sensitive to their realities [6, 98]. The pandemic times have required people with various levels of backgrounds and deprivations to participate in online activities, for example, students from the poorest parts of the world as well as the elderly who might not be technically conversant[5]. There is a clear need for developers of PETs to study and build for vulnerable groups who are less privileged, less abled or are in risky situations and who may be inadvertently rendered invisible during design. The extant pre-dominant approaches in human centered computing of interviews and focus groups are limited in their ability to capture the lived experiences of individuals [122].

*The impact on developers.* This *contractarian* attitude is also reflected in how security API developers relate to their primary users (developers). Applications developed with third party APIs and responsible for the privacy protection of their users often fail to do so. Hedin et al. studied the flow of information through libraries provided by browser APIs and found that some sites ensured data does not leave the browser, or they only share it with the originating server. Meanwhile, others were freely propagating it to third parties [50]. Acar et al. argue for a better understanding of the motivations and priorities of developers rather than blaming them for not being mindful of security. They stress the need for developer-centered studies to understand the challenges that developers face when using these APIs, and the resources available to improve the usability of these APIs [2]. The APIs used by developers are not easy to use and to add to the challenges, the documentation to use them safely is not readily available or comprehensible. They sometimes interfere with the functionalities of the applications.

**Gaps.** PETs have an expectation of a specified behavior, as well as adequate expertise from individuals who are supposed to benefit from them. However, individuals are *active* agents, acting and doing things on their own. The gap lies in accommodating individuals who might not behave in a particular way as specified by the PETs designer.

## 3.3 Narrowly viewing individual attitudes towards privacy

A manifest shortcoming of failing to recognize humans in different contexts and cultures is the problematic academic view that individuals do not value their privacy based on their seemingly contradictory online behaviour. The depiction of *individuals* as rational beings albeit *selfish* giving information in exchange for 'insignificant' goods and services, led to the characterization of the privacy paradox [3, 5]. This view however has attracted criticism over limitations in the rationale behind this concept where users are viewed as acting irrationally or not in accordance with their stated preferences [111]. Having to sacrifice one's privacy in exchange for access to basic digital services or perceived benefits in the digital economy, might in fact speak more to the existence of coercive data collection systems than users acting incoherently.

While the surface manifestations are studied in the context of HCI, as well as in the economics of privacy literature, we scrutinise if these manifestations are rational. Social choice theory is rich with research assuming rationality as one of many outcomes. When a wedding cake is cut some would want the icing while some the cake; however in most such cases individuals would seldom pick up the largest slice of the cake. This behaviour is inconsistent with the usual formulation with rationality as maximisation of *selfish* interests. However, Sen describes it as 'menu-dependent behavior' given an individual's presumptions about how others will behave. Such behaviors broaden the scope of well being to include social traditions, imitation, as well as behavior driven by morality, sympathy and cohesion among others [106].

When it comes to using online systems humans might have diverse yet perfectly rational reasons to trade-off their privacy (e.g., being overburdened with information or needing to access a service quickly, or just being kind and considerate towards others), which does not necessarily signify carelessness, naivety or indifference towards privacy.

**Gaps.** A distinct shortcoming of fixing users is to reduce the revealed preferences of individuals to simply reluctance or indifference towards privacy. The *functioning* of a private life will need to assess how preferences are moderated by social dynamics.

## 3.4 Power asymmetries and the creation of winners and losers

PETs can potentially rearrange power between individuals and large corporations/nation states who collect, store, process and benefit from information about their customers/citizens. Yet, the formulation of a uniform set of requirements of privacy as universally beneficial for everyone across contexts is canonical and blind to structural inequalities and asymmetries [113]. Such presumed uniformity across contexts fails to adequately account for diversity of circumstance and political reality.

The multidisciplinary field of surveillance studies has extensively debated how commercial and political interests around surveillance engender multiple ethical tensions and creates winners and losers [11, 65]. While disclosing certain information in certain contexts may be deemed fairly unproblematic (e.g., to access students discounts), in more complex cases like criminal records, the degree of disclosure may directly impact equal opportunities for ethnic minorities [113]. The situation is equally complex in the context of medical research. The absence of a transparent, verifiable data protection regime could directly affect legitimate and positive uses of data in medical research [80]. On the other hand the perpetual nature of web ensures that misdeeds of individuals are permanently stored leading to discrimination based on past behaviour [20]. However, enabling individuals to delete their unpleasant past might be in conflict with economic and political interests such as national security, immigration and mobility policies, fraud prevention or policing. In practice, it is not easy for people to delete information they do

[5]https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30169-2/fulltext

not want to have in the public domain about themselves [75, 88]. Indeed, individuals as organised groups are politically weak to sustain the political pressure required for effective regulatory control and regime[6]. Politics remains extremely relevant in the effectiveness of regulatory controls and the benefits of a compromised control regime accruing to whom are pertinent questions in the realm of provisioning of PETs as a social good.

**Gaps.** The provisioning of technology like any public good is political and affects social groups. It is important to assess and understand if the consequences of provisioning specific PETs at varying degrees spawns new kinds of disadvantages for some and/or advantages for others. This would be a reflection of the presence of deliberate influences, if any, on overall welfare interests and freedom in particular political contexts. PETs require appreciation of the individuals in their social, economic and political context; the ongoing tensions; and an evolved understanding of the winners and losers, they might end up creating.

## 4 A BRIEF OVERVIEW OF THE CAPABILITY APPROACH

Sen proposed the *Capability Approach* as a framework of thought and a formula to make interpersonal comparisons of welfare. The framework can be used to analyse well-being and poverty, liberty and freedom, development, gender bias and inequalities, justice and social ethics. Central to the *capability approach* is an active individual with its *beings* and *doings* [105]. The important primitives of the approach can be summarised as:

- Functionings - Functionings are the *beings and doings* of a person. For example, living a private life is functioning.
- Capabilities - This alludes to the idea of opportunity or advantage that an individual has, to achieve from the alternative set of functionings. It is a set of vectors of functionings.

There are two important constituents of the *capability approach*. One is a list of *basic capability*. Sen defines *basic capability* as the ability to *satisfy certain crucially important functionings up to certain minimally adequate levels* [104]. An example of a *basic capability* in the context of social welfare in particular geographies is avoiding premature death. The list is evolved through debate and participation, depending on the context, an example being the basic capabilities for gender inequality assessment in [94]. The other important ingredient is the evaluation of opportunities individuals have to achieve those *basic capabilities*. The reason being the mere possession of a good or service will not enable the functioning. What is needed is to have the skill, intelligence, physical ability, social and political environment – capabilities to achieve a particular functioning. A pertinent example can be in the deployment of differential privacy based systems for privacy preserving data sharing. There are implementation challenges which can benefit from an evaluation of the opportunities of particularly the small and medium enterprises while implementing such systems [37, 57].

[6]The Moral Character of Cryptographic Work, Phillip Rogaway 2015 IACR Distinguished Lecture

As way of illustration, let us consider that the ability to anonymously communicate over the Internet as a *basic capability*. If we have two individuals who both lack the functioning of anonymous communication. Let us now consider if one of them is living under an oppressed regime and the other in a liberal society – then from a political environment perspective, they would have different capabilities to achieve the functioning. So designing and provisioning of PETs would need to be sensitive to their individual political realities. That said, other relevant factors beyond political environment that would influence the functioning would also need to be considered. For example, access to the Internet, health, education, ability, and so forth. In sum, the *capability approach* can be effective to account for human diversities as it goes beyond the body and mind of the user to consider social and political conditions.

In terms of formalizations, Sen [101] and Robeyns [93] presented the *capability approach* as:

If $x_i$ be the vector of commodities possessed by person $i$ and $c(x_i)$ converts the commodities into corresponding characteristics. The function $f_i(c(x_i))$ converts the characteristics into functionings $b_i$ s.t

$b_i = f_i(c(x_i))$.

The function $f$ is $i$ specific because it depends on individual conversion factors, and each individual will choose a $f_i$ of the set $F_i$. Wang mentions that individuals with disability, vulnerability and the realities of socio-economically disadvantaged groups rarely find their interests and choices reflected in security and privacy mechanisms [122]. This function $f_i$ is the determinant in terms of physical and other abilities that Wang suggested to include for inclusive privacy analysis. A person with good health, nutrition and education will have a $f_i \in F_i$ different from someone who does not.

Robeyns extends the original formulation to account for social and environmental factors (e.g., policies, social norms, infrastructure) to be denoted as $z_i$. Then the functioning

$b_i = f_i(c(x_i, z_i))$.

For a given commodity vector $x_i$, $P_i(x_i)$ is the set of functionings feasible for a person $i$ where $f_i(.) \in F_i$.

For any $x_i \in X_i$ where $X_i$ is the set of entitlements (commodities) the capability (or feasible functionings) $Q_i$ is determined as $Q_i(X_i) = b_i | b_i = f_i(c(x_i, z_i))$ where $f_i(.) \in F_i$ and $x_i(.) \in X_i$.

It is worth noting that the strength of the *capability approach* lies in its attentiveness to context, diversity and choice – which might not be adequately reflected, nor should it be lost in formalizations of *capability approach* [93, 101].

**Significance.** We argue for an evaluation that will inform whether everyone is in a position to effectively benefit from the resources (i.e., PETs), irrespective of their deprivations. The *capability approach* offers an opportunity for designers and developers of PETs to build on a critical assessment and understanding of individual realities.

# 5 TOWARDS A SITUATED VIEW OF PETS: AN AGENDA FOR RESEARCH AND INNOVATION

The preceding sections highlighted the need for a sufficient assessment of the real opportunities diverse individuals have to achieve the functioning of a private life. The *capability approach* explicitly departs from welfare evaluations based on the availability of resources and/or policies. This emphasizes an assessment of individual abilities to achieve the *functioning* in a manner they have a *reason to value*. The advantage of this granularity is that diversity will not be subsumed under broad categorizations so as to preserve the interdependence among social groups [94]. For example individuals who do not necessarily fit into 'norms' [69] would not be subsumed within the majority groups. In this section, we propose a research agenda aimed at making those assessments in a rigorous manner.

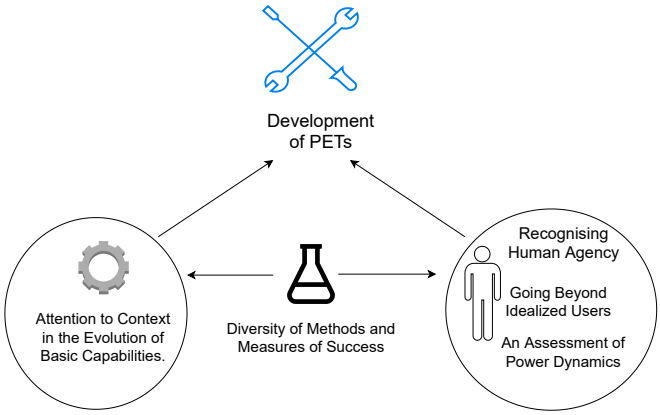


**Figure 1: The research themes with respect to the broad research agenda**

Figure 1 gives an overview of areas of research that should be considered to embed the capability approach as the foundation of PETs. The first area of research focuses on the evolution of the *basic capabilities* that everyone should have. The second area of research aims to understand the individual the PETs intend to protect. However, to fully achieve both elements, there is a need for novel methods and measures of success. Research should identify new ways of recognizing *basic capabilities* and the metrics to qualify PETs as successful and fit for purpose. We discuss these areas in detail below.

## 5.1 Attention to Context in the Evolution of *Basic Capabilities*

In the context of PETs a basic capability can be the *freedom* to perform basic actions online. We should note that *basic capabilities* are not a definite list but should be understood with attention to context. The list can differ across populations with similar parameters of health, education, needs in different socio-cultural contexts. There are distinct groups ranging from migrants, to those living under oppressive regimes as well as citizens living in more liberal societies [45, 47]. These political diversities, when juxtaposed with gender, race, education and other factors, can lead to a contextual granularity to a reasonable extent [99]. The list of *basic capabilities* would determine the basic minimum protection mechanisms to which everyone should have access.

For exposition, we refer to Solove's taxonomy; this is to give a shape to what we propose as *basic capabilities*. Solove proposes four categories of harmful activities, namely (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion [110]. In light of this taxonomy and the harms discussed within each of these four activities, the list of *basic capabilities* would need to be formulated in relation to how harms will provoke interventions such as (PETs) to *satisfy certain crucially important functionings up to certain minimally adequate levels*. A *basic capability* example would be the ability to access state welfare benefits without being subjected to unauthorized disclosure–for instance, surveillance when inferences (whether accurate or not) are made about individuals and groups to inform decisions that affect their lives [40, 115]. Furthermore, for disabled citizens, the *functioning* will be further granulated based on their interface with technology. A recent comprehensive study brings out the risk factors among marginalised and disadvantaged groups, while doing so they pay attention to *context, interactions, protective practices* and *barriers* [123]. This we believe can further support the need for a list of *basic capabilities* and at the same time provoke future research towards the contents of such a list.

The list of harms can be informed by frameworks that elicit the threats and risks associated with the distinct scenarios and interactions that citizen groups have with systems [117]. A pertinent issue is if developers would do this – this is where positioning of the *capability approach* is important. We discuss the alternatives of situating it in the policy layer or with developers/designers further in Section 7. Yet, because evaluations need to be situated, we pose the formulation of *basic capabilities* as an open question to be considered by researchers and practitioners. Prescribing a list risks presuming an antecedent uniformity and that there is a *right* method. Furthermore, the process in which a list of capabilities is evolved is very critical from the perspective of the *capability approach*. Nonetheless, it is pertinent to draw attention to the debates among scholars working in social justice and welfare, for a definite list against evolving a context-dependent list [67, 78].

Systems design consists of layers where each layer builds upon the abstractions of the layers below. The distillation of *basic capabilities* at the user facing layer needs adequate consideration of the layers below. For example a system implementation of a *basic capability* would need systems level reasoning of the rights and permissions of the user with respect to particular data as well as traceability of sub-system components independent of the user. Future research can build upon the foundations of capability architectures proposed in [59, 60].

**Agenda.** Future research can deliberate whether existing propositions like Solove's taxonomy or the LINDDUN framework [109] are adequate or if a nuanced contextual list should evolve through broader participation. A starting point would

be to explore the extent to which the existing recommendations are in synergy with the political and economic maturity of various geographies as well as their cultural and social histories [105].

## 5.2 Going beyond idealized users

However prevalent in the spheres of technology development, the term 'user' is reductive as it may unhelpfully gloss over diverse social realities and socio-technical relations. We need more nuanced categories to represent marginalized, vulnerable groups who do not fit into the conventional definitions of a user. A consideration of being inclusive of diverse observed abilities, needs and circumstances would require accepting them as legitimate focal variables as opposed to naive assumptions of universality. For example, individuals with different degrees of education should not be deceived by complex legal agreements. The plurality of focal variables means that there could be multiple conceptualizations of PETs and other privacy protections, in terms of distribution, participation, abilities, and changing circumstances; at both the individual and collective level.

There is a need to expand the scope of action of privacy protection mechanisms to attend to different socio-technical arrangements and human relations with technology. Designers ought to ask who will benefit from the enhanced privacy protections of a particular design, and who will not. Such assessments concern ethical questions of inclusivity, dignity, and justice [113], which call for a focus on the disadvantaged and their often invisible realities. Recognizing the heterogeneity of socio-technical relations will enable different groups to enjoy social good in a manner they can, neutralizing the limitations (if any) of their opportunities to do so to a reasonable extent. For example, a recent study on online safety settings for couples with memory concerns highlights their need for flexibility without fundamentally altering their relationship [72].

The development of PETs should turn to approaches in sociology such as intersectionality [99] and the well established practice of reflexivity within qualitative research whereby personal biases, assumptions, motivations and institutional commitments can be made visible, if not recognized as potential limitations of design [86]. In her work on 'locating accountabilities in technology production', Suchman has argued for a shift from flawed 'view from nowhere' ideals toward locating design –always from 'somewhere'–in synergy with different ways of being and partaking in technology design [114]. We highlight a few productive efforts which have started to look at ways to attend to the specific security and privacy needs of high-risk or vulnerable individuals such as whistle blowers, protesters, and refugees [38, 108]. Caring for the privacy of both users and non-users will help recontextualize the role of PETs beyond the interface, for example, in response to ubiquitous and pervasive technologies or the various layers of technical systems involving data collection, transport, and processing [34]. The *capability approach* seeks to enable plural conceptualizations of citizens through assessing the diverse abilities of individuals to operate systems, process the risks based on their knowledge and sensory abilities, and interactions (or not) with technology, leading to wider exercising of the *functioning* of a private life.

Our proposition for a nuanced understanding and delineation of *users* requires a broad understanding of the remit of designers/developers. The conceptual framework to operationalize the *capability approach* needs to be contextual with the explicit goal of avoiding generalizations that subsume human diversity. Moreover, discussion about the remits and responsibilities require understanding the distinction between a public good and provisioning of the same public good. Consider, for example, the case of a technology to anonymously browse the web. If agreed to be beneficial to all browser users (a desired *basic capability*), then how the tool is provisioned will determine if everyone is being able to use it in a manner they can and they value – design of the access to the relevant *basic capability*. Such a tool should be decoupled from market considerations and it would be in the remit of internet browser designers and developers to provision it by default. Because the *capability approach* does not presume uniformity, designers/developers will need to attend to specific scenarios and needs (e.g., protecting activists or journalists from state surveillance) where the abilities, needs and expectations will differ [52]. In fine, the mandate for the designer would be to adhere with the agreed *basic capability*, while the remit would be contextual on their target user group. Nevertheless, there will be overlaps between user groups and they are not deviations from the conceptual framework of the *capability approach* [94]. A pertinent question is whether contextuality harms interoperability – our view is that the latter is a back-end systems property [41] and can co-exist with contextuality. Furthermore, the *capability approach* is not restrictive of exclusive services beyond *basic capabilities* keeping specific sections of society in mind.

**Agenda.** Research should focus on a nuanced and systematic understanding of the diverse realities of the individuals that PETs intend to protect and the challenges faced by developers to acquire and act upon such understandings. More apt terminologies, beyond monolithic categories such as 'users', are needed to allude to the intended beneficiaries of PETs in all their diversity. On the other hand we recommend that developers engage in self-audit, reflective practices aimed at making assumptions explicit.

## 5.3 Recognizing human agency

A key consideration of the *capability approach* is that individuals should be able to achieve the *functioning* of a private life in a manner they have a *reason to value*. This puts *agency* at the heart of *functioning*. Individuals reveal information to remote entities and trust them to prevent identification, exposure, and other threats to misuse of the information [116]. Fears of misuse of sensitive information can lead to reticence or lying [89], where individuals act driven by morality, compassion, and less self-centered views of rationality. We argue for allowing self-selection by individuals as a possible alternative to a supply side decision of what is good for them. For example, individuals can choose to share information for medical research provided they are explicitly beneficial and governed by morally appropriate authorities [80]. In other applications,

an individual may willingly subscribe to receive advertisements for certain products without that being an indication that the individual does not value their privacy. A possible self-selection approach and a potential remedy against individuals having to lie (e.g., giving false email addresses) could be to allow them to have an anonymous account with minimum personal data or which cannot be traced back to them [7]; with the caution that this type of solution will still require users to trust an intermediary (i.e., Apple or DuckDuckgo).

While the GDPR Act 6(1)[8] states that *the data subject has given consent to the processing of his or her personal data for one or more specific purposes*, instances of violations [9] brings to the fore the dangers of sharing more information than is required. We are not asserting that making such decisions are within the cognitive load and cognitive capacity of all individuals [28, 111]; we are recommending a more nuanced understanding and representation of the contexts and proportionality thereof. Merchants who violate regulations keep on collecting more data than is required, hiding behind complex consent controls or the opacity that separates end-users from merchants. Such understanding can potentially influence the implementation of the law in both letter and spirit and eliminate excessive data collection right at the point where individuals actively or passively interface with online systems.

Van Der Linden et al. explores software developers' attitudes towards the collection of data from their users. They find that developer's attitudes are not guided by the established principles of being 'adequate, relevant' and 'limited' to the purpose for which the data is collected [118]. This conclusion is being arrived at by the authors while evaluating against specific regulations which might or might not be in sync with what citizens would prefer.

**Agenda.** We recommend further research to empirically understand individual *choices* to give an evaluative understanding of the interactions citizens have a *reason to value*. Our recommendation is for a rigorous understanding of people's choices, intentions, values, and motivations, irrespective of what developers/regulators think are good for citizens. This evaluation can feed into negotiating the proportionality of information disclosure particular to contexts and inform regulations/systems.

## 5.4 A reflexive assessment of power dynamics

While a disciplined assessment of the deprivations, valued interactions of active individuals should form the basis of PETs is an insufficient requirement. Any technical development is not a self-contained exercise but is largely contingent on power structures and what the political and economic forces would be willing to concede. As feminist scholars have shown, the spheres of development have been largely dominated by privileged groups who, despite good intentions, are unable to properly address the experiences of the oppressed, marginalized, disabled or vulnerable. Moreover, organizational affiliations and the exigencies of funding institutions, be they private or public, will constrain developers' scope of action.

There are applicable experiences from provisioning public goods in their disproportionate use and availability among the population– the ability to appropriate operates at many layers. In September 2019, the Court of Justice of the European Union (CJEU) ruled in two cases (C-136/17) and (C-507/17) [44]. In the former, while the court made an implicit acknowledgement of the right to be forgotten, in the latter, the same court limited the territorial scope of the same right. Since CJEU nudged the lawmakers to consider expanding the territorial limits of GDPR, the way forward is driving public opinion for the lawmakers to take it up with their counterparts in other jurisdictions. Google is a profit-making enterprise making use of and profiting from the information they store about individuals. A pertinent question thus relates to the prudence of entrusting Google to decide which information is in the public interest and which is not. The rise of the data economy has put corporations under mounting regulatory scrutiny when it comes to accommodating public interest which is at odds with profits [127].

The other issue concerns the ability among various groups to use a public service when it is available. Several factors engender the widespread uptake of such services, however, a significant contributor to ability is the awareness among citizens of their rights and recourse to violations. The experience is not encouraging among vulnerable sections of society for access to justice in general [43], and when there is access, the battle is far too long and draining[10]. The information asymmetry does not exist by itself but sometimes by bureaucratic design [55]. A strength of the *capability approach* is that along with the explicit consideration for human diversities; it actively factors in political realities as a critical conversion factor for individuals to lead the life they value.

The design of privacy protections should not only recognize the heterogeneity of individual abilities and needs, but interrogate who is (and should be) in a position to devise and recommend said privacy protections without conflict of interest, and which regulatory interventions and political supports are needed to further the technical goals of PETs. In the data economy, the provisioning of privacy protections should be free from the influence of actors who profit, directly or indirectly, from more data collection. Not only that, capability-informed privacy protections cannot, by definition, be subject to payment or tiers of exclusion that would lead to a situation of privacy haves and have-nots. These fundamental tensions demand self-critical reflection about the limitations of designers and developers, the need for more inclusivity in the spheres of research and innovation, and nuanced recognition of the influence of deliberate political and economic forces that can limit what can be achieved in practice.

**Agenda.** The political economy of privacy protection foregrounds that technological responses should not be viewed as a panacea where too much energy is put into driving adoption and carrying out continued usability improvements. The

[7] For this exposition, we refer to a recent initiatives by *DuckDuckgo* and *Apple* to allow users to hide their email addresses by redirecting emails based on preferences, and only those desired by the users will be delivered to them https://www.theverge.com/2021/7/20/22576352/duckduckgo-email-protection-privacy-trackers-apple-alternative

[8] https://eur-lex.europa.eu/eli/reg/2016/679/o

[9] https://ico.org.uk/media/action-weve-taken/enforcement-notices/2620027/emailmovers-limited-en.pdf

[10] The case of the UK post office miscarriage of justice is a good example. See https://www.postofficetrial.com

design of privacy protections should not only recognize the heterogeneity of individual abilities and needs, but interrogate who is (and should be) in a position to devise and recommend said privacy protections, and which regulatory interventions and political supports are needed to further the technical goals of PETs. This calls for a reflexive exercise of the limitations of developers, calls for more inclusivity in the spheres of technical development, and nuanced recognition of the influence of deliberate political and economic forces that can limit what can be achieved in practice.

## 5.5 Diversity of methods and measures of success

A shift from the supply side view of what citizens need to more downstream, plural, conceptualizations of individuals will bring in cogency and make their participation in online activities enjoyable and valuable. The method one adopts to realize the research agenda is crucial to the success of embedding the *capability approach* as a foundation of PETs.

*How to prepare the list of basic capabilities?* The process by which the list of *basic capabilities* and interpersonal comparisons will evolve is crucial for the *capability approach*. Such a list is significant for policy evaluations or measurements related to privacy (or lack thereof). The legitimacy of the list is critical in effecting PETs as a means of social justice and democracy. Sen explicitly recommends debate and democratic participation to evolve the list. Selection will be an inescapable part of this process; which would mean catering to the needs of particularly vulnerable groups, in terms of ability and/or education and environment. Contemporary political philosophers have been engaged with the issues concerning selection in other contexts; we refer to the work of Robeyns for exposition [94]; however, we are not rigid about a particular set of criteria. We briefly outline the criterion Robeyns used to evolve a list of *basic capabilities*. *The criterion of explicit formulation* and *the criterion of methodological justification* requires that the selected *basic capabilities* should be defensible on both these counts. The list is required to be sensitive to the *context* of the target group. *The criterion of generality* specifies that the list should be evolved in two stages. First, a general list and second, a *fine grained* list will be drafted enumerating all the *basic capabilities* a citizen should have. This list will be refined based on local conditions based on data and empirical research. It is important that selected *basic capabilities* might only have negligible overlaps with others to satisfy *the criterion of non-reducability* [94].

*Methods to include individuals with diverse abilities and situations.* Though *human-centered design* (HCD) has dominated conversations as an approach to promote increased adoption and use of systems, this has been often reduced to user studies and consultation [23]. Moreover, there is a limit to what developers can learn from their users, given several social, material, and political constraints [112]. This owes, among other factors, to varying degrees of ignorance and technical literacy, issues of accessibility (cognition, location, vulnerability, language, information overloads), and the presence of vast information asymmetries between users and highly opaque information systems. In re-imagining human-centricity, the *capability approach* entails much more than the notion of *utility* implicit in usability [81] – a preference ordering of satisfaction with regards to surface features. There is a moral obligation of PETs to cater to those whose "body and mind" do not fit the conventional construction of a *user*. Observed diversities and realities are as crucial as those that are unobserved. We borrow the term *unknown known* from [90] to emphasize the emergent and continuously evolving nature of individuals and the environment. Focus groups, interviews, and other participatory research methods have proven highly productive, yet they need to be cautiously implemented so as to avoid exploitation and burden [85] and allow for more generative spaces to understand issues of marginalization and evolving environmental realities. We advocate for more inclusivity in the spheres of design and alliances with methods from social sciences as a means to develop better interventions. For example, Albrecht et al. conducted ethnographic research with 11 protesters from Hong Kong to understand the improvisations and unusual tactics protesters resorted to in order to avoid state surveillance [8]. Schlesinger et al. introduce the sociological framework of 'intersectionality' in HCI to understand the complex identities and experiences with marginalization of individuals. While they acknowledge the progress made in unpacking questions of identity, they also point out the gaps in addressing multiple forms of exclusion and oppression based on gender, race or class [99]. Such conceptual and methodological frameworks can feed into the normative evaluations of the conversion factors of individuals to achieve the *functioning* of a private life in similar situations.

*How to measure success of adopting the capability approach?* While we depart from the comparison of welfare based on possession of resources, the critical question is how do we propose to evaluate PETs built using the *capability approach*. Conventionally, technologies have been mainly measured in terms of their adoption or acceptability which cannot always account for unexpected uses and reactions, or the effectiveness of the technology to live up to its promises. Future research can delve into the metrics and assessments which are not merely techno-centric but can more adequately reflect how citizens are able to exercise their *functionings* and enjoy their right to privacy. *Functionings* can be observed not only quantitatively but qualitatively, for example, if a journalist living under an oppressive regime can exercise their right to a private life without oppression. Measures of success should factor in the diversity of beneficiaries according to their situations and complex identities with respect to race, age, ethnicity, gender, sexuality, social and political realities, physical handicap, mental health, pregnancy, or have caring responsibilities. While factoring in diversity, adequate care should be taken to limit the discrimination among users and exclusion of non-users.

**Moral.** We do not advocate an explicitly reductionist [9] approach in operationalizing the *capability approach* by applying laws/results from one discipline to another. The inherent scale and complexity of human diversity and technology

respectively would reveal new assumptions, needs and compromises. These new assumptions, needs and compromises are as fundamental to our discipline as their counterparts in other disciplines. Adoption of the *capability approach* to address them for PETs would require as much rigor as any other discipline.

## 6 CASE ILLUSTRATION

In Section 2 we make a case for an informationally adequate approach to serve as the foundation of PETs, describing the *capability approach* and proposing a research agenda in Sections 4 and 5 respectively. Here we ground our framework by making a preliminary assessment of its implications on specific cases – this we term as case implication justification[11].

The National Cyber Security Centre UK (NCSC) annual review, 2020 highlights that many cyber security attacks can be prevented through simple steps. However a considerable proportion of the public are often found reluctant to take those steps[12]. We explore the safe social media usage guidelines published by NCSC[13], particularly the guideline on digital footprints in the Section "Understanding your digital footprint", as a case in point to explore:

- Can individuals take those steps in a manner they can and they value?
- Where and how do we situate capability approach?

We restrict our discussion of digital footprints with respect to social media in this paper.

*Can individuals take those steps in a manner they can and they value?* An important guideline suggested by NCSC states:

> "Think about what you're posting, and who has access to it. Have you configured the privacy options so that it's only accessible to the people you want to see it?"

McDonalds et al. explored the privacy narratives set by large social media companies which have a deliberate influence on the privacy features and controls available to their users [71]. Their findings report that Snapchat creates a false sense that user data is ephemeral through a misleading description of the self. The authors also identify the misleading assertions made by Facebook regarding data shared with friends without explicitly stating the same is shared with advertisers as well. Summarising, the authors report that the large companies are conservative with the truth, confusing users with hard to comprehend terms and create an illusion of control and power. A study by Marwick et al. highlights the helplessness felt among socio-economically disadvantaged youth when it comes to privacy in the networked world; they are the most susceptible to privacy violations yet they are unable to comprehend the dangers to which they are exposed [68]. In 2019, when deciding on whether a person has the capacity to decide on their internet and social media use, a judge in the United Kingdom observed [14]:

> I do not envisage that the precise details or mechanisms of the privacy settings need to be understood, but P should be capable of understanding that they exist and be able to decide (with support) whether to apply them.

The other pertinent issue is whether individuals can exercise those steps in a manner they value – this entails the notion of agency [106]. The continuous advancement of norms by the large social media companies as cultural adaptations leads to an environment of exclusion for those who do not fall into these norms [70]. The equation of norms to cultural adaptations subsumes the nuances of human diversity like vulnerable personal identities, as well as groups like socio-economically disadvantaged, refugees and the persecuted in oppressive regimes. Majoritarian norms as cultural adaptations do not augur well for those in the minority in social media platforms – for example, Facebook discounts bad behavior such as targeted bullying as a 'natural outcome of social interactions [71]'. Moving on from individuals to the environment, the cases of abuse of human rights and freedom of the press in various parts of the world are well documented[15]. Citizens in some parts of the world, even when equipped with the resources (e.g., devices and the Internet), are not able to exercise their *functioning* of private life and freedom of speech. Citizens live in an environment where they are profiled and watched without their knowledge or consent, even when they do not directly interact with technology. The prominent social media narrative of "nothing to fear" if conformed to "acceptable" behavior norms, leads to serious persecution of activists and political minority groups living in oppressed regimes[16].

*Where and how do we situate the capability approach?* This will be a brief theoretical exploration of the deployment of the *capability approach* to enable social media privacy for individuals in a manner they can and they value.

(1) **Basic capabilities** - The list of *basic capabilities* forms an important pivot of the *capability approach*. A key requirement of the *capability approach* is that such a list should evolve through public participation and democratic means. There are suggestions of using legal reasoning [126] to evolve cyber security controls – the authors contend that "Controls will be prioritised based on reasonableness or appropriateness rather than effectiveness". The distributive considerations of the *capability approach* can serve as an important ingredient in the paradigm of "law inheriting cyber-security" to consider matters of realised justice as opposed to only law [32, 107].
(2) **Understanding users** – We delineate *going beyond the user* and *recognizing human agency* as two key research agendas in the realization of the *capability approach*. With respect to our case of social media protections against digital footprints, the *capability approach* points to the information on social norms, habits, age, education and ability to make an evaluation of well being and deprivations. The individual, their freedom and choices are at the heart of this assessment. This information can be used to create personas [62] that

[11] Sen coined the term case implication critique while referring to the shortcomings of utilitarian utility and Rawlsian equality in [104]
[12] https://www.ncsc.gov.uk/news/annual-review-2020
[13] https://www.ncsc.gov.uk/pdfs/guidance/social-media-how-to-use-it-safely.pdf
[14] https://www.bailii.org/ew/cases/EWCOP/2019/3.html
[15] https://commonslibrary.parliament.uk/research-briefings/cdp-2020-0063/
[16] https://reutersinstitute.politics.ox.ac.uk/news/religious-riots-grow-india-critics-accuse-facebook-fanning-flames

represent those very individuals for whom the privacy controls are being designed. Cyber security narratives can be created to explain protection mechanisms to the personas in a manner that they understand, will be able to operate and that they would enjoy. An effective example of narration in cyber security can be referred in [63].

(3) **A reflexive assessment of power dynamics** – In our extant case, understanding human diversity is not enough due to the power asymmetry that exists between individuals and large social media companies. West examines the rise of data capitalism and the narratives that have always been built to propagate the appropriation of data, often at the cost of individual rights – language played an important role here [124]. This is further exacerbated when the less powerful are not conversant with the language with which power operates [19]. We propose that the *capability approach*, with its informational richness on *basic capabilities* and *human diversity*, be referred by the regulator to set the narrative so that individuals are not exploited through a false sense of security and benefit.

## 7 CONCLUSION

In our view of using the *capability approach* as a foundation for building PETs, we recognize the moral obligation of any privacy protection mechanism to human agency and diversity. This view attends to the need to cater for individuals in all their complexity, and advocates for empathy, accountability and transparency in the process of development. Much in line with Suchman's critique of objectivist 'design from nowhere' claims [114], we advance that the design of privacy protections should be reflective of partial views and institutional limitations, while sensitive to the plural realities of users and non-users of technology, their diverse needs, locations, lived experiences, identities, preferences, abilities, and social and environmental conditions. This can be achieved by foregrounding developers' commitments and preconceptions and inviting all stakeholders not only to deliberate but to conceive better ways to protect privacy. It is important to acknowledge that in any human-centered approach, the ability to garner privacy requirements is encumbered by limits in the knowledge possessed by the selected cohort of users and their actual means to inform designers on what is needed [112]. Overlooking these constraints could be detrimental if it creates a false sense of certainty and human centricity. As recent studies on surveillance have shown, privacy violations linked with algorithmic behavior prediction are highly complex and can occur completely unbeknownst to people even when *good* legal privacy provisions and technical measures are in place [73]. Because of this, more attention has been given to ethical issues associated with the datafication of human activity and its use for statistical inference and prediction of future behaviour [76]. Opacity not only makes locating responsibilities difficult but unavoidably creates a situation of unevenly distributed costs and benefits. This underpins our emphasis on promoting reflexivity to surfacing power asymmetries and structural inequalities in technology design and development. Our proposal calls for a bottom-up view of citizens in their environment (particularly those in vulnerable situations), which aims to expand the repertoire of empirical methods to inform socio-technical interventions.

We end with a high level view of the steps to enable a bottom-up view of citizens in their realities as in Figure 2.

(1) **Situation of capability approach** – This we believe is an immediate step – meaning whether it should be situated at the level of technology policy or at the level of implementation of technology. The former would mean the interventions at the level of policy leading to comprehensible guidelines for implementations.

(2) **Method of evolution of list of basic capabilities** – Once we ascertain the placement of the *capability approach* the next step can be the method to evolve the list of *basic capabilities* – the minimum functionings every individual should have. While there are examples between a definitive list against a more contextual ones – the method will output a list that is 'appropriate' and 'reasonable'.

(3) **Understanding of Opportunities** – One can refer to the work of United Nations Development Program's adoption of the *capability approach* to food security for exposition on the granularity of data collection [24]. This mixed method step includes:

- determining the focal variable(s) – would we assess individuals based only on their education or include more observed diversities. This would range from education, ability, gender, age to cultural and religious beliefs;
- agency – "the ability of people to help themselves and also to influence the world" [103];
- political and social environment – an understanding of the individual in its circumstances.

(4) **Assessment of opportunities against functioning** – Once we have a understanding of opportunities, this is used to evaluate them against the functioning of, for example, private life. Here, cultural beliefs would indicate their language and communication preferences, along with their privacy beliefs.

The steps we present here are for exposition and are not comprehensive – drawn from the applications of the *capability approach* in other domains.

## ACKNOWLEDGMENTS

We thank the anonymous reviewers, Ola Michalec and our shepherd Tara Whalen & Karl Levitt whose comments helped improve the paper greatly. This work is supported by REPHRAIN: National Research centre on Privacy, Harm Reduction and Adversarial Influence online (EPSRC Grant: EP/V011189/1).

## REFERENCES

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. 137–153. https://doi.org/10.1109/SP.2017.65

[2] Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2016. You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. In *2016 IEEE Cybersecurity Development (SecDev)*. 3–8. https://doi.org/10.1109/SecDev.2016.013

[3] Alessandro Acquisti. 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. In *Proceedings of the 5th ACM Conference on Electronic*

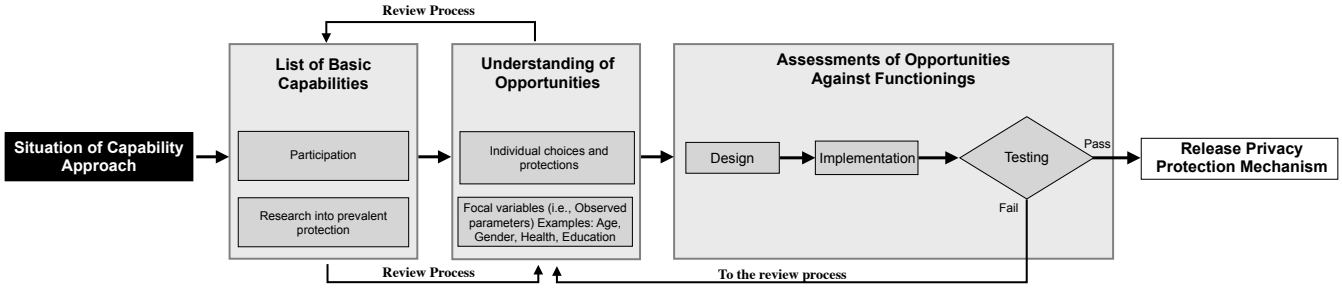


**Figure 2: Stages of Implementation**

*Commerce* (New York, NY, USA) *(EC '04)*. Association for Computing Machinery, New York, NY, USA, 21–29. https://doi.org/10.1145/988772.988777

[4] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2021. Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving it in the Digital Age. *Journal of Consumer Psychology* (2021).

[5] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The Economics of Privacy. *Journal of Economic Literature* 54, 2 (June 2016), 442–92. https://doi.org/10.1257/jel.54.2.442

[6] Anne Adams and Martina Angela Sasse. 1999. Users Are Not The Enemy. *Commun. ACM* 42, 12 (1999), 40–46. https://doi.org/10.1145/322796.322806

[7] George A. Akerlof. 1970. The Market for "Lemons":: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics* 84, 3 (1970), 488–500. https://ideas.repec.org/a/oup/qjecon/v84y1970i3p488-500..html

[8] Martin Albrecht, Jorge Blasco Alis, Rikke Bjerg Jensen, and Lenka Marekova. 2021. Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong. In *Proceedings of the 30th USENIX Security Symposium*. USENIX.

[9] P. W. Anderson. 1972. More Is Different. *Science* 177, 4047 (1972), 393–396.

[10] Ross Anderson. 2001. Why information security is hard-an economic perspective. In *Seventeenth Annual Computer Security Applications Conference*. IEEE, 358–365.

[11] Mark Andrejevic and Kelly Gates. 2014. Big Data Surveillance: Introduction. *Surveillance & Society* 12, 2 (May 2014), 185–196. https://doi.org/10.24908/ss.v12i2.5242

[12] Pauline Anthonysamy, Phil Greenwood, and Awais Rashid. 2013. Social Networking Privacy: Understanding The Disconnect From Policy to Controls. *Computer* 46, 6 (2013), 60–67.

[13] Pauline Anthonysamy, Awais Rashid, and Phil Greenwood. 2011. Do the Privacy Policies Reflect the Privacy Controls on Social Networks?. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. 1155–1158. https://doi.org/10.1109/PASSAT/SocialCom.2011.150

[14] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).

[15] Susan B Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* (2006).

[16] Solon Barocas and Andrew D. Selbst. 2016. Big Data's Disparate Impact. *California Law Review* 104, 3 (2016), 671–732. http://www.jstor.org/stable/24758720 Publisher: California Law Review, Inc..

[17] Omri Ben-Shahar. 2019. Data pollution. *Journal of Legal Analysis* 11 (2019), 104–159.

[18] Jeremy Bentham. 1970. An Introduction to the Principles of Morals and Legislation, eds. *The collected works of Jeremy Bentham. University of London/The Athlone Press, London* (1970).

[19] Pierre Bourdieu. 1991. *Language and symbolic power*. Harvard University Press.

[20] L. Brandimarte, J. Vosgerau, and A Acquisti. 2018. Differential discounting and present impact of past information. *Journal of Experimental Psychology: General* (2018).

[21] Sarah Brayne. 2017. Big Data Surveillance: The Case of Policing. *American Sociological Review* 82, 5 (Oct. 2017), 977–1008. https://doi.org/10.1177/0003122417725865 Publisher: SAGE Publications Inc.

[22] Ian Brown. 2015. Social media surveillance. *The international encyclopedia of digital communication and society* (2015), 1–7.

[23] Richard Buchanan. 2001. Human Dignity and Human Rights: Thoughts on the Principles of Human-Centered Design. *Design Issues* 17, 3 (07 2001), 35–39. https://doi.org/10.1162/074793601750357178 arXiv:https://direct.mit.edu/desi/article-pdf/17/3/35/1713490/074793601750357178.pdf

[24] Francesco Burchi, Pasquale De Muro, et al. 2012. A human development and capability approach to food security: Conceptual framework and informational basis. *Background paper* 8 (2012).

[25] David Chaum. 1985. Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. ACM* 28, 10 (Oct. 1985), 1030–1044. https://doi.org/10.1145/4372.4373

[26] Bruce Christianson. 2013. Living In An Impossible World. *Philosophy and Technology* 26, 4 (January 2013), 411–429.

[27] Lizzie Coles-Kemp and Rikke Bjerg Jensen. 2019. Accessing a New Land: Designing for a Social Conceptualisation of Access. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12.

[28] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. *Informing the Design of a Personalized Privacy Assistant for the Internet of Things*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[29] Kovila P.L. Coopamootoo. 2020. *Usage Patterns of Privacy-Enhancing Technologies*. 1371–1390.

[30] Lorrie Faith Cranor. 2008. A Framework for Reasoning about the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (San Francisco, California) *(UPSEC'08)*. USENIX Association, Article 1, 15 pages.

[31] David A. Crocker and Ingrid Robeyns. 2009. *Capability and Agency*. Cambridge University Press, 60–90. https://doi.org/10.1017/CBO9780511800511.005

[32] Partha Das Chowdhury and Bruce Christianson. 2010. More Security or Less Insecurity, In B. Christianson and J. A. Malcolm editors, The 18th International Security Protocols Workshop, Cambridge, UK,. *Unknown Journal* 115-119.

[33] Steve Dodier-Lazaro, Ruba Abu-Salma, Ingolf Becker, and M Angela Sasse. 2017. From paternalistic to user-centred security: Putting users first with value-sensitive design. In *CHI 2017 Workshop on Values in Computing*. Values In Computing.

[34] Andrés Domínguez Hernández. forthcoming 2022. On Being Specific About Internet of Things Users and Non-users. In *EMPATHY: Empowering People in Dealing with Internet of Things Ecosystems. Workshop co-located with AVI 2022, June 8, 2022* (Rome).

[35] Niels van Doorn and Liesbet van Zoonen. 2008. Theorizing gender and the internet: Past, present, and future. In *Routledge Handbook of Internet Politics*. Routledge. Num Pages: 14.

[36] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media & Society* 21, 8 (Aug. 2019), 1824–1839. https://doi.org/10.1177/1461444819833331 Publisher: SAGE Publications.

[37] Cynthia Dwork, Nitin Kohli, and Deirdre Mulligan. 2019. Differential privacy in practice: Expose your epsilons! *Journal of Privacy and Confidentiality* 9, 2 (2019).

[38] Ksenia Ermoshina, H. Halpin, and F. Musiani. [n. d.]. Can Johnny build a protocol? Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols. https://doi.org/10.14722/EUROUSEC.2017.23016

[39] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-Scale Readability Analysis of Privacy Policies. In *Proceedings of the International Conference on Web Intelligence, Leipzig, Germany, August 23-26, 2017*. ACM, 18–25. https://doi.org/10.1145/3106426.3106427

[40] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. 2017. Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 1800–1811. https://doi.org/10.1145/2998181.2998273

[41] Interoperability Framework. 2004. European interoperability framework for pan-european egovernment services.

[42] Batya Friedman. 1996. Value-sensitive design. *interactions* 3, 6 (1996), 16–23.

[43] Nick Gill, Jennifer Allsopp, Andrew Burridge, Daniel Fisher, Melanie Griffiths, Natalia Paszkiewicz, and Rebecca Rotter. 2021. The tribunal atmosphere: On

qualitative barriers to access to justice. *Geoforum* 119 (2021), 61–71. https://doi.org/10.1016/j.geoforum.2020.11.002

[44] Jure Globocnik. 2020. The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17). *GRUR International* 69, 4 (02 2020), 380–388. https://doi.org/10.1093/grurint/ikaa002 arXiv:https://academic.oup.com/grurint/article-pdf/69/4/380/33045743/ikaa002.pdf

[45] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. *Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants.* Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3173574.3173688

[46] Seda Gürses, Carmela Troncoso, and Claudia Diaz. 2011. Engineering privacy by design. *Computers, Privacy & Data Protection* 14, 3 (2011), 25.

[47] Seda Gürses. 2010. PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. *Identity in the Information Society* 3, 3 (Dec. 2010), 539–563. https://doi.org/10.1007/s12394-010-0073-8

[48] David Harborth and Sebastian Pape. 2020. How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 51, 1 (2020), 51–69.

[49] David Harborth, Sebastian Pape, and Kai Rannenberg. 2020. Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and Jondonym. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020).

[50] Daniel Hedin, Arnar Birgisson, Luciano Bello, and Andrei Sabelfeld. 2014. JSFlow: Tracking Information Flow in JavaScript and Its APIs. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing* (Gyeongju, Republic of Korea) *(SAC '14)*. Association for Computing Machinery, New York, NY, USA, 1663–1671. https://doi.org/10.1145/2554850.2554909

[51] David G Hendry, Batya Friedman, and Stephanie Ballard. 2021. Value sensitive design as a formative framework. *Ethics and Information Technology* 23, 1 (2021), 39–44.

[52] Dominik Herrmann, Jens Lindemann, Ephraim Zimmer, and Hannes Federrath. 2015. Anonymity Online for Everyone: What is missing for zero-effort privacy on the Internet?. In *International Workshop on Open Problems in Network Security*. Springer, 82–94.

[53] Morten Hertzum. 2010. Images of usability. *Intl. Journal of Human–Computer Interaction* 26, 6 (2010), 567–600.

[54] Morten Hertzum. 2018. Commentary: Usability—A Sensitizing Concept. *Human–Computer Interaction* 33, 2 (2018), 178–181.

[55] Christopher Hood. 1995. Control over Bureaucracy: Cultural Theory and Institutional Variety. *Journal of Public Policy* 15, 3 (1995), 207–230. http://www.jstor.org/stable/4007533

[56] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A Survey on Interdependent Privacy. *ACM Comput. Surv.* 52, 6, Article 122 (Oct. 2019), 40 pages. https://doi.org/10.1145/3360498

[57] Marko Jäntti. 2020. Studying Data Privacy Management in Small and Medium-Sized IT Companies. In *2020 14th International Conference on Innovations in Information Technology (IIT)*. IEEE, 57–62.

[58] Rikke Bjerg Jensen, Lizzie Coles-Kemp, and Reem Talhouk. 2020. *When the Civic Turn Turns Digital: Designing Safe and Secure Refugee Resettlement.* Association for Computing Machinery, New York, NY, USA, 1–14.

[59] Anita K Jones. 1980. Capability architecture revisited. *ACM SIGOPS Operating Systems Review* 14, 3 (1980), 33–35.

[60] Paul A Karger and Andrew J Herbert. 1984. An augmented capability architecture to support lattice security and traceability of access. In *1984 IEEE Symposium on Security and Privacy*. IEEE, 2–2.

[61] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* (2018).

[62] Makayla M Lewis and Lizzie Coles-Kemp. 2014. Who says personas can't dance? The use of comic strips to design information security personas. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. 2485–2490.

[63] Genevieve Liveley. [n. d.]. Stories of Cyber Security Combined Report. ([n. d.]).

[64] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a Light on Dark Patterns. *Journal of Legal Analysis* 13, 1 (March 2021), 43–109. https://doi.org/10.1093/jla/laaa006 Publisher: Oxford Academic.

[65] David Lyon. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society* 1, 2 (July 2014), 2053951714541861. https://doi.org/10.1177/2053951714541861 Publisher: SAGE Publications Ltd.

[66] Ivan Manokha. 2018. Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society* 16, 2 (July 2018), 219–237. https://doi.org/10.24908/ss.v16i2.8346

[67] Nussbaum Martha. 1988. Nature, Function, and Capability: Aristotle on Political Distribution. *Oxford Studies in Ancient Philosophy* (1988), 145–184.

[68] Alice Marwick, Claire Fontaine, and Danah Boyd. 2017. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society* 3, 2 (2017), 2056305117710455.

[69] Nora McDonald, Karla Badillo-Urquiola, Morgan G Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J Wisniewski. 2020. Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.

[70] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[71] Nora McDonald and Andrea Forte. 2021. Powerful Privacy Norms in Social Network Discourse. 5, CSCW2, Article 421 (2021), 27 pages.

[72] Nora McDonald and Helena M. Mentis. 2021. Building for 'We': Safety Settings for Couples with Memory Concerns. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, Article 554.

[73] Kevin Miller. [n. d.]. Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm. 19, 1 ([n. d.]), 105–146. https://heinonline.org/HOL/P?h=hein.journals/jtlp19&i=111

[74] Lynette I. Millett, Batya Friedman, and Edward Felten. 2001. Cookies and Web Browser Design: Toward Realizing Informed Consent Online. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Seattle, Washington, USA) *(CHI '01)*. Association for Computing Machinery, New York, NY, USA, 46–52. https://doi.org/10.1145/365024.365034

[75] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. 2018. "If I press delete, it's gone" - User Understanding of Online Data Deletion and Expiration. In *Fourteenth Symposium on Usable Privacy and Security, SOUPS 2018, Baltimore, MD, USA, August 12-14, 2018*, Mary Ellen Zurko and Heather Richter Lipford (Eds.). USENIX Association, 329–339. https://www.usenix.org/conference/soups2018/presentation/murillo

[76] Rainer Mühlhoff. 2020. Predictive Privacy: Towards an Applied Ethics of Data Analytics. *SSRN Electronic Journal* (2020). https://doi.org/10.2139/ssrn.3724185

[77] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[78] Martha C. Nussbaum. 2000. *Women and Human Development: The Capabilities Approach.* Cambridge University Press. https://doi.org/10.1017/CBO9780511841286

[79] Andrew Odlyzko. 2003. Privacy, Economics, and Price Discrimination on the Internet. In *Proceedings of the 5th International Conference on Electronic Commerce* (Pittsburgh, Pennsylvania, USA) *(ICEC '03)*. Association for Computing Machinery, New York, NY, USA, 355–366. https://doi.org/10.1145/948005.948051

[80] Nuffield Council on Bio-Ethics. 2015. *The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues.* Technical Report 558. Nuffield Council on Bio-Ethics.

[81] Ilse Oosterlaken. 2009. Design for Development: A Capability Approach. *Design Issues* 25, 4 (10 2009), 91–102. https://doi.org/10.1162/desi.2009.25.4.91 arXiv:https://direct.mit.edu/desi/article-pdf/25/4/91/1714696/desi.2009.25.4.91.pdf

[82] Nelly Oudshoorn, Els Rommes, and Marcelle Stienstra. 2004. Configuring the User as Everybody: Gender and Design Cultures in Information and Communication Technologies. *Science, Technology, & Human Values* 29, 1 (Jan. 2004), 30–63. https://doi.org/10.1177/0162243903259190

[83] Xinru Page, Bart P. Knijnenburg, and Alfred Kobsa. 2013. What a Tangled Web We Weave: Lying Backfires in Location-Sharing Social Media. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*. 273–284.

[84] Charith Perera, Rajiv Ranjan, Lizhe Wang, Samee U Khan, and Albert Y Zomaya. 2015. Big data privacy in the internet of things era. *IT Professional* 17, 3 (2015), 32–39.

[85] Jennifer Pierre, Roderic Crooks, Morgan Currie, Britt Paris, and Irene Pasquetto. [n. d.]. Getting Ourselves Together: Data-centered participatory design research & epistemic burden. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2021-05-06) *(CHI '21)*. Association for Computing Machinery, 1–11. https://doi.org/10.1145/3411764.3445103

[86] Suvi Pihkala and Helena Karasti. 2016. Reflexive Engagement: Enacting Reflexivity in Design and for 'Participation in Plural'. In *Proceedings of the 14th Participatory Design Conference: Full Papers - Volume 1* (Aarhus, Denmark) *(PDC '16)*. Association for Computing Machinery, New York, NY, USA, 21–30. https://doi.org/10.1145/2940299.2940302

[87] Sarah Pink, Debora Lanzeni, and Heather Horst. 2018. Data anxieties: Finding trust in everyday digital mess. *Big Data & Society* 5, 1 (Jan. 2018), 2053951718756685. https://doi.org/10.1177/2053951718756685 Publisher: SAGE Publications Ltd.

[88] Kopo M. Ramokapane, Awais Rashid, and Jose M. Such. 2017. "I feel stupid I can't delete...": A Study of Users' Cloud Deletion Practices and Coping Strategies. In *Thirteenth Symposium on Usable Privacy and Security, SOUPS 2017, Santa Clara, CA, USA, July 12-14, 2017*. 241–256.

[89] Kopo M. Ramokapane, Gaurav Misra, Jose Such, and Sören Preibusch. 2021. Truth or Dare: Understanding and Predicting How Users Lie and Provide Untruthful Data Online. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY,

USA, Article 557, 15 pages. https://doi.org/10.1145/3411764.3445625
[90] Awais Rashid, Syed Asad Ali Naqvi, Rajiv Ramdhany, Matthew John Edwards, Ruzanna Chitchyan, and Muhammad Ali Babar. 2016. Discovering "unknown known" security requirements. In *Proceedings of the 38th International Conference on Software Engineering, ICSE 2016, Austin, TX, USA, May 14-22, 2016*. 866–876. https://doi.org/10.1145/2884781.2884785
[91] Karen Renaud and Lizzie Coles-Kemp. 2022. Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science* 3, 5 (2022), 1–14.
[92] Jesse C Ribot and Nancy Lee Peluso. 2003. A theory of access. *Rural sociology* 68, 2 (2003), 153–181.
[93] Ingrid Robeyns. 2001. An Unworkable Idea or a Promising Alternative? Sen's Capability Approach Re-examined. (05 2001).
[94] Ingrid Robeyns. 2003. SEN'S CAPABILITY APPROACH AND GENDER INEQUALITY: SELECTING RELEVANT CAPABILITIES. *Feminist Economics* 9, 2-3 (2003), 61–92. https://doi.org/10.1080/1354570022000078024 arXiv:https://doi.org/10.1080/1354570022000078024
[95] Minna Ruckenstein and Natasha Dow Schüll. 2017. The Datafication of Health. *Annual Review of Anthropology* 46, 1 (2017), 261–278. https://doi.org/10.1146/annurev-anthro-102116-041244 _eprint: https://doi.org/10.1146/annurev-anthro-102116-041244.
[96] Scott Ruoti, Jeff Andersen, Luke Dickinson, Scott Heidbrink, Tyler Monson, Mark O'neill, Ken Reese, Brad Spendlove, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. 2019. A Usability Study of Four Secure Email Tools Using Paired Participants. *ACM Trans. Priv. Secur.* 22, 2, Article 13 (April 2019), 33 pages. https://doi.org/10.1145/3313761
[97] Shruti Sannon, Natalya N. Bazarova, and Dan Cosley. 2018. Privacy Lies: Understanding How, When, and Why People Lie to Protect Their Privacy in Multiple Online Contexts. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.
[98] Angela Sasse. 2015. Scaring and Bullying People into Security Won't Work. *IEEE Security Privacy* 13, 3 (2015), 80–83. https://doi.org/10.1109/MSP.2015.65
[99] Ari Schlesinger, W. Keith Edwards, and Rebecca E. Grinter. 2017. *Intersectional HCI: Engaging Identity through Gender, Race, and Class.* Association for Computing Machinery, New York, NY, USA, 5412–5427. https://doi.org/10.1145/3025453.3025766
[100] Amartya Sen. 1979. *Equality of What? Tanner Lectures on Human Values, Volume 1.* Reprinted in John Rawls et al., Liberty, Equality and Law (Cambridge: Cambridge University Press, 1987).
[101] Amartya Sen. 1985. *Commodities and Capabilities.* North-Holland, Amsterdam. http://www.amazon.com/Commodities-Capabilities-Amartya-Sen/dp/0195650387/ref=sr_1_1?s=books&ie=UTF8&qid=1310679705&sr=1-1 New Delhi: Oxford University Press, 1987; Italian translation: Giuffre Editore, 1988; Japanese translation: Iwanami, 1988..
[102] Amartya Sen. 1991. Utility: ideas and terminology. *Economics & Philosophy* 7, 2 (1991), 277–283.
[103] Amartya Sen. 1992. The Political Economy of Targeting. Keynote Address In D. van de Walle and K. Nead, eds., Public Spending and the Poor (Washington, DC, World Bank 1995)..
[104] Amartya Sen. 1992. *The Quality of Life.* Clarendon Press, Oxford.
[105] Amartya Sen. 1993. *Capability and Well-Being.* Clarendon Press, Oxford.
[106] Amartya Sen. 1994. The Formulation of Rational Choice. *American Economic Review* 84, 2 (1994), 385–90.
[107] Amartya Sen. 2009. *The Idea Of Justice.* Penguin.
[108] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. [n. d.]. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA, 2018-05). IEEE, 409–423. https://doi.org/10.1109/SP.2018.00023
[109] L. Sion, K. Wuyts, K. Yskout, D. Van Landuyt, and W. Joosen. 2018. Interaction-Based Privacy Threat Elicitation. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 79–86. https://doi.org/10.1109/EuroSPW.2018.00017
[110] Daniel J. Solove. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (2006), 477–564. https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf
[111] Daniel J. Solove. 2021. The Myth of the Privacy Paradox. *George Washington Law Review* 89 (2021), 1.
[112] James K. Stewart and Robin Williams. 2005. *The Wrong Trousers? Beyond the Design Fallacy: Social Learning and the User.* SSRN Scholarly Paper ID 2176794. Social Science Research Network, Rochester, NY. http://papers.ssrn.com/abstract=2176794
[113] Lior Jacob Strahilevitz. 2013. Toward a Positive Theory of Privacy Law. *COASE-SANDOR Institute for Law and Economics Working Paper No. 637 Public Law and Legal Theory Working Paper NO. 421, University of Chicago* (2013).
[114] Lucy Suchman. 2002. Located accountabilities in technology production. *Scandinavian Journal of Information Systems* 14, 2 (Jan. 2002). https://aisel.aisnet.org/sjis/vol14/iss2/7
[115] Lucy Suchman. 2020. Algorithmic warfare and the reinvention of accuracy. *Critical Studies on Security* 0, 0 (May 2020), 1–13. https://doi.org/10.1080/21624887.2020.1760587 Publisher: Routledge _eprint: https://doi.org/10.1080/21624887.2020.1760587.
[116] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. Kelley, D. Kumar, D. McCoy, S. Meiklejohn, T. Ristenpart, and G. Stringhini. 2021. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *2021 2021 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 473–493. https://doi.org/10.1109/SP40001.2021.00028
[117] Dirk Van Der Linden, Pauline Anthonysamy, Bashar Nuseibeh, Thein Tan Tun, Marian Petre, Mark Levine, John N. Towse, and Awais Rashid. 2020. Schrödinger's Security: Opening the Box on App Developers' Security Rationale. In *ICSE '20: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*. Institute of Electrical and Electronics Engineers (IEEE), United States, 149–160. https://doi.org/10.1145/3377811.3380394 The 42nd International Conference on Software Engineering, ICSE 2020 ; Conference date: 23-05-2020 Through 29-05-2020.
[118] Dirk van der Linden, Irit Hadar, Matthew Edwards, and Awais Rashid. 2019. Data, data, everywhere: quantifying software developers' privacy attitudes.
[119] Bart van der Sloot. 2020. Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR*. Routledge. Num Pages: 21.
[120] Max Van Kleek, Dave Murray-Rust, Amy Guy, Daniel A. Smith, Kieron O'Hara, and Nigel R. Shadbolt. 2015. Self Curation, Social Partitioning, Escaping from Prejudice and Harassment: The Many Dimensions of Lying Online. In *Proceedings of the ACM Web Science Conference*. Association for Computing Machinery.
[121] Konstantina Vemou and Maria Karyda. [n. d.]. A Classification of Factors Influencing Low Adoption of PETs Among SNS Users. In *Trust, Privacy, and Security in Digital Business* (Berlin, Heidelberg, 2013) *(Lecture Notes in Computer Science)*, Steven Furnell, Costas Lambrinoudakis, and Javier Lopez (Eds.). Springer, 74–84. https://doi.org/10.1007/978-3-642-40343-9_7
[122] Yang Wang. 2018. Inclusive Security and Privacy. *IEEE Security Privacy* 16, 4 (2018), 82–87. https://doi.org/10.1109/MSP.2018.3111237
[123] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. 2022. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2344–2360.
[124] Sarah Myers West. 2019. Data capitalism: Redefining the logics of surveillance and privacy. *Business & society* 58, 1 (2019), 20–41.
[125] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, 1–17.
[126] Daniel W Woods and Aaron Ceross. 2021. Blessed Are The Lawyers, For They Shall Inherit Cybersecurity. In *New Security Paradigms Workshop*. 1–12.
[127] Shoshana Zuboff. 2019. *The age of surveillance capitalism: the fight for the future at the new frontier of power.* Profile Books, London.