REPHRAIN
Protecting citizens online

From Utility to Capability: A Manifesto for Equitable Security and Privacy for All

January, 19, 2023

Preamble

We live in a world where there is an increased push towards adoption of digital technologies in every walk of life – be it access to welfare services, financial services, healthcare, and/or migrants fleeing oppression/conflict. However, there is an inescapable reality — every individual is not equally disposed to engage with digital technologies. People differ in terms of their health, ability, education, economic situation, and/or can be in vulnerable situations, displaced from their homes and/or living under oppressive regimes. This lived reality negatively affects marginalised and/or vulnerable individuals in their ability to engage with digital systems and also to protect themselves from exploitation that data collection and aggregation can facilitate. Consequently, security and privacy has become a privilege with better protections available to individuals in better circumstances than others. The challenge of protecting all individuals in our increasingly digital societies is ever growing. The National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) organised the First Capability Approach Workshop for Protecting Citizens Online, 2022.

The workshop was attended by key members from academia in the UK. The workshop recognised the need for a new paradigm upon which protection mechanisms should be designed and engineered— and produced a manifesto. This manifesto represents

- an endeavour to highlight the criticality of opportunities and contexts of the individuals for whom digital protection mechanisms are being developed.
- a research agenda for the scientific community.

This manifesto is founded upon the recognition that safer Internet is a public good and everyone should have access to protection mechanisms on the Internet. The members of the workshop invite the research community and every stakeholder involved in protecting citizens online, to positively engage with the manifesto.

Signatories

Dr. Partha Das Chowdhury
University of Bristol

Professor Lizzie Coles-Kemp
Royal Holloway University London

Dr. Karolina Follis
Lancaster University

Dr. Sanja Milivojevic
Bristol Digital Futures Institute

Professor Awais Rashid
University of Bristol

Professor Genevieve Liveley
University of Bristol

Dr. Gina Netto
Heriot Watt University

Dr. Andres Dominguez
University of Bristol

Professor Ross Anderson
University of Cambridge
University of Edinburgh

Lee, C4
National Cyber Security Center

Dr. Kopo Marvin Ramokapane
University of Bristol

Dr. Ola Michalec
University of Bristol

Introduction

As researchers and practitioners we have a moral obligation to design and develop protection mechanisms for everyone irrespective of their personal, social, economic and political realities [24]. Socio-economically disadvantaged groups and individuals in vulnerable situations often find it difficult to make use of technologies to their advantage and rather end up being victims of pervasive digital push [19]. The usable security community has made a strong case for putting *humans* at the heart of systems design [1,10]. However, the notion of *utility* implicit in usability [22] is not enough to capture human needs in their diverse personal situations and environmental context. In this research manifesto we propose the adoption of *capability approach* [26] as a foundation to develop protection mechanisms [8] for citizens in a digital first society.

Capability Approach Amartya Sen proposed *capability approach* [26] as i) a framework of thought ii) a critique to other approaches of welfare evaluation and iii) a formula to make interpersonal comparison [28]. *Capability approach* explicitly recognises individuals in their beings and doings: i.e. active individuals who would want to live a life they can and have a reason to value. The fundamental primitives of *capability approach* are active individuals who would want to live a life they can and have a reason to value. The fundamental primitives of *capability approach* are

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

Functionings are more related to living conditions, whereas capabilities denote the ability to achieve a particular functioning. For example a safety tool can be viewed as a good or service to enable a functioning of having safe interactions online. Merely possessing the safety tool only will not enable the functioning. What is needed is to have the skill, education, physical ability, and social and political environment to use the tool. Functionings can be viewed as achievements while capability is the freedom to achieve something.

Manifesto

Policy makers should assess deliberate influences to freedom

While understanding of diverse deprivations and environmental realities is important— it is not enough. A critical conversion factor is dependent on what the politically powerful forces are willing to drive and/or concede. The availability and use of public goods (we consider safer Internet as a public good) has not been proportionate across diverse strata of society [27]. In a telling judgement on Capacity: Social Media: Care and Contact, a Judge in England and Wales noted the exclusion that disabled users of social media suffer [33]. More needs to be done for appropriate liability in tech policy and regulation [3]. The field of surveillance studies has reasoned how commercial and political interests engender ethical tensions [6, 17]. Regulations can play a critical role as crime shifts online from the physical world [4]. Policy formulation based on *capability approach* would therefore require a thorough understanding of the deliberate influences upon individual freedom in different contexts.

Approaching capability through ethos

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 [21]. This highlights the need to address this reluctance going beyond utility propositions on the surface of the protection mechanisms. *Capability approach* foregrounds the plural formulations of individual well- being as integral to its effectiveness. A deeper inspection would reveal that individuals do not always act to appropriate a utility function [29]. For protection mechanisms to cater to diverse customs and habits, researchers and practitioners need to step into the shoes of those whose very security and safety they aim to ensure. Adoption of *capability approach* can start by exploring the extent to which it can adopt the work on user personas [15] and expand this to help narrate customs, habits, through stories [16]. Systems engineering in turn can design end points and controls to reflect user contexts and diversity.

Democratic participation to evolve a list of basic minimum online protections

A key finding from various studies is the absence of basic protections against various online harms [34]. If we unpack this we can better see the diverse needs of individuals – a clear departure from the often monolithic security assumptions and policies based on antecedent uniformity. A particular example might be of whistle-blowers in particular contexts or journalists in other contexts [11, 30]. *Capability approach* advocates for the need to define basic capabilities — which means the ability to achieve some basic functionings. Sen explicitly advocates for evolving a list of capabilities in particular contexts to accommodate diverse realities and requirements. An example of a basic capability might be protection from threats of surveillance while accessing welfare services online [13].

A reasoned understanding of the winners and losers

Security is not an absolute property — different entities participating (directly or indirectly) in a system have different trust assumptions and security expectations from the same system [9]. Precedence of one set of expectations over another hinders adoption, potentially manifesting into reticence, lying and/or resignation [23, 35, 18]. When one set of security goals and assumptions are pushed across different participants then it creates winners and losers. For example, absence of disclosures leads to discrimination against ethnic minorities while graded disclosures hurt applicants with less serious offences while benefiting applicants with more serious convictions. The tension scales across to the employers as well in this example of disclosures [32]. We invite the wider community to explore the extent to which *capability approach* can be used for inter-personal comparisons of welfare for effective understanding of the winners and losers.

Individuals should value participating in the online community

We build systems for humans — requiring humans to adhere to practices against their will have consistently proved to be counterproductive. People do not have incentives to engage in behaviour they do not have a reason to value [3]. Burdening individuals with disproportionate cognitive loads is not good for security either [7, 12]. Evidence from health care contexts shows a negative adoption pattern can be directly related to cumbersome compliance practices [20]. There should be positive efforts to understand why systems fail in practice rather than in theory [5]. We propose to encourage challenging 'best practices' where it does not work for particular social groups. *Capability approach* inherently highlights the conversion factors particular to diverse individuals – this can encourage calibrating compliance practices to recognise the diversity.

Steps towards Adoption of Capability Approach

Capability Approach places explicit emphasis on opportunity rather than outcome. The discussions in the workshop also reflected on methods to adequately reflect the opportunities. Focus group and interviews are highly productive to elicit the observed diversities among individuals. However, they need to be complemented with methods that can also elicit the unobserved diversities, including marginalisation and wider environmental realities. We advocate that practicing reflexivity in the design of participatory practices would positively contribute towards adoption of *capability approach*. This can be complemented with ethnographic studies [2] to understand the beings and doings of individuals and intersectionality [25] to understand the integrated identities of individuals across race, gender and other contexts. The steps we propose in this manifesto are for exposition and not a definitive list— we aim for more inclusivity in the spheres of design and inter-disciplinary research as a means to develop better interventions.

[References

1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun*. ACM, 42(12):40–46, 1999.

[2] Martin Albrecht, Jorge Blasco Alis, Rikke Bjerg Jensen, and Lenka Marekova. Collective information security in large-scale urban protests: the case of Hong Kong. *In Proceedings of the 30th USENIX Security Symposium*. USENIX, August 2021.

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

[4] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. *Measuring the Cost of Cybercrime*, pages 265–300. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[5] Ross J. Anderson. Why cryptosystems fail. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*, pages 215–227. ACM, 1993.

[6] Mark Andrejevic and Kelly Gates. Big Data Surveillance: Introduction. *Surveillance & Society*, 12(2):185–196, May 2014.

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

[8] Partha Das Chowdhury, Andrés Domínguez Hernández, Marvin Ramokapane, and Awais Rashid. From utility to capability: A new paradigm to conceptualize and develop inclusive pets. In *New Security Paradigms Workshop*. Association for Computing Machinery (ACM), 2022.

[9] Bruce Christianson. Living in an impossible world. *Philosophy and Technology*, 26(4):411–429, January 2013.

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

[11] Ksenia Ermoshina, H. Halpin, and F. Musiani. *Can Johnny Build a Protocol?* Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols.

[12] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-Scale Readability Analysis of Privacy Policies. In *Proceedings of the International Conference on Web Intelligence*, Leipzig, Germany, August 23-26, 2017, pages 18–25. ACM, 2017.

[13] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. 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, CSCW '17, page 1800–1811, New York, NY, USA, 2017*. Association for Computing Machinery.

[14] Nick Gill, Jennifer Allsopp, Andrew Burridge, Daniel Fisher, Melanie Griffiths, Natalia Paszkiewicz, and Rebecca Rotter. The tribunal atmosphere: On qualitative barriers to access to justice. *Geoforum*, 119:61–71, 2021.

[15] Makayla M Lewis and Lizzie Coles-Kemp. 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*, pages 2485–2490. 2014.

[16] Genevieve Liveley. *Stories of Cyber Security Combined Report*, (last accessed July 6, 2022).

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

[18] Ivan Manokha. Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, 16(2):219–237, July 2018.

[19] Nora McDonald, Karla Badillo-Urquiola, Morgan G Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J Wisniewski. 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*, pages 1–8, 2020.

[20] Amalia R. Miller and Catherine E. Tucker. Electronic Discovery and the Adoption of Information Technology. *The Journal of Law, Economics, and Organization*, 30(2):217–243, 11 2012.

[21] National Cyber Security Center, UK. Anuual Review 2020 – Making the UK the safest place to live and work online). https://www.ncsc.gov.uk/news/annual-review-2020.

[22] Ilse Oosterlaken. Design for Development: A Capability Approach. *Design Issues*, 25(4):91–102, 10 2009.

[23] Kopo M. Ramokapane, Awais Rashid, and Jose M. Such. "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., pages 241–256, July 2017.

[24] Phillip Rogaway. The moral character of cryptographic work. *Cryptology* ePrint Archive, 2015.

[25] Ari Schlesinger, W. Keith Edwards, and Rebecca E. Grinter. *Intersectional HCI: Engaging Identity through Gender, Race, and Class*, page 5412–5427. Association for Computing Machinery, New York, NY, USA, 2017.

[26] Amartya Sen. *Equality of What? Tanner Lectures on Human Values*, Volume 1. 1979. Reprinted in John Rawls et al., Liberty, Equality and Law (Cambridge: Cambridge University Press, 1987).

[27] Amartya Sen. The political economy of targeting, 1992. Keynote Address In D. van de Walle and K. Nead, eds., Public Spending and the Poor (Washington, DC, World Bank 1995).

[28] Amartya Sen. *Capability and Well-Being*. Clarendon Press, Oxford, 1993.

[29] Amartya Sen. The formulation of rational choice. *American Economic Review*, 84(2):385–90, 1994.

[30] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the united states. In 2018 IEEE Symposium on Security and Privacy (SP), pages 409–423. IEEE.

[31] Daniel J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477–564, 2006.

[32] Lior Jacob Strahilevitz. 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.

[33] THE HONOURABLE MR JUSTICE COBB. Re B (Capacity: Social Media: Care and Contact). https: //www.bailii.org/ew/cases/EWCOP/2019/3.

[34] 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. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In 2021 2021 *IEEE Symposium on Security and Privacy* (SP), pages 473–493, Los Alamitos, CA, USA, may 2021. IEEE Computer Society.

[35] Iman Vakilinia and Shamik Sengupta. A coalitional cyber-insurance framework for a common platform. *IEEE Transactions on Information Forensics and Security*, 14(6):1526–1538, 2019.