Google | Privacy, Safety & Security

Privacy for All: Achieving Inclusive Privacy in the Digital Age

Sri Maddipati, Norbert Nthala

July 3, 2023

1. Introduction

Sri Maddipati
Senior Privacy Engineer
Google LLC

Norbert Nthala
Privacy Engineer
Google LLC

Agenda

1. Introduction
2. Why Inclusive Privacy
3. Challenges to Inclusive Privacy
4. Opportunities for Inclusive Privacy
5. Case Study
6. Conclusion

2. Why Inclusive Privacy

- Privacy is a fundamental human right
    - It is grounded on people's interest in having a reasonable measure of control over ways in which they present themselves (and what is theirs) to others [1].

- However, mainstream privacy mechanisms often do not consider the wide variety of users [2] and are not inclusive of various characteristics, abilities, needs and values.

- *Inclusive Privacy* ensures that privacy mechanisms are built around people's varying characteristics, identities, abilities, needs, and values.

[1] Marmor, Andrei. "What is the Right to Privacy?." *Philosophy & Public Affairs* 43.1 (2015): 3-26.
[2] Wang, Yang. "Inclusive security and privacy." IEEE Security & Privacy 16.4 (2018): 82-87.

3. Challenges to Inclusive Privacy

- Awareness and Knowledge Gap
- The Digital Divide
- Algorithmic Bias and Discrimination

3. Awareness and Knowledge Gap

- Evidence indicates that most people have limited understanding of privacy threats, risks, mechanisms / tools, and rights [1].

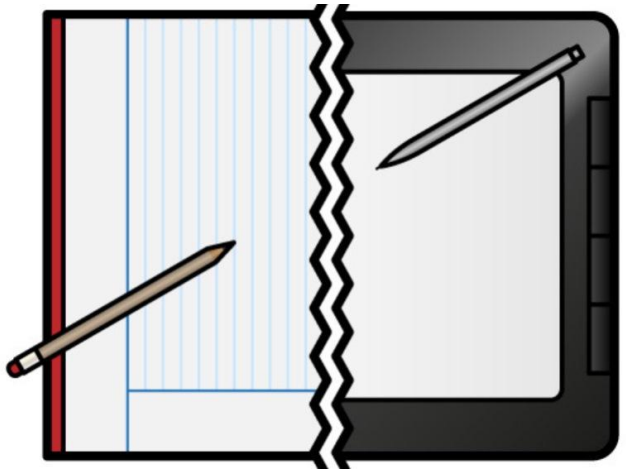
- As a result, people consent to sharing data with limited or no understanding of the range of data that is collected or can be inferred, and potential privacy implications thereof [2].
  - And hence, the Privacy Paradox!

[1] Gerber, Nina, Benjamin Reinheimer, and Melanie Volkamer. "Home sweet home? Investigating users' awareness of smart home privacy threats." Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP). 2018.
[2] Klasnja, Predrag, et al. "Exploring privacy concerns about personal sensing." Pervasive Computing: 7th International Conference

3. The Digital Divide

- Socioeconomic disparities, lack of infrastructure, and limited digital literacy can hinder marginalized communities' ability to engage fully in the digital realm and protect their privacy

- Low self-efficacy in technology and privacy management = poor privacy practices.



3. Algorithmic Bias and Discrimination

- AI technologies have been shown to perpetuate discrimination in housing[1], financial lending, hiring processes and more.

- Marginalized communities may experience disparate impacts in data collection, profiling, and algorithmic decision-making processes.
    - E.g., [2] found that ads for arrest records are significantly more likely to show up on searches for distinctively black names.

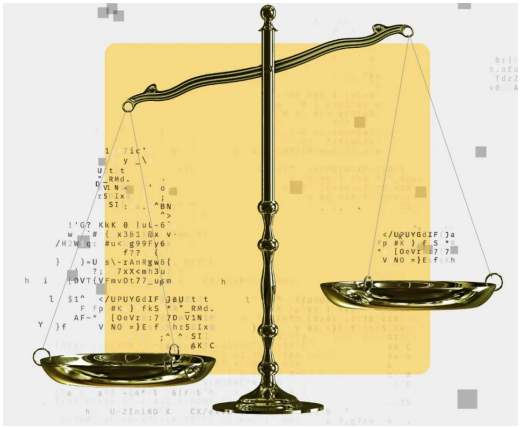


Image from vox.com

1. Sisson, P. "Housing discrimination goes high tech." (2019).
2. Sweeney, Latanya. "Discrimination in online ad delivery." *Communications of the ACM* 56.5 (2013): 44-54.

4. Opportunities for Inclusive Privacy

- Empower Users
- Design for Diversity
- Address Algorithmic Bias

4. Empower Users

- Privacy involves individual decisions and multi-stakeholder actions.
    - All users face privacy risks, but some users face circumstances that expose them to outsized risks.
- Individuals should have the knowledge, tools, and agency to make informed decisions about their privacy.
- How can we empower users to manage their privacy and assert their rights?
    - By promoting digital literacy
    - Through accessible privacy settings
    - Through user-friendly interfaces

4. Design for Diversity

- “Almost everyone is a minority of one kind”.
- Privacy features and technologies should be inclusive by design.
- How can we design for diversity?
    - Conduct user research to identify and understand various attributes and needs of target users and bystanders.
    - Practice inclusive design.
    - Through comprehensive accessibility standards.

4. Address Algorithmic Bias

- Recognizing the biases and discriminatory outcomes of algorithms is vital to achieving inclusive privacy.
- How can we mitigate privacy harms from algorithmic biases?
    - Strive for fairness, transparency, and accountability in algorithmic decision-making.
    - Identify and mitigate potential sources of bias (e.g., data inputs and algorithm)

5. Case Analysis - Refugees Privacy

- Refugees rely on digital platforms and communication tools to connect with their families, access important information, and seek support [1].
- What is the Risk?
    - Most refugees have limited understanding privacy threats, risks, and countermeasures, hence exposing themselves to online privacy harms (e.g., surveillance).
    - Despite recognizing the importance of online privacy, refugees feel powerless to protect themselves online [2].
    - In addition, refugees trust their case managers with more sensitive information and personal assets than expected [1].

[1] Simko, Lucy, et al. "Computer security and privacy for refugees in the United States." *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018.
[2] Martin, Aaron. "Connecting with confidence: managing digital risks to refugee connectivity." UNHCR. (2021).

5. Case Analysis *Cont'd*

- How did UNHCR improve online privacy practices of refugees? [1]
  - Implemented a comprehensive data protection policy to safeguard the privacy and personal information of refugees.
  - Provided digital privacy workshops for refugees on digital security practices, including
    - Secure communication
    - Safe browsing, and
    - Protecting personal information online.

Empower users!

[1] Martin, Aaron. "Connecting with confidence: managing digital risks to refugee connectivity." UNHCR. (2021).

6. Conclusion

- Currently there are no industry standards for Inclusive privacy design.
- Implementing inclusive privacy requires collective action from various stakeholders.

  Where to start ?
  - Lay out foundational principles for designing privacy for diverse user groups.
  - Invest in Inclusive research which can identify areas to maximize the focus on inclusion.
  - Integrate privacy inclusion into product testing programs.
  - Outline an approach to seek user feedback on inclusivity and act upon it.

Thank you

Q&A