Inclusive Privacy

CS 7375: Seminar: Human-Centered Privacy Design and Systems (co-located with PHIL 5110)

Tianshi Li | Assistant Professor

Agenda

- What is “inclusive privacy” and why do we need to study it?
- Accessibility and Privacy
- Marginalized/Vulnerable populations and privacy

How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)

- WEIRD = Western, Educated, Industrialized, Rich, and Democratic
- Research studies that primarily rely on "WEIRD" participants pose a common challenge to the generalizability of findings.

Hasegawa, Ayako A., Daisuke Inoue, and Mitsuaki Akiyama. "How WEIRD is Usable Privacy and Security Research?." 33rd USENIX Security Symposium. 2024.

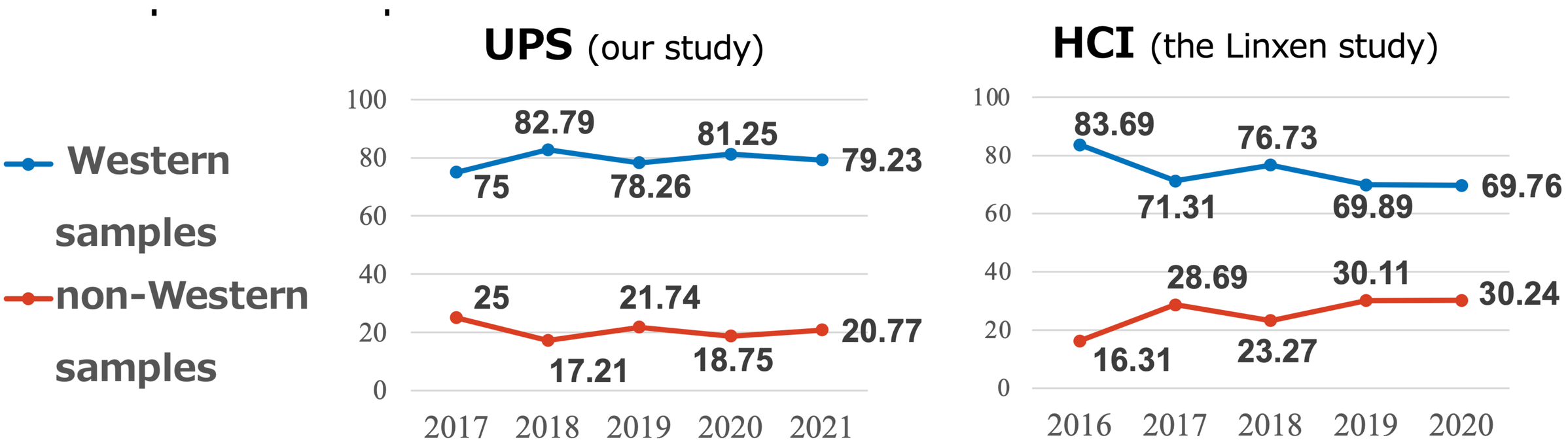
How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)

- Psychology
  - Henrich et al. (2010) : The majority of participants have been reported to be Western, Educated, Industrialized, Rich, and Democratic (WEIRD) population.
- Human-Computer Interaction (HCI)
  - Linxen et al. (2021) : “How WEIRD is CHI?” confirming the WEIRD skew of participant samples.
- This study: “How WEIRD is Usable Privacy and Security (UPS) Research?”
  - quasi-replication of the Linxen study for UPS

How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)



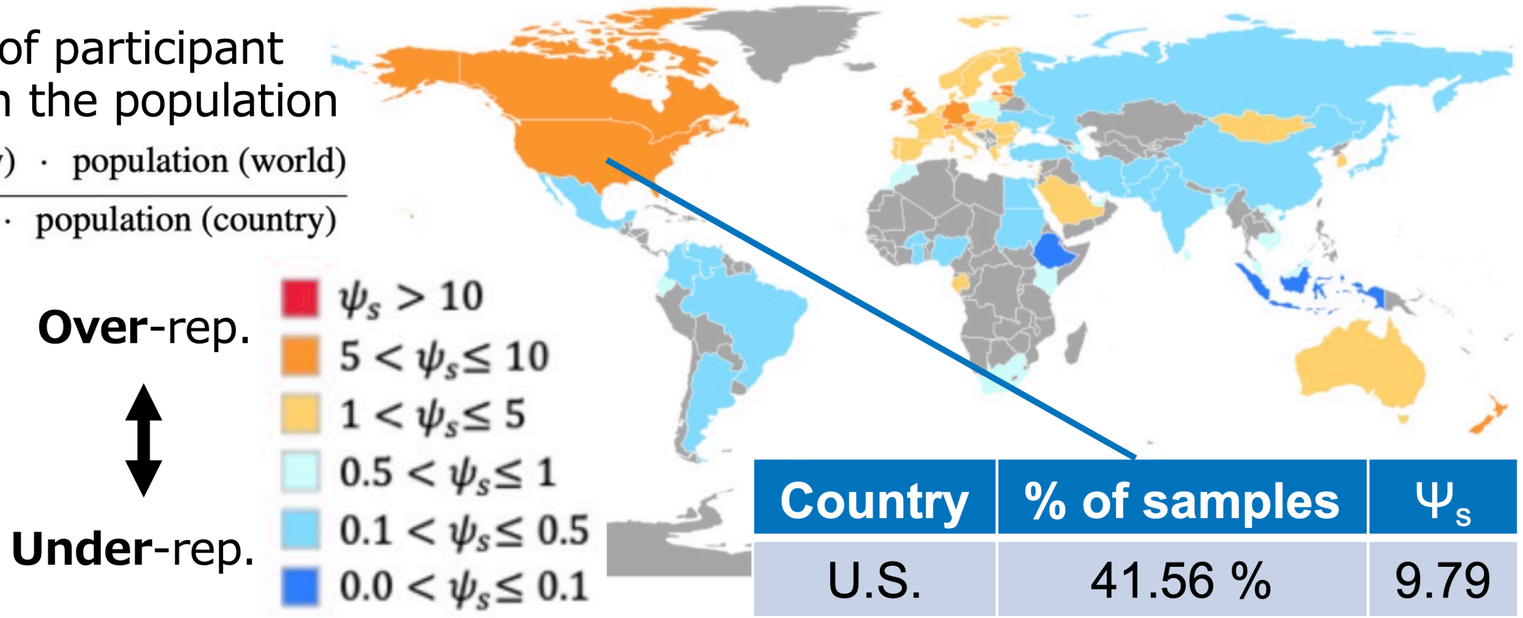
Hasegawa, Ayako A., Daisuke Inoue, and Mitsuaki Akiyama. "How WEIRD is Usable Privacy and Security Research?." 33rd USENIX Security Symposium. 2024.

How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)

Normalized ratio of participant samples based on the population

$$\psi_s = \frac{n_{samples}\ (\text{country}) \cdot \text{population (world)}}{n_{samples}\ (\text{total}) \cdot \text{population (country)}}$$



Country	% of samples	Ψ_s
U.S.	41.56 %	9.79

Under-represented or marginalized:
Africa, South America, the Middle East, and Asia

How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)

- From national stats.:
  Most participant samples come from countries with generally highly educated populations, industrialized (high GDP), rich (high GNI), and democratic (high political-right index).
- From self-reported data:
  Majority of participants (71%) had a college-level or higher education.
- Reasons of the skew toward highly educated participants
  - Recruitment within the authors' institution (e.g., university)
  - Recruitment through crowdsourcing (Workers are generally highly educated.)

Hasegawa, Ayako A., Daisuke Inoue, and Mitsuaki Akiyama. "How WEIRD is Usable Privacy and Security Research?." 33rd USENIX Security Symposium. 2024.

How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)

		% W-only samples
Participant type	**Non-experts**	85.38% (**Western-skewed**)
	Experts (excluding developers)	88.57% (**Western-skewed**)
	Experts (developers)	66.67% (**Relatively diverse**)
User study type	**Feasibility of cyber attack** User study only for demonstrating the feasibility of the proposed attack (e.g., keystroke inference)	92.31% (**Western-skewed**)

How WEIRD is Usable Privacy and Security Research?

(Hasegawa et al. USENIX Security 2024)

- The UPS research does not naturally represent or benefit all users.
- Gaps between WEIRD and non-WEIRD populations: Misconceptions, privacy preferences, susceptibility to phishing, IT resource usage, security documentation, privacy laws, ...

Hasegawa, Ayako A., Daisuke Inoue, and Mitsuaki Akiyama. "How WEIRD is Usable Privacy and Security Research?." 33rd USENIX Security Symposium. 2024.

“The third wave in privacy research”

(Wang 2017)

First wave

Second wave

Third wave

Wang, Yang. "The third wave? Inclusive privacy and security." Proceedings of the 2017 new security paradigms workshop. 2017.

Inclusive Security and Privacy

(Wang 2017)

- Inclusive security and privacy designs must be inclusive of different human abilities, characteristics, values, and needs

	Population
Disability	disability in general [11], visual [6, 7, 9, 102], cognitive [26, 60, 81], motor [48, 66]
Non-western/developing countries	Middle East [2–4, 31], Africa [74], India [49, 51, 64, 95], China [95]
Other under-served populations	older adults [20, 59], LGBT [14], children [2, 17, 27, 63, 88, 91, 93, 103], veterans [78], migrants [2, 75], refugees [75]

Table 1: Privacy of under-served populations

Wang, Yang. "The third wave? Inclusive privacy and security." Proceedings of the 2017 new security paradigms workshop. 2017.

Accessibility and Privacy

Privacy challenges related to people's abilities/disabilities

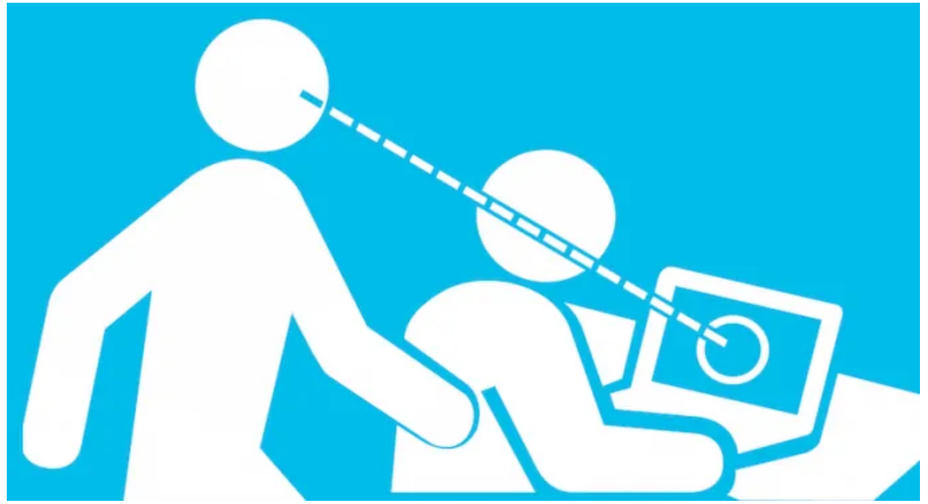
Ability assumptions

- All human-operated technologies contain embedded “ability assumptions,” whether explicit or implicit
- Consider a touch screen
- What are the assumed abilities?
- Consider situational impairments

Adapted from https://courses.cs.washington.edu/courses/cse510/16wi/slides/14-AbilityBasedDesign.pdf

Ability assumptions for S&P tasks

- How can you protect yourself from shoulder surfing?
- What are the assumed abilities?



Privacy Concerns and Behaviors of Visual Impaired People

Physical privacy concerns

- Lack of independence: Visually-impaired people often need help from others, including strangers.
  - Lack of accessibility, Finding items, navigation and transportation
- Eavesdropping (visually or aurally)
  - low-vision users use large fonts; Concerns about the use of screenreader
- Security of computing devices (password management)
- Technical support

Ahmed, Tousif, et al. "Privacy concerns and behaviors of people with visual impairments." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2015.

Privacy Concerns and Behaviors of Visual Impaired People

Privacy concerns with virtual interaction

- Online transactions
- Social media privacy
  - Complex privacy settings
  - Unintentionally sharing embarrassing or sensitive images

Ahmed, Tousif, et al. "Privacy concerns and behaviors of people with visual impairments." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2015.

Privacy Concerns and Behaviors of Visual Impaired People

Privacy-enhancing behaviors

- Requesting help from acquaintances
- Try to be alone; do not engage in personal activities in the public
- Use head phones to prevent aural eavesdropping; but this carries other privacy and safety risks
- Use caution with passwords

Ahmed, Tousif, et al. "Privacy concerns and behaviors of people with visual impairments." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2015.

Universal design

- The design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design.

- For example, a building ramp can be used by different people and it will benefit those with and without wheelchairs (e.g., when people have strollers or luggage)

Ability-based design

- Two core principles of ability-based design:
  - **Ability:** Shift the focus **from people's disabilities to their abilities**
  - **Accountability:** Designers will respond to poor performance by **changing systems, not users**, leaving users as they are.

Wobbrock, Jacob O., et al. "Ability-based design: Concept, principles and examples." ACM Transactions on Accessible Computing (TACCESS) 3.3 (2011): 1-27.

Ability-based design vs. Universal design

Ability-based design

- Focus on abilities of a user
- Focus on what one person can do
- $\lim_{n \to \infty}$ Design for one
- Runtime adaptation
- Sense, model, adapt
- Usually dynamic

Universal design

- Focus on accessibility of environment
- Focus on what most people can do
- $\lim_{n \to \infty}$ Design for all
- Design-time accommodation
- Understand, design, test, deploy
- Usually fixed

Adapted from https://courses.cs.washington.edu/courses/cse510/16wi/slides/14-AbilityBasedDesign.pdf

- How can ability-based design and/or universal design help address these issues?
- How do new interaction devices or technologies present new security/privacy attack surfaces or opportunities for mitigation?

Marginalized/ Vulnerable populations and privacy

What do we mean by marginalization?

- Marginalized populations are defined as persons who are peripheralized based on their identities, associations, experiences and environments. As a result, these groups are excluded from mainstream social, economic, cultural, or political life.

- People can be marginalized based on several factors, including race, disability, gender identity, sexual orientation, socioeconomic status, and immigration status.

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

What do we mean by vulnerable populations?

- Vulnerable populations are those whose race class, gender, or sexual identity, and other intersectional characteristics or circumstances put them at **particular risks** in the society at large.

- Vulnerable populations include, but are not limited to, survivors of domestic abuse, those living in poverty or within child welfare systems, immigrants, those with HIV, LGBTQ, as well as he very young, and very old.

- Emphasis on the structural inequalities (i.e., **power**) that make some individuals more susceptible to privacy violations

McDonald, Nora, et al. "Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations." Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. 2020.

Networked Privacy

- Our interactions are connected. Privacy matters are not just for the individual but also the collective
- When parents choose to blog about their lives with their children, they are not only sharing personal information but also creating a lasting and potentially embarrassing record of their children's experiences.
- In the area of online safety for teens, current technology design focuses on parental control, introducing power imbalances between teens and parents regarding privacy, safety, and autonomy.

Boyd, Danah. "Networked privacy." Surveillance & society 10.3/4 (2012): 348.

McDonald, Nora, et al. "Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations." Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. 2020.

Privacy research about marginalization

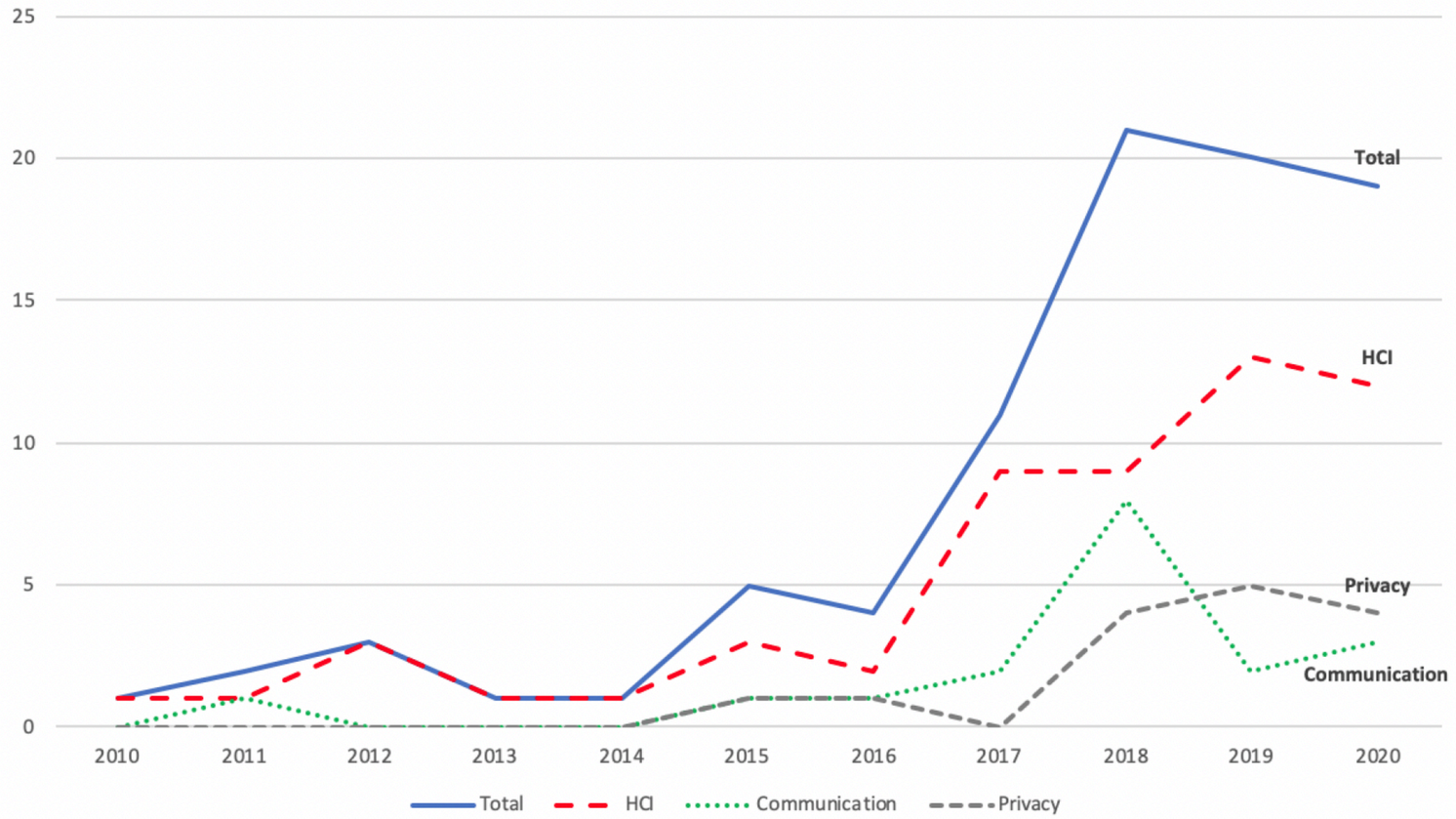
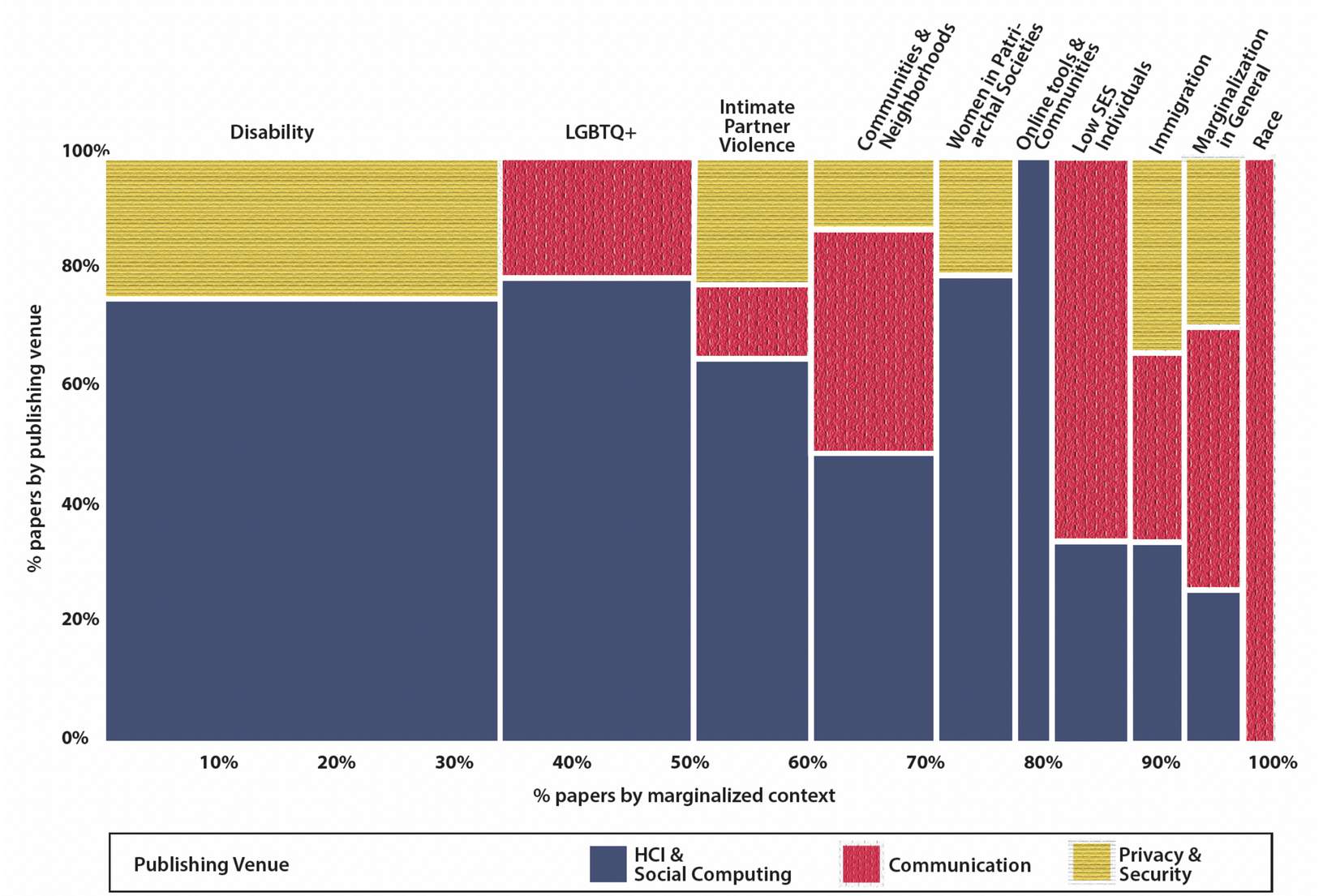


Fig. 2. Publication counts from 2010 to 2020 in HCI, Communication, Privacy-focused venues, as well as the total number of papers across venues over time

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

Privacy research about marginalization



Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

Why studying privacy and marginalization?

Disproportionate risks and challenges

- Identity-related goal lead to elevated privacy risks
- Ramifications of privacy violations: Consider the case of a person living with HIV, who may risk social stigma, discrimination, or the dissolution of relationships should their HIV status become publicly known without their consent, as compared to the impact of a health information leak for a person who does not have to navigate a marginalized and often stigmatized identity.
- Disparities in digital literacy, skills, technological access, as well as linguistic and cultural barriers

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

Why studying privacy and marginalization?

Technological and societal exclusion

- Technologies are often designed without consideration for the needs of marginalized groups
- Structural challenges that are not always tied to technology

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

PETs and marginalization

- Define the vulnerability disparity (VD) of membership inference attack (MIA) as:

$$VD = P(\hat{Y} = 1|Y = 1, A = a) - P(\hat{Y} = 1|Y = 1, A = \bar{a}),$$

- Intuitively, VD describes the difference of the success probability of MIA for the protected group versus the unprotected group.

- DP cannot eliminate VD completely on both gender and race attributes. There is no consistent pattern of how VD changes by DP deployment.

Zhang, Bo, et al. "Privacy for all: Demystify vulnerability disparity of differential privacy against membership inference attack." arXiv preprint arXiv:2001.08855 (2020).

Privacy Responses and Costs Framework

Privacy Response	Cost/Consequence	Select Examples from the Dataset
Apathy i.e. lack of response	• Exposure to risks	Undocumented immigrants felt government surveillance is inescapable, leading to inaction [45]; women transitioning from incarceration felt they have "nothing to lose" [105].
Non-use e.g. not using a technology, deleting an account	• Opportunity loss • Exclusion • Silencing • Isolation	Economically disadvantaged populations lose opportunities due to non-use of technologies [110].
Withholding disclosure e.g. self-censorship, information removal	• Restricts self-expression • Silencing	Low-SES youth [74], marginalized Cambodians [58], and political refugees in the U.S. [107] self-censored to avoid conflict and danger but were further silenced by doing so. Men who have sex with men may not disclose HIV status on dating apps but can inadvertently signal positive status [116].
Controlling disclosure e.g. compartmentalizing identity, multiple accounts, privacy controls, segmenting audiences	• Restricts self-expression • Labor-intensive • Social cost • Financial cost	Trans men crowdfunding top surgery used privacy controls to limit audiences [39], young Azerbaijanis maintained multiple accounts for political activism [90], and LGBTQ+ social media users managed identities across platforms [24]. Disclosure controls require extensive labor and restrict self-expression [8]. Complex privacy controls can be costly to access [95] and can be used incorrectly due to accessibility issues [3].
Privacy lies [102] i.e. providing false information	• Cognitive burden • Social/legal repercussions	Rural Appalachians provided false information as a form of vigilanteism [49]; South Asian women provided false information to protect themselves from online abuse [99].

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

Privacy Responses and Costs Framework

Privacy Response	Cost/Consequence	Select Examples from the Dataset
Privacy-enhancing technologies (PETS) e.g., authentication, cloaking, encryption	• Social liability • Erasure of records	Women in patriarchal societies used private modes and locks on devices, which may be seen as incriminating and invite coercion to obtain access [100]. People who are financially insecure who lose access to trusted devices lose access to services that require two-factor authentication [108].
Physical workarounds e.g. hiding device, use of camera covers & headphones	• Limits environmental awareness • Vulnerable to physical coercion	People with visual impairments used headphones to avoid aural eavesdropping when using screen readers at the cost of physical safety [3].
Asking for help e.g. learning new practices, consulting network, websites, professionals	• Bad information • Involves risk/trust • Limited to help available	Professionals who provide support for survivors of intimate partner violence did not feel equipped to advise on identifying or coping with technology-enabled IPV [38]. People with visual impairments asked allies for help, but this risked trusting the ally with personal information [52].
Collaborative privacy practices e.g. shared guidelines, boundaries	• Loss of autonomy • Involves risk/trust	LGBTQ+ adults considered not only their own privacy boundaries but also those of their families, ex-partners, and children [8]. Families co-developed privacy guidelines for shared devices in Bangladesh [2].
Third-party protections e.g. parents removing devices, organizations destroying info	• Loss of autonomy • Outside of the person's control	Art therapists removed identifying information from art created by persons with dementia to protect their privacy, but this also removed their voice [19]. Canadian government's legal decision to destroy data documenting colonial abuses of indigenous people to protect their personal privacy also erased evidence of their abuse [40].

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

Privacy-related tensions for marginalized users

- Privacy vs. disclosure of identity
- Privacy vs. support
- Privacy vs. autonomy
- Individual vs. collective

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

Recommendations from prior research

- Prioritizing autonomy and dignity in design
- Recognizing the influence of power relations on technology use
- Providing greater control over information (e.g., granular privacy settings)
- Facilitating management of communal and networked aspects of privacy
- Making privacy decisions easier
- Building in technical safeguards
- Providing people with education and resources

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." Proceedings of the ACM on Human-Computer Interaction 6.CSCW2 (2022): 1-33.

- Reflecting on your research or course project, how does the perspective of inclusive privacy give you something new to think about?

- What new research methods, paradigms, or techniques do we need in response to inclusive privacy as the third wave of S&P research?