





# Inclusive Privacy and Security

**Apu Kapadia**  | Indiana University Bloomington  
**Yang Wang**  | University of Illinois at Urbana-Champaign

**This special issue features six articles on addressing the privacy and security needs of diverse populations. These articles provide insights into design guidelines, techniques, and specific populations for building technologies for inclusive privacy and security.**

**T**his special issue on “Inclusive Privacy and Security” aims to cover the state-of-the-art knowledge and outline future directions of inclusive privacy and security, a vision where privacy and security policies, mechanisms, or tools can support a wide range of users, including those who are vulnerable, marginalized, or at-risk.

Although mechanisms for computer security and privacy can offer a degree of protection to everyone, certain groups may encounter distinct and heightened challenges related to their privacy and security. These groups might face specific barriers when trying to address these concerns, and their unique needs and concerns may not be widely recognized outside of their communities. For example, consider the barriers a low-vision or blind person might face when presented with a typical CAPTCHA that scrambles letters on the screen and assumes visual acuity. Security cameras, which can improve security and safety, can also be used for intimate partner surveillance in the home. Older adults and children might also be particularly vulnerable to online scams. Over the past decade, the security and privacy community has made strides in addressing such challenges and has begun to systematize the needs of diverse populations.

We clearly remember when we started studying underserved populations. Wang’s first foray into this area was an attempt to make authentication more accessible to people with visual impairments.<sup>1</sup> This project was an eye-opener for Wang, and he later realized that the (usable) privacy and security community had not paid much attention to a wide range of underserved populations, including people with disabilities. He then started giving talks about this topic, using the term *inclusive privacy and security*, advocating for more research.

Kapadia first started studying low-vision and blind populations in the early 2000s when approached by his Ph.D. student, Tousif Ahmed. He wanted to study how wearable cameras could help these populations assess the surrounding physical environment for security and privacy threats. Despite our initial trepidation about trying to publish on a topic outside the mainstream, we concluded that this research was simply too important. Not able to find any comprehensive work on the needs of low-vision and blind users in this context, our first work in this area focused on an interview-based study to uncover the “Privacy Concerns and Behaviors of People with Visual Impairments.”<sup>2</sup> Soon after publishing this work, Kapadia attended Wang’s talk on inclusive privacy and security, and was excited and inspired to see how Wang was helping to build a community around a broader agenda to address the needs of diverse

Digital Object Identifier 10.1109/MSEC.2024.3433708  
Date of current version: 13 September 2024

populations. This community was developed through the annual workshop series on inclusive privacy and security, co-located with The Symposium on Usable Privacy and Security (SOUPS). This year marks the ninth edition of the workshop, which has grown into a vibrant community of scholars, practitioners, and policymakers around the world.

We are excited to publish six articles on addressing the privacy and security needs of diverse populations. The first two articles concern overarching guidelines for inclusive design. The first article, by Sharevski,<sup>A1</sup> addresses the involvement of at-risk users in cybersecurity research. With a growing emphasis on inclusive design, research on at-risk users deserves heightened attention and ethical guidelines. This article adapts guidelines focused on research subjects with mental health conditions to the cybersecurity context. The second article, by Chowdhury and Renaud,<sup>A2</sup> addresses the growing trend of “digital first” policies by governments, where people are expected to interact with government services online. They argue for a policy-driven approach toward inclusive privacy and security and discuss how Amartya Sen’s Capability framework can be adapted to this problem.

The next two articles focus on two techniques in enhancing privacy and security: labels and gamification. Ramokapane et al.,<sup>A3</sup> in their article, underscore the importance of designing Internet of Things privacy labels that are inclusive to a wide range of underserved user populations. They further discuss various challenges and offer concrete design considerations toward inclusive privacy labels. Zhong et al.,<sup>A4</sup> in their article, explore various strategies of making gamification in cybersecurity training more inclusive to diverse populations. They conducted an empirical study to test these strategies and propose a set of design principles based on the study results. These principles can be useful for anyone who plans to include gamification in cybersecurity training.

The last two articles focus on two specific underserved populations: teens and people with visual impairments. Park et al.,<sup>A5</sup> in their article, challenge the common approach of restrictive protection for teens’ online safety and instead advocate for more resilient-based and privacy-preserving approaches, such as family-based collaborative approaches. Their empirical study shows promising results of the resilient-based approach. They also offer thoughtful considerations about how to ethically engage teens in privacy/security research. Finally, Janeiro et al.,<sup>A6</sup> in their article, dive into the problem of phishing from the perspective of screen-reader users, who are often individuals with visual impairments. Since common countermeasures for phishing are visual in nature, it is unclear how screen-reader users handle phishing. The authors conducted an empirical study, which yields insights into

these users’ phishing experiences and coping behavior. They also make recommendations for phishing prevention that could benefit future antiphishing tool design.

**A**lthough the articles in this special issue signal significant progress on this topic, more work is urgently needed, particularly in the bustling era of artificial intelligence (AI). A telling example is the recent incorporation of AI models in the Be My Eyes app to automatically generate captions of images submitted by individuals who are low vision or blind. However, they made a significant change to the app: turning off captioning if an image contains any human body to protect the privacy of those captured in the image. The blind and low-vision community was unhappy about this design change, as they often use the app to get captions for images that include people. Some of our own recent research has shown that not only do low-vision and blind populations respect the privacy of people in such imagery, but also people in the surroundings are willing to be analyzed depending on the type of information being conveyed.<sup>3,4</sup> Yet, challenges remain in striking a balance in practice, and this example highlights the importance of engaging underserved populations in the design of AI, as they could be disproportionately affected by design decisions based on typical security and privacy concerns. ■

---

#### Appendix: Related Articles

- A1. F. Sharevski, “Inclusive involvement of at-risk users in cybersecurity research,” *IEEE Security Privacy*, vol. 22, no. 5, pp. 13–22, Sep./Oct. 2024, doi: [10.1109/MSEC.2024.3416878](https://doi.org/10.1109/MSEC.2024.3416878).
- A2. P. D. Chowdhury and K. Renaud, “Advocating a policy push toward inclusive and secure “digital-first” societies,” *IEEE Security Privacy*, vol. 22, no. 5, pp. 23–31, Sep./Oct. 2024, doi: [10.1109/MSEC.2024.3431278](https://doi.org/10.1109/MSEC.2024.3431278).
- A3. K. M. Ramokapane, M. Sameen, and Z. Dkaidek, “Inclusive internet of things privacy labels,” *IEEE Security Privacy*, vol. 22, no. 5, pp. 32–39, Sep./Oct. 2024, doi: [10.1109/MSEC.2024.3417819](https://doi.org/10.1109/MSEC.2024.3417819).
- A4. C. Zhong, J. B. Kim, H. Liu, “The art of inclusive gamification in cybersecurity training,” *IEEE Security Privacy*, vol. 22, no. 5, pp. 40–51, Sep./Oct. 2024, doi: [10.1109/MSEC.2024.3427666](https://doi.org/10.1109/MSEC.2024.3427666).
- A5. J. K. Park, M. Akter, P. Wisniewski, and K. Badillo-Urquiola, “It’s still complicated: From privacy-invasive parental control to teen-centric solutions for digital resilience,” *IEEE Security Privacy*, vol. 22, no. 5, pp. 52–62, Sep./Oct. 2024, doi: [10.1109/MSEC.2024.3417804](https://doi.org/10.1109/MSEC.2024.3417804).
- A6. J. Janeiro, S. Alves, T. Guerreiro, F. Alt, and V. Distler, “Understanding phishing experiences of screen reader users,” *IEEE Security Privacy*, vol. 22, no. 5, pp. 63–72, Sep./Oct. 2024, doi: [10.1109/MSEC.2024.3430110](https://doi.org/10.1109/MSEC.2024.3430110).

## References

1. B. Doso, J. Hayes, and Y. Wang, "I'm Stuck!": A contextual inquiry of people with visual impairments in authentication," in *Proc. 12th Symp. Usable Privacy Secur. (SOUPS)*, Ottawa, CA, USA, Jul. 2015, pp. 151–168.
2. T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia, "Privacy concerns and behaviors of people with visual impairments," in *Proc. ACM SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, Seoul, South Korea, Apr. 2015, pp. 3523–3532, doi: [10.1145/2702123.2702334](https://doi.org/10.1145/2702123.2702334).
3. T. Akter, T. Ahmed, A. Kapadia, and M. Swaminathan, "Shared privacy concerns of the visually impaired and sighted bystanders with camera based assistive technologies," *ACM Trans. Accessible Comput.*, vol. 15, no. 2, pp. 1–33, May 2022, doi: [10.1145/3506857](https://doi.org/10.1145/3506857).
4. T. Ahmed, A. Kapadia, V. Potluri, and M. Swaminathan, "Up to a limit? Privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies," in *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol. (IMWUT/UbiComp)*, Sep. 2018, vol. 2, no. 3, pp. 1–27, doi: [10.1145/3264899](https://doi.org/10.1145/3264899).

**Apu Kapadia** is a professor of computer science and director of the Indiana University Privacy Lab in the Luddy School of Informatics, Computing, and Engineering, Indiana University Bloomington, Bloomington, IN 47408 USA. His research interests include usable security and HCI, with a recent focus on privacy in the context of online photo sharing. Kapadia received a Ph.D. in computer science from the University of Illinois at Urbana-Champaign. He is a Member of the IEEE. Contact him at [kapadia@iu.edu](mailto:kapadia@iu.edu).

**Yang Wang** is a professor of information science, and codirector of the Social Computing Systems Lab, University of Illinois at Urbana-Champaign, Champaign, IL 61820-6211 USA. His research interests include designing inclusive privacy and security mechanisms for underserved users. Wang received a Ph.D. in information and computer science from the University of California, Irvine. He is a Member of IEEE. Contact him at [yvw@illinois.edu](mailto:yvw@illinois.edu).



IEEE COMPUTER SOCIETY  
**Call for Papers**

Write for the IEEE Computer Society's authoritative computing publications and conferences.

**GET PUBLISHED**  
[www.computer.org/cfp](http://www.computer.org/cfp)

IEEE COMPUTER SOCIETY

IEEE