Article Type: THEME

Inclusive IoT Privacy Labels

Kopo M. Ramokapane, *University of Bristol, Bristol, BS8 1UB, United Kingdom*
Maria Sameen, *University of Bristol, Bristol, BS8 1UB, United Kingdom*
Zaina Dkaidek, *University of Bath, Bath, BA2 7AY, United Kingdom*

Abstract—IoT privacy labels present an opportunity for consumers to learn about the security and privacy of IoT devices and make informed decisions about their privacy. However, to make this a reality, they need to be inclusive and serving all users in a manner that they can use and value.

Index Terms: *User Privacy, IoT Privacy Labels, Inclusive Security, Inclusive Design, Smart home devices, At-risk users, Marginalized and Vulnerable populations (MVPs)*

While privacy research has made significant advancements in adopting a user-centered approach, achieving equitable privacy experiences for many remains a challenge. Disparities persist between those who are protected and those who are not. Prior research [1], [2] continues to argue that certain populations continue to be excluded from privacy protections due to factors beyond surface features such as usability. Exclusions are often rooted in individual circumstances, these can include but are not limited to: disabilities, long-term conditions as well as short- and long-term social, political, and economic conditions. Consequently, there has been a paradigm shift in the field, with researchers [1], [2], [3] advocating for greater consideration of these multifaceted factors in the design of protection mechanisms.

The aim is to ensure that no one is left behind in the pursuit of privacy. However, achieving equitable privacy goes beyond ensuring that the provision of technical protection mechanisms is fair; it also demands the development of privacy awareness and education mechanisms that inform users' decisions to be equitable. Privacy awareness and educational campaigns that are equitable have the potential to provide everyone with the opportunity to make informed decisions about their privacy, as a result, experience a private life.

Since their launch, consumer smart home Internet of Things (IoT) devices have suffered breaches, been misused to cause harm, and, in some cases, secretly collected consumer data. Indeed, the security and privacy of these devices have come under scrutiny by mainstream media, and studies indicate that consumers are primarily concerned about their security and privacy. Research suggests that there is a significant information asymmetry regarding the safety and security of these devices. Consequently, various government agencies and researchers have advocated for the implementation of security and privacy labels for IoT devices. Privacy labels are an awareness-raising mechanism that falls under the notice and choice framework [4], which aims to provide users with notice to assist them in making informed privacy choices.

Given the rapidly growing interest and research in equitable privacy and privacy labels, in this article, we pose an important question: **Can we design IoT Privacy labels that are inclusive, and ensure equal opportunities for everyone to use them in ways that are accessible and valuable?** We view this as a crucial consideration in achieving equitable privacy experiences with IoT devices. All consumers need to be equipped with sufficient information to make informed choices regarding the ownership of IoT devices. A well-informed consumer has a better chance of understanding the threats posed by various IoT devices.

If we have privacy labels that are not accessible to everyone, we risk endangering the privacy and safety of some specific populations. Privacy labels have the potential to help people decide which IoT devices to own or avoid, thus preventing harm. For example,

XXXX-XXX © 2021 IEEE
Digital Object Identifier 10.1109/XXX.0000.0000000

This article has been accepted for publication in IEEE Security & Privacy. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MSEC.2024.3417819

if a user is informed that the device can only be administered and controlled by one person, they may decide against purchasing it if they know they would not be allowed to configure or control it themselves. They could also assist users in understanding which security mechanisms are available to protect them. For instance, parents could choose to only purchase devices that have child protection mechanisms.

We define *Inclusive IoT Privacy Labels* as a design approach for privacy labels that aims to accommodate the diverse needs, preferences, and circumstances of all users, particularly those who may be marginalized or underrepresented. Inclusive privacy labels strive to ensure that the design and the information provided are accessible, understandable, and relevant to a wide range of individuals, regardless of their circumstances, identity, or abilities. An inclusive approach needs to be attentive to the privacy and security needs of different communities and the challenges they face when seeking information about the security and privacy of IoT devices. This would foster transparency, trust, and accountability in the IoT ecosystem. The best time to make these labels is right now, when there is yet to be a standard design of IoT Privacy Labels.

PRIVACY LABELS CONCEPT

The concept of nutrition labels initially emerged from the food industry, designed to offer consumers concise information about the nutritional contents of their products. In the context of privacy, this idea was first introduced in 2009 by Kelley et al. [5], focusing on improving the visual presentation and comprehensibility of privacy policies. The aim was to offer consumers concise information about the data practices of service providers, thereby enhancing the visual presentation and understandability of privacy policies. Privacy labels serve as a mechanism to help reduce information asymmetry between service providers and users. Privacy labels provides a new way of addressing the challenges of privacy policies, which are overly descriptive and contain legal jargon that is not understandable to the typical user. Consequently, users often avoid reading the privacy policies which leaves them unaware of the potential implications of using a specific service or device.

The success of privacy labels relies on the assumption that the service provider would honestly declare what data they collect and how it is processed. While this idea seemed absurd initially, with reports suggesting that service providers would not have any incentive to be truthful, this perspective has changed significantly since the prevalence of data-intensive systems has shown that people still use systems that collect and use sensitive data. Truthful information is critical for users to make informed decisions on whether they would want to use the service or allow data collection and processing. Initial studies showed that labels were successful in helping people decide on services; participants using the privacy nutrition label design could consistently select the companies that had privacy-friendly policies. Research also showed that the format of the label has a significant impact on users' understanding and interpretation of the data practices of the service providers.

Since their inception, mobile app privacy labels have gathered significant attention and have been embraced by Apple, followed by Google, for their mobile application ecosystems. The primary goal of these labels is to encourage transparency among app developers and foster trust among users. The purpose of a privacy label is to provide clear and understandable information about the data practices of a mobile application in a standardized way.

The Apple privacy labels (APL) describe data collection practices under four categories: privacy type (information on how the collected data is categorized and handled, e.g., data linked to you), purpose (the intended reason for data collection, e.g., analytics), data category (high-level data being collected, e.g., financial info), and data type (information in granular format, e.g., email address). Similarly, Google labels, referred to as Data Safety Section (DSS), are categorized into four sections: data practices, data categories, data types, and purpose.

In the context of mobile apps, developers are expected to honestly declare their data handling practices, and users, in turn, use this information to make informed decisions about their privacy [6]. Consequently, there has been extensive research on the integrity, accuracy, and usability of these labels. Results are mixed; some studies show that the adoption of labels has improved the transparency of data practices for most app developers, while others indicate that many declared data practices are not truthful. Additionally, some studies have highlighted developers' struggles in accurately declaring data practices, revealing instances of underreporting, overreporting, and inconsistencies in labels.

However, the adoption of privacy labels in the mobile app ecosystem has rapidly expanded into other contexts, such as IoT smart home devices. Various researchers [7], [8] have proposed labels for IoT smart home devices, all with the common goal of making data practices transparent and raising awareness about other aspects, such as sensors, type and number, and

other mechanisms that may impact users' privacy and security. While these proposals are still in the early stages, there is empirical evidence suggesting they are useful and have the potential to help users make informed decisions regarding the ownership of smart home IoT devices.

SECURITY AND PRIVACY OF AT-RISK USERS

In recent years, a growing body of literature has emerged with the aim of comprehensively understanding and addressing the security and privacy needs of at-risk users. Wang [3] characterizes these efforts as the third wave of privacy research, labeling it *Inclusive Privacy*. The fundamental argument put forth in these studies is that privacy considerations have historically been narrow, primarily focusing on the needs of the majority while neglecting users with specific identities, vulnerabilities, and circumstances. Criticism has also been focused at the conventional definition of a "user," which often depicts a passive individual from a WEIRD (Western, Educated, Industrialized, Rich, and Democratic) context, whose identity is assumed to be relatively secure from privacy violations. This narrow view of the user has been criticized for perpetuating powerful privacy norms that cater to specific groups while excluding others.

Moreover, scholars [1], [2], [9] have pointed out the limitations of exclusively prioritizing surface-level features, such as usability, in assessing privacy. They argue that while ease of use is important, it can often be insensitive and overlook the diverse needs and realities of users. Instead, there is a call for more nuanced approaches to understanding and responding to the privacy needs of diverse user populations. While acknowledging that the use of norms provides valuable insights into what a particular community considers acceptable, others [8] argue that these norms may sometimes converge unexpectedly, or fail to encompass certain identities or circumstances that particularly lie outside the general norms. Consequently, designing systems to uniquely conform to prevailing norms runs the risk of leaving users that these norms do not represent unprotected, causing them to resist using the systems or engage in self-censorship.

In response to these challenges, researchers have expanded the notion of the "user" to include previously overlooked groups, including children, older adults, immigrants, activists, journalists, LGBTQ+ individuals, non-Western users, survivors of domestic abuse, and those with various disabilities, such as visual impairments and cognitive disabilities. By incorporating these diverse perspectives, prior studies argue that threat models can better align with people's real-life circumstances, thus mitigating the risk of technology aggravating vulnerabilities within these populations.

Other researchers advocate for technologists to move beyond considerations of usability alone, instead urging them to take into account individuals' vulnerabilities [1] and capabilities [2]. They suggest that designers should purposefully identify vulnerabilities and capabilities before developing and designing protection mechanisms. By considering these factors, these studies also broaden the approaches to understanding the privacy needs of marginalized groups. Researchers and technologists are urged to consider power structures that can discriminate against certain identities, as well as the conditions of capitalism that may pose risks to certain identities. Other efforts [10] have explored equitable ways for researchers to collaborate with these groups to prevent power dynamics that might bias the understanding of their privacy needs or exploit them for research purposes.

While previous efforts represent a significant step toward fostering equitable privacy experiences, there remains a need to explore how we can achieve equity in privacy awareness mechanisms, such as privacy labels. Framing discussions on privacy labels through the lens of inclusive security represents a crucial step toward ensuring that all individuals have an equal opportunity to make informed choices regarding their privacy.

IoT PRIVACY LABELS

While the sales of consumer IoT devices continue to grow, security and privacy remain among the greatest concerns. Reports have surfaced detailing instances where these devices have been hacked, misused, or involved in the undeclared collection of data, leading to malfunctions that compromise consumers' safety. Moreover, these devices have been shown to advance the methods through which abusers can facilitate abuse. Previously, abusers used technologies like mobile phones, computers, and GPS trackers to inflict pain, harass, or track other individuals. However, with IoT devices, the scale of the problem has grown. Research has shown that due to the wide range of sensors available and their internet and connectivity capabilities, the tactics that abusers can use to harm others have expanded. These devices grant abusers significant power to cause more harm than previous methods. They are designed on the assumption of trust, assuming they will be used in households where everyone trusts each other. However, in many situ-

This article has been accepted for publication in IEEE Security & Privacy. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MSEC.2024.3417819

FIGURE 1. Illustrative example of IoT Privacy label showing sensors and the data they collect. Designed and proposed by Emami-Naeini et al. [7]

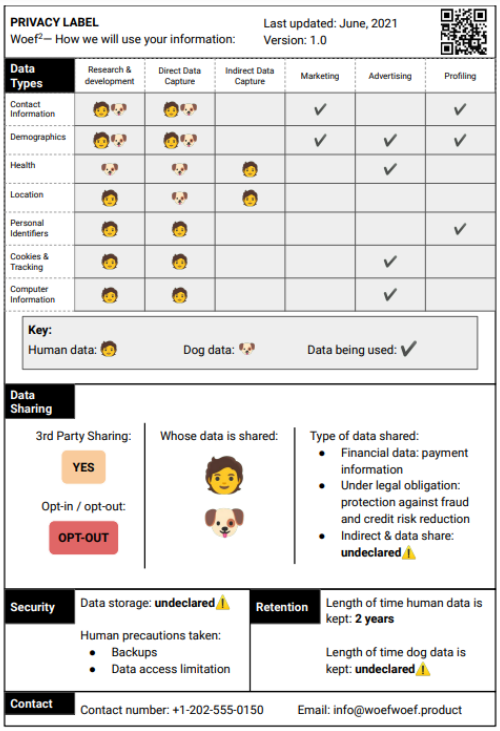

FIGURE 2. Illustrative example of IoT Privacy Label for pets wearables. Designed and proposed by McParlan and Van der Linden [12]

ations, this assumption causes numerous problems, including abusive relationships, bystanders, elderly homes, and situations involving children.

Consequently, numerous research [11] efforts have focused on understanding the prevalence of these issues and how consumers can be protected. Research has focused on survivors of intimate partner abuse, gender-based violence, children, older adults, and the devices themselves to understand how they have been used. Many of these studies cite a lack of awareness regarding how these devices work, available protection mechanisms, data collected, available sensors, or even how they can be misused. Without this knowledge, it is challenging for consumers to make decisions regarding their ownership, configuration, or how to behave around them. While this may seem trivial to the manufacturers of these devices, for some individuals, this can be a matter of life and death.

There have been efforts to address this issue and some researchers argue that the closed nature of these devices, such as proprietary software, is the primary reason why most users are unaware of the type of devices they are purchasing and whether they possess all the necessary protection mechanisms to meet their privacy needs. They contend that only the manufacturers are privy to such information, highlighting a need for greater transparency in this regard.

As a response, several researchers [7], [12], [13] have proposed various privacy labels for IoT devices as a means of addressing this issue. These proposals focus on various aspects of security and privacy; some highlight the number and types of sensors and data being collected (e.g., Figure 1), while others emphasize firmware updates and upgrades. Additionally, some labels target specific sets of devices, such as medical devices and pet wearables (Figure 2). While these labels are not yet standardized, many of these researchers argue that they are a more effective way of conveying information to users than traditional privacy policies. The assumption is that by manufacturers being transparent about these features and data practices, consumers can then make more informed decisions about which devices to own or which features are available for them to use in the devices to protect themselves.

Helping users make informed decisions about their

privacy has been extensively researched under the umbrella of the Notice and Choice framework [4]. Consequently, many mechanisms have been proposed to assist users in making better decisions regarding their privacy. However, many of these mechanisms have been criticized for their limitations, including inattention, dark patterns, causing fatigue, non-compliance, and excluding some users. This underscores the importance of enhancing the usability and inclusivity of privacy labels to mitigate similar shortcomings experienced by other notice and choice mechanisms. Moreover, if we are looking to standardize IoT security and privacy labels, it is important to ensure that they are accessible to everyone. With this in mind, one important question to answer is: how do we design IoT Privacy Labels to be more inclusive?

In other words, can we design privacy labels that not only provide IoT consumers with pertinent privacy and security information but also consider their diverse needs, preferences, and circumstances? This is an important step if we are to be inclusive and ensure that everyone can enjoy the benefits of IoT in a safer and more respectful manner. Making labels inclusive means ensuring that everyone has the opportunity to use them in a way that they can understand and appreciate; usable and accessible.

DESIGN CONSIDERATIONS

Inclusive design principles are well understood in the literature [14]. In this section, we discuss various factors that should be considered to make IoT Privacy labels more inclusive. This is not an exhaustive list but rather an initial step in raising awareness around the design of privacy labels. Designers should consider:

Diverse Cognitive abilities

Designers should prioritize the consideration of neurodiversity (ND) when creating labels, taking into account users with various cognitive disabilities. Neurodiversity encompasses the wide range of neurological differences in the human brain, which can affect emotions, learning ability, self-control, and memory. Conditions falling under this spectrum include attention deficit hyperactivity disorder (ADHD), autism spectrum disorder (ASD), dyslexia, dyscalculia, and others. While these conditions can stem from injury or illness, they can be noticed as individuals grow older. In the context of security, research [15] has shown that these cognitive disorders may contribute to the creation of insecure passwords and difficulties in solving CAPTCHAS or detecting phishing emails.

Designing for neurodiverse users therefore demands thoughtful consideration of color, shapes, text, and how elements relate to one another. Designers should ensure that there are multiple means of accessing the content of the labels, such as providing an audio version of the label for users who struggle with reading. Consumers can use assistive technology to help them access this information. Moreover, it is also crucial to present only essential information in an easily digestible format to avoid overwhelming consumers mentally. This may involve categorizing information or presenting it in a layered manner, starting with primary details and gradually introducing other information.

Some of the current designs of labels contain a significant amount of information and icons that can be challenging to interpret even for those without cognitive disabilities. It is therefore crucial for designers to acknowledge that some groups may struggle to process this information or link concepts together, thus by minimizing cognitive load and refraining from requiring users to remember excessive details would improve the usability of the labels.

Physical disabilities

Privacy label designers should take into account various visual impairments that may affect users' interactions with the labels. This includes individuals who are completely blind, those with limited vision, and those who are color blind. Designers should carefully consider the use of color, font, and icons in labels to ensure that they remain accessible to those with visual impairments. While current label designs often rely on icons and colors to differentiate various elements or indicate the level of risk associated with using the product, this approach excludes individuals who cannot see or interpret colors. Therefore, it is crucial for designers to explore alternative methods of communicating the same risks without relying solely on color.

Moreover, the volume of content or items within the label can also impact individuals with physical disabilities, underscoring the importance of including only necessary information. Lastly, labels could be made more inclusive for individuals with visual impairments by offering alternative versions, such as a tactile or audio version of the label, or providing it in braille. It is also important to ensure that labels are compatible with readers and other assistive technologies.

Language

The challenges posed by technical terms and jargon are well-known phenomena in security and privacy studies. When technologists use an abundance of

This article has been accepted for publication in IEEE Security & Privacy. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MSEC.2024.3417819

technical terms, users may struggle to understand them, thus affecting how they utilize such information to make decisions. It is crucial that privacy label designers consider using clear and simple language that is easily understandable by individuals with varying levels of literacy. They should refrain from employing jargon or technical terms that are regionally specific and may be unfamiliar to users around the world. Moreover, designers should provide alternative labels in other languages, which could be made available on various platforms such as the manufacturer's website. Relying only on English may disadvantage some particular groups, for example, immigrants who may not be proficient in English may encounter difficulties in comprehending the provided information.

Context of Use

One additional design consideration that should be noted is the context of use of IoT devices. For example, whether the device is safe for use in a household with children. There have been reports of children using devices to access content that is not appropriate for their age. Without specific information regarding the intended users, individuals (e.g., parents) would be unable to make informed decisions about which devices are suitable for their households. Moreover, the use of such devices by children may inadvertently result in manufacturers collecting and processing data related to minors, potentially leading to the serving of inappropriate advertisements. To protect children, designers could specifically include information about whether the device can be used by children or has mechanisms for child safety.

IoT Privacy labels should also aim to mitigate technology-facilitated abuse by providing security and privacy information that may influence the misuse of IoT devices. For example, designers could ensure that labels include information about whether the devices allow more than one account to have administrative rights, thereby enabling users to determine if there is an opportunity to share full control of the device. This design consideration may reduce the likelihood of devices being misused by individuals who set them up or whose accounts are used to register or activate the devices.

REFLECTIONS

Designing to enable various users to make better privacy decisions through privacy labels has its challenges. First, it is challenging to consider all situations and circumstances. There are users with capabilities that are complex to capture and design for, designers should not pressure themselves but should cater for as many scenarios as possible. All IoT users are important, and empowering them to make decisions about their privacy will not only protect them but also make them feel valuable in our communities.

Designing for everyone may also come at a cost; it might mean acquiring new skills or larger budgets. However, the benefits of including communities that have historically been excluded from tech design over time will outweigh the cost of implementation. The IoT ecosystem continues to grow with newer devices offering services that were initially unimaginable; therefore, not considering other communities may hinder their participation and enjoyment of the benefits.

Inclusive design also means proposing better approaches that can capture the needs of underrepresented communities. Previous research has suggested focusing on capabilities and vulnerabilities. The capability approach argues that designers should focus on what individuals can do and value, termed as basic capabilities, while the vulnerabilities approach emphasizes identifying vulnerabilities and then focusing on solutions to mitigate them. This means we need to understand what various users seek when getting information from labels and what they value or consider important from the labels. Then, we need to consider which vulnerabilities can be mitigated by using information from the privacy labels. In other words, we need to reconsider how we capture and scrutinize the content that appears on these labels. We need realistic use cases and definitions of people. Designers may have to study people naturally using the labels to capture more nuanced insights about how they can meet their needs.

The realization of *Inclusive IoT Privacy Labels* would also require significant input from policymakers. Policymakers have rightly called for labels for IoT; now it is important that they evaluate proposals considering their inclusivity. If standardized labels disregard the various realities we previously discussed in this article, then IoT device manufacturers will continue to exclude vulnerable users and those with differing capabilities.

CONCLUSIONS

In conclusion, this article emphasizes the need for *Inclusive IoT Privacy Labels* to enhance user awareness around the privacy and security of IoT devices across a diverse range of consumer groups. It argues for the necessity of designing privacy labels that are not only informative but also accessible to all users, highlighting the importance of giving all users an equal opportunity to make decisions around their privacy concerning IoT

devices. By taking this approach, IoT privacy label designers can acknowledge and address the diverse needs, circumstances, and preferences of users as well as aim to eliminate barriers that might prevent certain groups from fully understanding and utilizing privacy labels. While this article discusses inclusivity considering four design considerations—physical disabilities, language, context of use, and neurodiversity—this is not exhaustive list, but instead a preliminary step towards encouraging label designers to adopt a more inclusive perspective. Prioritizing inclusivity allows developers and label designers to foster equitable access to privacy information for all users which can lead to better-informed consumer choices and a more privacy-conscious IoT ecosystem.

ACKNOWLEDGMENTS

This work was supported in part by REPHRAIN EP/V011189/1, Equitable Privacy EP/W025361/1, EPSRC CDT TIPS-at-Scale EP/S022465/1.

REFERENCES

1. N. McDonald, and A. Forte, The politics of privacy theories: Moving from norms to vulnerabilities. *In Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2020, (pp. 1-14).
2. P. Das Chowdhury, A. D. Hernández, K. M. Ramokapane, and A. Rashid. From utility to capability: A new paradigm to conceptualize and develop inclusive pets. *In Proceedings of the New Security Paradigms Workshop*, 2022, (pp. 60-74).
3. Wang, Yang. “The third wave? Inclusive privacy and security." *In Proceedings of the new security paradigms workshop*, 2017.
4. Cranor, Lorrie Faith. "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice." in *Telecomm. and High Tech*, 2012
5. P. G. Kelley, J. Bresee, L. F. Cranor, and E. W. Reeder, A “nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* 1999, pp. 1-12.
6. R. Khandelwal, A. Nayak, P. Chung, and K. Fawaz, Unpacking Privacy Labels: A Measurement and Developer Perspective on Google’s Data Safety Section. In *USENIX security symposium 2024*
7. P. Emami-Naeini, Y. Agarwal, L.F. Cranor, and H. Hibshi, “Ask the Experts: What should be on an IoT privacy and security label?," in *IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 447–464.
8. S. Shruti, and A. Forte. "Privacy research with marginalized groups: what we know, what’s needed, and what’s next." In *Proceedings of the ACM on Human-Computer Interaction 6.CSCW2*, 2022: 1-33.
9. K. Renaud, and L. Coles-Kemp. “Accessible and inclusive cyber security: a nuanced and complex challenge.” in *SN Computer Science*, 2022, 346.
10. K. M. Ramokapane, et al. "Towards Equitable Privacy." In *arXiv preprint arXiv:2308.00004*, 2023.
11. S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart, Clinical computer security for victims of intimate partner violence. In *28th USENIX security symposium* (pp. 105-122).
12. J. McParlan, and D. van der Linden. "Privacy labels should go to the dogs." In *Proceedings of the Eight International Conference on Animal-Computer Interaction*, 2021.
13. Y. Shen, and V. Pierre-Antoine, "Iot security and privacy labels." *In Privacy Technologies and Policy: 7th Annual Privacy Forum, APF*, 2019, Rome, Italy
14. P. J. Clarkson, and R. Coleman. "History of inclusive design in the UK." in *Applied ergonomics*, 2015, 235-247.
15. J. Kävrestad, A. Hagberg, R. Roos, J. Rambusch, and M Nohlberg, "Usable Privacy and Security from the Perspective of Cognitive Abilities." In *IFIP International Summer School on Privacy and Identity Management. Springer International Publishing*, 2021. 105-121.

Kopo M. Ramokapane is an assistant professor and researcher at the University of Bristol Cyber Security Group, specializing in Usable Security. His interdisciplinary research focuses on making security measures more user-friendly and effective, particularly in the context of smart home technologies and equitable privacy. Through his research, Ramokapane works to bridge the gap between technology and human behavior to improve overall security posture. He received a Ph.D. in Computer Science from the Lancaster University. Contact: marvin.ramokapane@bristol.ac.uk

This article has been accepted for publication in IEEE Security & Privacy. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MSEC.2024.3417819

Maria Sameen is a Ph.D. student under the Centre for Doctoral Training in Cyber Security (TIPS-at-Scale) programme at the University of Bristol, UK. She is also a visiting postgraduate researcher at the University of Bath, UK. Her current research interests include socio-technical aspects of dark patterns, usable security and privacy, and privacy testbeds. Sameen received her MEng degree in Computer Engineering from Gachon University, Republic of Korea. She is an ACM Professional Member. Contact her at maria.sameen@bristol.ac.uk.

Zaina Dkaidek is a Ph.D. candidate in the Centre for Doctoral Training in Cyber Security (TIPS-at-Scale) program at the Univerity of Bath and the University of Bristol, United Kingdom. Her current research interests include decision-making and expertise within the context of cyber security, usable security and privacy, cyber policy, cyber's global impact particularly the altering balance of power, and cyber diplomacy. Dkaidek received her MSc degree in Security Studies from the University College London, United Kingdom. Contact information: zd420@bath.ac.uk.