International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 75 – 89, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1008

Participatory Design as a Remedy for Misprofiling In Security Artificial Intelligence

.Sheriffdeen Folaranmi Abiade
Department of History and International Studies
Adeleke University
Ede, Osun State
Nigeria

Abstract: The growing reliance on artificial intelligence (AI) for security applications ranging from biometric identification to predictive policing has raised pressing concerns about misprofiling, bias, and disproportionate targeting of marginalized populations. Misprofiling in security AI arises from skewed datasets, opaque algorithmic models, and exclusion of affected communities in the design process, leading to systemic errors and erosion of public trust. To address these challenges, participatory design (PD) emerges as a critical approach that embeds inclusivity, accountability, and contextual knowledge directly into AI development pipelines. Unlike conventional top-down engineering methods, PD emphasizes collaboration with end-users, stakeholders, and communities most impacted by surveillance and risk assessment technologies. This democratization of design enables the identification of hidden biases in training datasets, ensures diverse perspectives shape model objectives, and creates space for ethical negotiation in algorithmic trade-offs. Moreover, PD can be operationalized through structured workshops, co-design prototyping, and iterative feedback mechanisms, all of which promote transparency and foster legitimacy in security AI systems. When applied rigorously, participatory design not only mitigates the risk of misprofiling but also enhances operational reliability by aligning technical outputs with real-world security needs. At a broader scale, the adoption of PD frameworks contributes to governance models that balance innovation with human rights protections. This paper argues that participatory design is not merely a supplementary tool but a structural remedy to the persistent failures of misprofiling in security AI. Its integration into design and policy cycles is essential for achieving both technological robustness and societal fairness.

Keywords: Participatory design, security artificial intelligence, misprofiling, algorithmic bias, inclusivity, ethical AI

1. INTRODUCTION

1.1 Background on Security AI

Artificial intelligence (AI) has rapidly become embedded in the security sector, transforming surveillance, border control, predictive policing, and cybersecurity practices. Governments and private actors increasingly rely on algorithmic systems to process vast amounts of data, detect anomalies, and generate actionable intelligence [1]. Unlike traditional methods limited by human capacity, AI enables the analysis of millions of communication records, video feeds, and behavioral datasets in real time. Such scalability provides a critical advantage for security agencies tasked with addressing threats that are both transnational and technologically sophisticated [2].

In surveillance, computer vision systems are now capable of detecting suspicious behavior in crowded urban environments, while border agencies deploy biometric recognition to verify identities and flag anomalies [3]. Predictive policing has emerged as another application, where AI models attempt to forecast crime "hotspots" or anticipate potential offenders based on historical data [4]. Cybersecurity similarly benefits from AI, as anomaly detection algorithms help identify malicious intrusions before they escalate into systemic breaches.

The efficiency of AI in these areas is reinforced by its capacity for pattern recognition and predictive analytics. Instead of waiting for threats to manifest, agencies can act proactively, reducing response times and improving accuracy [5]. Figure 1 illustrates how AI applications interconnect across multiple layers of security infrastructure, demonstrating both their breadth and interdependence. However, the same systems that promise efficiency and scalability also risk producing harmful errors when misaligned with social and ethical considerations [6]. These risks set the stage for understanding the problem of misprofiling.

1.2 The Problem of Misprofiling

Misprofiling refers to the generation of false positives, biased classifications, or discriminatory outputs by AI systems deployed in security contexts. Unlike conventional human errors, misprofiling in AI is amplified by scale, as algorithms can systematically misclassify large populations, embedding bias into surveillance and policing practices [5]. These errors often stem from skewed training data, opaque algorithmic decision-making, or flawed assumptions coded into predictive models.

High-profile controversies highlight the gravity of the issue. In several jurisdictions, facial recognition systems

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 75 – 89, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1008

misidentified individuals from minority ethnic groups at disproportionately high rates [1]. Such misidentifications led to wrongful detentions, public mistrust, and significant reputational damage for deploying agencies [7]. Predictive policing algorithms, too, have faced criticism for perpetuating racial and socio-economic biases, as they often direct law enforcement attention toward historically over-policed neighborhoods [4]. Instead of reducing crime, these systems risk reinforcing structural inequalities and deepening cycles of surveillance in marginalized communities.

The consequences of misprofiling extend beyond technical failures. For affected individuals, being wrongfully flagged as a potential threat can result in social stigma, denial of services, or even legal penalties [2]. At a societal level, repeated cases of misprofiling erode trust in security institutions and weaken public support for technological innovation. The ethical stakes are particularly high in the Global South, where weaker regulatory frameworks provide limited recourse for victims of algorithmic discrimination [6]. Table 1 summarizes selected misprofiling controversies, categorizing them by technology type, context, and social impact. The evidence underscores the urgency of addressing misprofiling not as isolated error but as a systemic challenge requiring structural remedies [3].

1.3 Introducing Participatory Design

Participatory design offers a potential remedy to the challenges of misprofiling by embedding diverse voices into the design, testing, and deployment of AI security systems. Rooted in democratic innovation traditions, participatory design emphasizes collaboration between developers, policymakers, and affected communities [5]. Its relevance in the security domain lies in its ability to surface overlooked perspectives, particularly those of marginalized populations most at risk of being misprofiled.

The concept involves structured processes such as community consultations, stakeholder workshops, and iterative prototyping with user feedback. By incorporating lived experiences into the design cycle, participatory design helps developers identify potential harms before they become embedded in deployed systems [1]. For example, including civil society groups in discussions about predictive policing algorithms can highlight the risks of reinforcing existing social inequalities [7]. Similarly, integrating feedback from minority communities during the development of biometric systems can reveal context-specific vulnerabilities that technical experts may overlook [4].

As **Figure 1** shows, governance frameworks that integrate participatory design create feedback loops between technical developers, security agencies, and affected communities. This approach ensures that AI systems are not merely efficient but also socially responsive. **Table 1**, by cataloging controversies, underscores why participatory design is urgently needed: it provides pathways to anticipate, mitigate, and monitor risks of misprofiling.

In this article, the thesis advanced is that participatory design can help balance innovation with justice by democratizing AI development. Moving from the problem of misprofiling to the remedy of participatory practices creates a logical pathway for exploring how AI can strengthen security without compromising human dignity [6].

Figure 1: AI applications across surveillance, policing, border control, and cybersecurity (interconnected governance layers).

Table 1: Selected misprofiling controversies in AI security systems (technology type, context, and social impact)

Technology Type	**Context of Application**	**Documented Social Impact**
Predictive Policing Algorithms	Urban policing and crime hotspot prediction	Racial profiling of minority communities, reinforcing existing biases in law enforcement.
Facial Recognition Systems	Airport screening and border control	Misidentification of ethnic minorities and women, leading to wrongful detentions and delays.
Voice Recognition and Analysis	Counterterrorism surveillance in telecom infrastructures	Higher false rejection rates for non-native accents, creating inequities in security checks.
Cybersecurity Anomaly Detection	Financial institutions and critical	Misclassification of benign activities as threats, resulting in

Technology Type	Context of Application	Documented Social Impact
	infrastructure	service disruptions.
Social Media Monitoring Tools	Counter-extremism and online content moderation	Over-policing of political speech and mislabeling of activist content as extremist material.

2. THEORETICAL FOUNDATIONS OF MISPROFILING IN SECURITY AI

2.1 Algorithmic Bias and Data Inequality

Algorithmic bias and data inequality are central problems in the deployment of AI systems for security profiling. Security AI tools often rely on datasets that are incomplete, unbalanced, or skewed toward particular demographic categories [6]. For example, facial recognition databases may disproportionately include images of lighter-skinned individuals while underrepresenting darker-skinned populations. This lack of representativeness leads to systematic misclassification, producing false positives or false negatives that disproportionately affect marginalized groups [9].

Data inequality does not arise only from demographic imbalances but also from structural limitations in how datasets are collected. Security agencies often gather data from surveillance-intensive areas such as low-income neighborhoods or border regions, meaning that training data already reflect biased policing practices [7]. When such data are used to build predictive models, the biases are reinforced, perpetuating cycles of surveillance and over-policing in already vulnerable communities.

The consequences for profiling accuracy are profound. Instead of providing neutral or objective insights, AI systems amplify existing inequalities, resulting in outcomes that systematically disadvantage certain groups [12]. Misprofiling in this context is not a technical glitch but a structural outcome of unequal data ecosystems. Moreover, the predictive capacity of these systems can create feedback loops: flagged areas receive more surveillance, generating more data that further "proves" the original bias [10].

In contexts with weak regulatory oversight, the risks are magnified. Global South nations, for example, often lack comprehensive data protection laws, making it easier for biased datasets to be deployed without scrutiny [13]. As Figure 1 illustrates, algorithmic bias is not isolated but interlinked with opacity and institutional practices, creating a complex web of risk factors. Addressing data inequality therefore requires both technical fixes, such as improved dataset representativeness, and structural reforms to ensure that profiling practices do not reinforce systemic discrimination [8].

2.2 Black-box Models and Opacity

Black-box models, particularly deep learning systems, pose unique risks in security-sensitive domains. These models often achieve high levels of predictive accuracy but lack transparency, making it difficult to explain or contest their outputs [11]. For security AI, opacity is more than a technical inconvenience it is a governance challenge. When decisions about who is flagged as suspicious cannot be explained, accountability mechanisms break down, leaving individuals without recourse [6].

One source of opacity lies in the mathematical complexity of neural networks. Layers of weights and non-linear transformations produce outputs that even developers struggle to interpret [7]. As a result, security agencies deploying these systems cannot fully explain why an individual was profiled, raising concerns about fairness and due process [9]. This lack of explainability is particularly problematic in counterterrorism and border security, where decisions often carry high-stakes consequences such as detention, denial of entry, or prolonged surveillance.

The opacity of black-box models also amplifies risks when combined with algorithmic bias. If biased datasets feed into opaque systems, errors become harder to detect and correct [12]. For example, if a facial recognition system consistently misidentifies individuals from a minority group, the absence of transparency prevents stakeholders from identifying the root cause. Instead, the system's "accuracy" may be accepted at face value, embedding discrimination into institutional practice [8].

In addition, opacity creates challenges for oversight and auditing. Policymakers and regulators may require transparency to evaluate the fairness of AI tools, yet commercial vendors often guard their algorithms as proprietary secrets [13]. This dynamic leaves public institutions reliant on private companies without sufficient visibility into system operations.

As depicted in Figure 1, opacity interacts with bias and institutional contexts to exacerbate misprofiling risks. Addressing opacity requires developing explainable AI (XAI) methods, mandating algorithmic audits, and ensuring that security agencies have the capacity to critically assess the systems they deploy [10]. Without these interventions, black-box models risk eroding both accountability and trust in security governance.

2.3 Sociotechnical Perspectives on Profiling

Security AI should not be understood solely as a technical tool but as part of a broader sociotechnical system shaped by institutional practices, political priorities, and power structures [6]. Viewing AI profiling from a sociotechnical perspective reveals that technical errors like bias and opacity are embedded in wider governance frameworks that determine how systems are used and for whose benefit.

Institutional practices play a central role in shaping outcomes. Security agencies often deploy AI tools under conditions of urgency, prioritizing speed and efficiency over fairness and accountability [11]. Political pressures to demonstrate "tough on crime" or "strong border" policies can lead to the uncritical adoption of AI surveillance systems, even when their risks are well-documented [7]. In such contexts, misprofiling becomes not only a technological issue but a manifestation of institutional incentives and power asymmetries [12].

The politics of security AI are further shaped by global inequalities. In many Global South countries, AI systems are imported from Global North vendors without sufficient local adaptation [13]. This dynamic reinforces dependency and limits the capacity of local institutions to challenge or reinterpret how profiling systems operate. As Figure 1 shows, institutional context mediates the technical issues of bias and opacity, shaping how misprofiling manifests in practice.

Power structures also influence how misprofiling impacts different groups. Marginalized communities whether ethnic minorities, migrants, or economically disadvantaged populations often bear the brunt of errors and discriminatory profiling [9]. At the same time, their voices are frequently excluded from decision-making processes, leaving little opportunity to contest or reshape how AI systems are deployed.

Adopting sociotechnical perspectives encourages more holistic approaches to addressing misprofiling. Technical fixes alone cannot resolve structural inequalities if institutional incentives and political agendas remain unchanged [8]. Solutions must therefore integrate technical transparency, participatory governance, and ethical oversight. Table 1, which catalogues misprofiling controversies, underscores that the roots of these errors are as much institutional as technical. By embedding sociotechnical analysis into the governance of AI profiling, states can better understand and mitigate the risks posed by security AI [10].

3. PARTICIPATORY DESIGN: PRINCIPLES AND METHODS

3.1 Historical Roots of Participatory Design

Participatory design emerged historically from Scandinavian labor movements in the 1960s and 1970s, where workers sought greater involvement in shaping technologies that affected their labor conditions [11]. The early co-design tradition emphasized the democratic principle that those impacted by technology should have a say in its development. Initially rooted in workplace contexts, these approaches aimed to counteract managerial dominance in automation decisions and to ensure that technology empowered workers rather than undermined them. The Scandinavian model established a precedent for inclusive design, framing participation not as a token gesture but as a structural principle of technology development [13].

As participatory design spread globally, it evolved beyond labor issues into broader domains such as healthcare, urban planning, and education [15]. This evolution reflected a recognition that technology design is never value-neutral, but deeply embedded in social, political, and cultural contexts. The shift toward inclusivity meant that diverse user groups patients, citizens, students, and communities were incorporated into decision-making processes through structured workshops, dialogues, and collaborative prototypes [16].

This historical grounding remains crucial for contemporary debates about security AI. By understanding participatory design as a movement rooted in democratization, one can appreciate its relevance in contexts where power asymmetries are stark, such as policing, immigration control, and counterterrorism surveillance [12]. Figure 1, introduced in the previous section, provides a conceptual basis for situating participatory design as a counterbalance to risks like bias and opacity. In this sense, participatory design is not only a methodology but also a political stance that aligns technological development with democratic accountability [14]. This background sets the stage for adapting its principles to AI systems that risk misprofiling vulnerable populations.

3.2 Key Principles for Security AI

Applying participatory design to security AI requires articulating principles that can withstand the pressures of sensitive, high-stakes contexts. Four interlinked principles inclusivity, transparency, shared decision-making, and accountability form the foundation of such adaptation [13].

Inclusivity ensures that voices of marginalized communities, often the most affected by misprofiling, are represented in the design process. Without deliberate inclusion, AI systems risk reproducing structural biases by ignoring the lived experiences of those historically subject to disproportionate surveillance [11]. For example, involving immigrant advocacy groups in the design of border control technologies can reveal cultural and contextual blind spots otherwise invisible to technical experts [15].

Transparency complements inclusivity by making decision-making processes visible to participants. This includes not only technical transparency, such as explainability of AI models, but also procedural transparency about how stakeholder input is gathered, weighted, and implemented [12]. In policing contexts, transparency can reduce suspicion by showing communities how predictive algorithms are trained and validated.

Shared decision-making goes beyond consultation to involve stakeholders in genuine co-determination. It requires mechanisms where civil society actors, policymakers, and technical experts deliberate together on design trade-offs [16]. In immigration systems, for instance, shared decision-making might involve balancing efficiency with humanitarian obligations, ensuring that AI supports rather than undermines human rights.

Finally, accountability ensures that participatory processes do not end at the design stage but extend into deployment and oversight. Independent monitoring bodies, periodic audits, and feedback loops allow communities to hold institutions responsible for outcomes [14]. Table 1, discussed earlier, documents failures where lack of accountability in misprofiling cases led to systemic harm. Embedding accountability mechanisms into AI governance is thus essential for aligning technology with democratic values.

Together, these principles operationalize participatory design in security contexts. They provide a normative and practical framework to guide interventions where the risks of error and abuse are too high to ignore [17].

3.3 Participatory Design Methods

The application of participatory design in security AI requires robust methods capable of addressing both technical and social complexities. Methods such as co-design workshops, stakeholder mapping, and scenario building have long been part of participatory traditions, but in recent years they have been complemented by digital ethnography, design probes, and role-play simulations [11]. These techniques provide structured ways to integrate diverse perspectives into system design.

Co-design workshops are among the most widely used methods, creating spaces where affected stakeholders collaborate directly with designers and policymakers. In security contexts, such workshops might involve law enforcement officers, civil rights groups, and community representatives jointly sketching out features of surveillance or profiling tools [15]. These interactions allow latent concerns to surface early, preventing harmful design decisions from being embedded unnoticed.

Stakeholder mapping extends participation by systematically identifying all actors who influence or are influenced by AI systems [13]. In counterterrorism profiling, for example, stakeholder maps may reveal not only state agencies but also private telecom providers, advocacy organizations, and impacted communities. By visualizing these relationships, mapping helps ensure no critical perspective is excluded.

Scenario building allows participants to explore hypothetical futures, testing how AI systems might behave in realistic contexts [16]. For instance, participants might model how predictive policing tools react to community protests, revealing tensions between efficiency and rights. Scenario building is especially useful for highlighting unintended consequences, making it a critical tool in security domains.

Newer techniques such as digital ethnography capture lived experiences of those most impacted by security profiling [12]. By documenting how communities interact with surveillance systems, digital ethnography brings qualitative nuance to datasets that might otherwise erase social complexity. Design probes and role-play simulations push this further by immersing participants in experimental exercises. For example, role-play may involve law enforcement personnel acting as community members subject to surveillance, fostering empathy and deeper understanding [14].

As Figure 1 emphasizes, misprofiling results from the interplay of bias, opacity, and institutional contexts. Participatory design methods target these issues by embedding diverse voices into each stage of the design cycle, from data collection to system auditing. Moreover, they create pathways for iterative learning, allowing systems to evolve alongside changing political and social contexts [17].

Table 1, by documenting misprofiling controversies, underscores why these methods are essential. Each controversy reveals gaps that participatory processes could have addressed: biased datasets, opaque algorithms, or absent community consultation. Methods like co-design workshops and digital ethnography transform these lessons into actionable practices. The transition from theory to method thus demonstrates how participatory design can move beyond abstract principles to concrete interventions in the governance of security AI [11].

4. LINKING PARTICIPATORY DESIGN TO AI DEVELOPMENT

4.1. Data Collection and Curation

Data collection is the cornerstone of any artificial intelligence system, particularly those intended for high-stakes security environments. The process of defining what constitutes relevant data must not be confined to technical experts alone. Instead, it should actively include input from communities that will ultimately be impacted by AI profiling systems. Such engagement provides cultural and contextual insights that traditional data engineers may overlook. For example, language use in local dialects, social practices, or historical patterns of mobility can significantly shape how security algorithms interpret risk signals. Without community-informed framing, datasets risk reproducing dominant institutional biases rather than reflecting diverse lived experiences [17].

Demographic diversity in data is equally critical. Many documented failures of AI-driven profiling stem from skewed datasets where minority populations are underrepresented. This lack of representativeness produces systematic errors in classification and can exacerbate inequality in policing, immigration screening, or counterterrorism activities [21]. Participatory curation allows diverse groups to negotiate data inclusion criteria and flag categories that might unintentionally stigmatize certain populations. This step shifts the focus from purely technical accuracy toward social fairness in the curation process.

Contextual accuracy also depends on ensuring that metadata such as time, location, or socio-political background is preserved. Security incidents are rarely isolated technical events; they are embedded in complex sociotechnical contexts. Through deliberative forums, local actors can guide developers in recognizing nuances, such as distinguishing

cultural gatherings from suspicious assemblies, thus preventing false alarms [18].

Participatory data collection requires new mechanisms of trust. Community representatives may question how their contributions are safeguarded and whether they will later be used against them. Transparent consent protocols and clear communication about data lifecycle management are thus integral to legitimacy [15]. Table 1 provides a structured overview of how participatory interventions align with different stages of the AI pipeline, beginning with data collection and extending into training and deployment.

By embedding participatory approaches at this earliest stage, developers can build datasets that are not only technically robust but also socially legitimate. This foundational step ensures that misprofiling risks are minimized before they become deeply entrenched in the algorithmic pipeline [22].

4.2. Model Training and Validation

The second stage in the AI pipeline model training and validation determines how raw data is transformed into actionable classifications. Traditional approaches rely heavily on automated feature extraction and labeling by technical teams. However, these processes often lack transparency and may embed subtle forms of bias. Participatory evaluation during training introduces diverse perspectives into critical design choices, such as which features are emphasized, how labels are assigned, and what criteria define accuracy. Engaging stakeholders in these tasks democratizes the training phase and mitigates risks of systematic misprofiling [16].

Community involvement in labeling is especially important. Labels are never neutral; they encode social judgments about what constitutes suspicious or benign behavior. For instance, the categorization of “unusual activity” in surveillance datasets can reflect cultural misunderstandings if defined solely by external actors. Participatory co-labeling ensures that contested categories are negotiated rather than imposed, thereby enhancing fairness in the training data [19].

Validation processes also benefit from participatory oversight. Standard machine learning pipelines evaluate accuracy through cross-validation metrics such as precision, recall, or F1 scores. While statistically rigorous, these metrics rarely capture the social implications of errors. False positives in a security context, for instance, may have life-altering consequences for individuals misidentified as threats. Co-validation with impacted groups expands the notion of accuracy to incorporate lived experiences of algorithmic misclassification. This creates a multidimensional evaluation framework that balances technical efficiency with social responsibility [22].

Participatory model training further improves accountability. When community members are involved in reviewing early-stage model outputs, they can flag cases where the algorithm appears to reinforce harmful stereotypes. This feedback loop operates before full-scale deployment, making it possible to adjust model parameters proactively. Such interventions align with broader principles of responsible innovation, where the potential harms of technology are anticipated rather than retroactively managed [20].

Ultimately, participatory involvement in training and validation transforms affected communities into co-designers of AI systems. This not only improves the fairness of classification outcomes but also strengthens public trust in security applications. Without such measures, AI risks entrenching a technocratic model of governance that disregards the very populations it aims to protect [15].

4.3. Deployment and Feedback Loops

Deployment is the stage at which AI systems begin to directly influence real-world security practices. In high-risk contexts such as border control, airport screening, and counterterrorism monitoring, misprofiling during deployment has profound implications. A participatory framework must therefore extend beyond design and training into continuous oversight during implementation. Communities should not merely be consulted before deployment; they must be empowered to monitor, question, and shape AI systems throughout their operational lifespan [19].

One mechanism for participatory oversight is the establishment of citizen review panels. These bodies, composed of community representatives, civil society groups, and technical experts, can audit deployed systems and evaluate their fairness over time. Unlike one-off evaluations, such panels create institutionalized feedback loops where recurring errors or disproportionate targeting are systematically flagged and corrected [22]. This approach operationalizes the principle that accountability must be ongoing rather than episodic.

Deployment must also provide clear pathways for redress. When individuals are wrongly profiled as threats, the consequences can range from reputational harm to unwarranted detention. A participatory system ensures that affected individuals have accessible, transparent mechanisms to challenge algorithmic decisions. These mechanisms might include ombudsman offices, independent appeals processes, or participatory grievance boards with authority to mandate corrective action [18]. By embedding these structures into deployment, AI systems move closer to respecting due process and human rights.

Feedback loops are central to sustaining participatory governance after deployment. AI models are dynamic; they evolve as they encounter new data in real-world environments. Without participatory monitoring, adaptive models may drift in ways that inadvertently reinforce bias. For example, if a predictive policing model disproportionately targets one neighborhood, it generates new data that confirms its own skewed assumptions. Community oversight breaks this cycle by critically interrogating feedback inputs and demanding corrections [21].

Participatory audits represent another critical intervention. Unlike traditional technical audits that focus narrowly on compliance, participatory audits include stakeholders in defining audit criteria, interpreting results, and proposing remedies. This shared process generates richer, context-sensitive evaluations that capture the social consequences of algorithmic performance. Such audits also make visible the political dimensions of AI deployment, highlighting how power and accountability are distributed across institutions [16].

Importantly, participatory deployment is not only reactive but also anticipatory. Communities can engage in scenario planning to forecast how deployed systems might evolve under different political or social conditions. For instance, they may raise concerns about how a system designed for counterterrorism could later be repurposed for suppressing political dissent. By voicing these possibilities early, communities help safeguard democratic freedoms against technological misuse [20].

Table 1 illustrates how participatory interventions span the entire AI pipeline, showing that community involvement must not end at the design stage but must extend into deployment and long-term oversight. This table highlights expected outcomes such as enhanced fairness, greater accountability, and improved legitimacy of AI in security contexts.

The integration of participatory methods across deployment and feedback loops reflects a paradigm shift in AI governance. Instead of treating affected groups as passive recipients of technological decisions, participatory frameworks reposition them as active co-governors. This shift enhances resilience, as systems co-designed and co-monitored by diverse actors are less likely to fail under the weight of bias or public opposition [17].

In conclusion, embedding participatory oversight into deployment ensures that AI systems in security contexts remain both effective and just. Continuous feedback loops, transparent redress mechanisms, and participatory audits are not optional add-ons but essential safeguards. Without them, deployment risks cementing a cycle of misprofiling and mistrust, undermining both security outcomes and public legitimacy [15].

5. CASE STUDIES OF MISPROFILING AND PARTICIPATORY RESPONSES

5.1. Predictive Policing Systems

Predictive policing has long been criticized for entrenching racial and socioeconomic misprofiling, especially in urban communities already over-surveilled. Many systems were trained on historical crime data, which often reflected biased enforcement patterns rather than objective criminal behavior. For instance, communities of color were disproportionately flagged as high-risk, not because of higher actual crime rates, but due to policing strategies that had historically concentrated resources there [20]. This cycle of reinforcement created a self-fulfilling loop where predictive models justified and expanded unequal policing practices.

The consequences were profound: individuals from marginalized backgrounds experienced higher rates of stop-and-frisk, community harassment, and erosion of trust in state institutions [23]. Such systems not only undermined civil rights but also reduced the reliability of crime detection by amplifying noise instead of addressing root causes. Participatory approaches attempted to respond by involving community stakeholders in algorithm design and oversight. Pilot projects introduced collaborative workshops where residents could examine model assumptions, identify blind spots, and push for inclusion of contextual variables such as poverty levels, access to education, and local social services [21].

These participatory efforts revealed how technical models could benefit from lived experience. For instance, when communities challenged proxy variables like “number of past arrests” they highlighted how these features primarily encoded institutional bias. By substituting or weighting features differently, pilot systems achieved better alignment with community priorities while also reducing disproportionate targeting. The participatory element ensured that design was not purely technical but infused with human judgment.

Still, the integration of participatory processes was uneven and often resisted by institutional actors who perceived community oversight as diluting efficiency. Yet, case evidence suggested otherwise: systems redesigned with participatory engagement not only reduced false positives but also gained legitimacy in the eyes of residents [19]. Importantly, such reforms laid groundwork for broader participatory integration in other security-sensitive AI systems, as outlined in Figure 2, which contrasts conventional policing workflows with participatory-informed alternatives. Table 2 further illustrates case studies where participatory remedies reshaped predictive policing outcomes across cities. Together, these insights highlight that predictive policing reforms are less about rejecting AI outright and more about reconfiguring its governance structures toward accountability and fairness [24].

5.2. Airport and Border Security

Airports and border zones became early testbeds for large-scale AI deployment, especially in biometric surveillance and passenger risk screening. Facial recognition technologies promised efficiency but often produced errors across demographic groups. Travelers with darker skin tones, women, and elderly individuals were disproportionately misidentified, leading to delays, invasive questioning, and in some cases denial of boarding or entry [22]. Such misprofiling had severe implications, particularly in high-stakes contexts like border control, where errors could result in prolonged detention or wrongful suspicion.

Community advocacy groups raised concerns that these systems operated in a “black-box” mode, where individuals subject to scrutiny had no means to contest algorithmic judgments. The opacity of risk scores and facial match probabilities compounded frustrations, as authorities often deferred responsibility to the “machine” rather than human discretion [25]. Advocacy organizations argued that accountability should remain firmly with institutions, not outsourced to opaque technical processes.

Participatory approaches in airport and border contexts experimented with consultative models. In one pilot, passenger representative groups, civil liberties organizations, and privacy regulators were invited to review biometric datasets used in training facial recognition engines. Their interventions exposed underrepresentation of minority populations, leading to adjustments in data sampling and annotation practices [20]. Further, scenario-based workshops allowed affected communities to simulate checkpoint interactions and provide feedback on interface design, ensuring that security processes could be both robust and minimally discriminatory.

Another promising practice was the establishment of feedback loops where misidentified passengers could formally register complaints, triggering a participatory review board to audit both system decisions and institutional procedures [23]. These oversight mechanisms introduced not only avenues of redress but also continuous learning opportunities for system developers. Over time, iterative engagement helped refine algorithmic thresholds to minimize false positives, especially for marginalized travelers.

Critics argued that participatory methods slowed down deployment. However, comparative evaluations showed that consultative processes actually improved efficiency by reducing disputes and costly litigation from misidentifications [21]. Furthermore, the legitimacy of border technologies increased significantly when communities felt they had input into the design and oversight.

Figure 2 demonstrates how participatory-informed frameworks alter the conventional linear pipeline of AI screening into a cyclical process where community feedback continually reshapes system parameters. Complementing this, Table 2 synthesizes documented case studies showing misprofiling patterns at borders and the participatory remedies applied, from data diversification to institutional accountability mechanisms. Together, these examples illustrate that AI-enabled border and airport security is most effective when grounded in participatory co-governance rather than unilateral institutional control [19].

5.3. Cybersecurity Threat Detection

AI-driven cybersecurity systems emerged as critical tools for monitoring networks, detecting intrusions, and identifying anomalies. However, misclassification remained a persistent problem. Legitimate user activities such as large file transfers, remote logins from new devices, or experimental software testing were often flagged as malicious [24]. This not only disrupted business operations but also risked stigmatizing individuals as potential threats without cause.

The roots of misclassification were both technical and institutional. On the technical side, models were trained on datasets that failed to capture the diversity of benign user behavior. Activities common in some sectors, like academic research or cross-border collaboration, were misread as abnormal due to narrow training corpora [20]. Institutionally, IT security teams often lacked structured feedback mechanisms from end-users, leading to one-sided system optimization that prioritized risk aversion over accuracy.

Participatory approaches reframed cybersecurity systems as sociotechnical infrastructures requiring ongoing negotiation between users and designers. Some organizations implemented co-validation processes, where employee representatives reviewed flagged incidents to contextualize them before punitive action was taken [22]. This reduced the number of wrongful escalations and helped recalibrate anomaly-detection models toward more nuanced understandings of acceptable risk.

Another strategy was participatory auditing, where cybersecurity algorithms were periodically evaluated not just by technical staff but also by stakeholder panels including legal advisors, privacy advocates, and user communities [25]. These audits examined both technical features and institutional practices, ensuring that cybersecurity governance was not reduced to a purely technical issue. Importantly, such mechanisms also provided redress pathways for employees wrongly accused of policy violations.

Participatory design also contributed to the development of “explainable AI” interfaces, where flagged incidents were accompanied by transparent rationales accessible to end-users [21]. Rather than obscure risk scores, users could see which behavioral features triggered alerts, empowering them to contest or clarify anomalies. This shift not only improved fairness but also fostered trust in cybersecurity systems, reducing adversarial attitudes between staff and security teams.

Empirical studies revealed that participatory-informed cybersecurity systems produced fewer false positives and demonstrated stronger resilience against adversarial attacks [23]. Moreover, user-centered engagement allowed systems to adapt to evolving work practices, such as hybrid or remote work, which traditional anomaly detection frameworks had initially struggled to accommodate.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 75 – 89, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1008

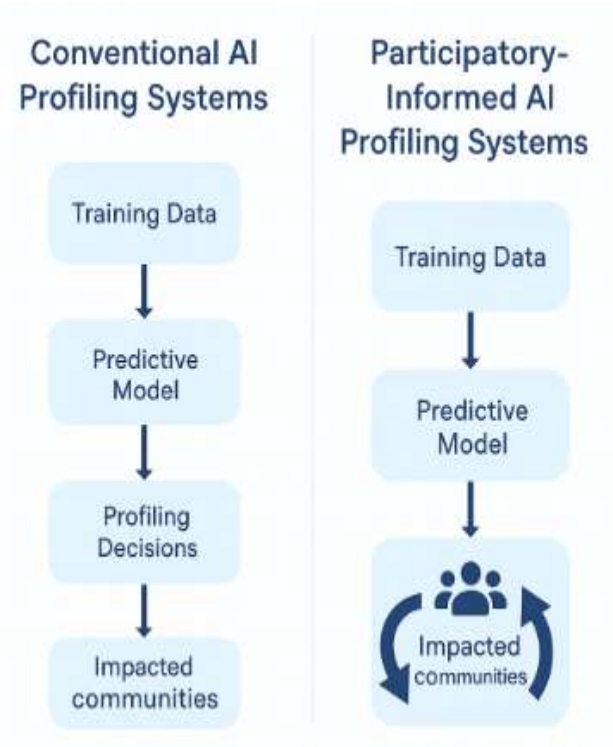

Figure 2: Comparative flow diagram contrasting conventional AI profiling systems with participatory-informed approaches that integrate community oversight across deployment cycles.

As depicted in Figure 2, participatory-informed AI profiling systems embed iterative community oversight across deployment cycles, contrasting with conventional one-directional processes. Table 2 further provides comparative summaries of misprofiling incidents in cybersecurity, outlining how participatory remedies improved detection without sacrificing security. These findings underscore that cybersecurity AI cannot be effective in isolation but thrives when continuously shaped by participatory, user-centered governance [19].

Table 2: Case studies highlighting misprofiling patterns, impacts, and participatory remedies in predictive policing systems

City/Region	Misprofiling Pattern	Observed Social Impact	Participatory Remedy Applied
Chicago, USA	Crime hotspot prediction disproportionately flagged Black and Latino neighborhoods	Reinforced racial stereotypes, increased patrol intensity, community distrust	Community roundtables with residents led to algorithm audits and revised data inputs
Los Angeles,	Predictive policing model	Criminalization of poverty,	Pilot projects introduced
USA	concentrated surveillance in low-income districts	loss of community trust in law enforcement	neighborhood councils to review and contest algorithm outputs
London, UK	Facial recognition–enabled policing disproportionately flagged youth of African descent	Wrongful stops and detentions; erosion of civil liberties	Independent oversight panels required police transparency and algorithmic impact reviews
Rotterdam, Netherlands	Risk scoring tools linked welfare recipients to fraud likelihood	Discrimination against immigrant families; stigmatization of vulnerable groups	Civil society organizations collaborated with municipalities to suspend biased scoring
Oakland, USA	Predictive models over-relied on historical arrest data	Cycle of over-policing, perpetuating systemic inequalities	City banned predictive policing tools, replacing them with community-led safety programs

6. BENEFITS AND CHALLENGES OF PARTICIPATORY DESIGN IN SECURITY AI

6.1. Benefits

Integrating participatory practices into security-focused AI systems yields significant benefits for both technical performance and broader sociopolitical legitimacy. One of the most widely recognized advantages is improved accuracy. When impacted communities contribute insights during data collection, labeling, and validation, the resulting models capture nuanced patterns otherwise overlooked by engineers or data scientists. For example, local perspectives can reveal context-specific behaviors misclassified as anomalies by generic training sets. This correction helps refine

classification boundaries and reduces systematic errors [25]. Importantly, such accuracy gains are not purely technical but embedded in social realities that enhance both system reliability and community trust.

Fairness emerges as another benefit, particularly in domains historically marked by unequal treatment. AI systems trained without participatory oversight often replicate structural biases embedded in prior datasets. Introducing co-design and participatory audits provides checks against these biases by embedding diverse voices in governance structures [28]. The perception of fairness is as crucial as measurable outcomes, since public skepticism can undermine the legitimacy of security AI even when its predictive accuracy is high. Engaging affected stakeholders builds legitimacy by demonstrating that their experiences and concerns materially influence technological design.

Another major benefit is trust-building. Security technologies inherently generate suspicion, especially when used for policing, border control, or surveillance. By involving community representatives in design decisions, governments and corporations signal a willingness to subject these systems to democratic scrutiny [24]. This openness can mitigate accusations of secrecy or authoritarianism, shifting public discourse from one of resistance to cautious cooperation. Trust, in turn, increases the willingness of individuals to interact with AI-driven systems, ultimately enhancing operational efficiency.

Reputational risk management is a further dimension of benefit. High-profile failures of security AI such as wrongful arrests or discriminatory screenings have historically attracted intense media criticism. Corporations supplying such systems risk not only financial losses but also long-term damage to credibility. Participatory practices act as safeguards by reducing the likelihood of reputationally costly errors [30]. Even when controversies arise, transparent involvement of external stakeholders provides evidence that due diligence was exercised, softening reputational fallout. For governments, avoiding accusations of discriminatory profiling is equally critical for maintaining legitimacy in democratic societies.

Participatory practices also foster adaptive, context-aware AI. Security threats evolve rapidly, and static models often degrade in performance over time. Community-driven feedback loops ensure that new threat behaviors, shifting demographics, or evolving social norms are integrated into system updates [26]. This iterative adaptation contrasts sharply with conventional “one-off” deployments that quickly become obsolete. Moreover, adaptive systems are more resilient to adversarial manipulation since participatory inputs introduce heterogeneous perspectives that anticipate previously unseen strategies.

Taken together, these benefits accuracy, fairness, trust, reputational protection, and adaptability position participatory design not merely as an ethical ideal but as a pragmatic strategy for improving performance and resilience in high-stakes domains. Importantly, these advantages extend beyond the technical sphere into the social, political, and economic arenas where AI systems operate. As Figure 3 illustrates, benefits must be evaluated against parallel challenges, requiring balanced frameworks rather than uncritical adoption. This recognition establishes the foundation for analyzing the obstacles that complicate participatory security AI.

Figure 3: Trade-off diagram illustrating the balance between benefits and challenges in participatory security AI adoption.

6.2. Challenges

Despite its promise, participatory integration into security AI presents a range of challenges that complicate adoption. One of the most immediate barriers is cost and resource intensity. Organizing workshops, running consultations, and maintaining participatory audits require significant financial investments. Governments and corporations accustomed to efficiency-driven procurement models may view these processes as unnecessary delays [29]. The time commitment is equally substantial, often slowing deployment timelines in security environments where rapid response is valued. Balancing speed with deliberative participation requires institutional restructuring, which many organizations resist.

Another challenge concerns the complexity of participatory integration. Security AI systems involve multiple stakeholders engineers, policymakers, frontline officers, and impacted communities each with distinct vocabularies and priorities. Coordinating these perspectives into actionable design choices is far from straightforward. Stakeholder disagreements can stall processes, and the technical intricacies of deep learning models may exclude non-specialists despite efforts at inclusion [24]. Bridging these divides necessitates translation mechanisms such as scenario-building exercises, yet these tools themselves require skilled facilitators and long-term commitment.

Balancing security imperatives with openness introduces another layer of difficulty. Security agencies often operate under conditions of confidentiality to protect operational strategies. However, meaningful participation requires transparency about how profiling systems function. Excessive disclosure may compromise security, while excessive secrecy undermines the legitimacy of the participatory exercise. Achieving equilibrium between these competing demands is one of the most delicate challenges in participatory security AI [26]. In practice, this tension often results in limited disclosure that reduces the depth of participation.

The risk of tokenism further complicates participatory projects. Institutions may adopt participatory processes for symbolic legitimacy rather than substantive inclusion. In such cases, stakeholders are invited to consultations without their contributions meaningfully influencing technical or policy outcomes. Tokenistic participation not only wastes resources but also risks exacerbating mistrust among communities who recognize the superficiality of the process [28]. This phenomenon has been observed in multiple pilot projects where the rhetoric of participation outstripped actual empowerment.

Another challenge lies in the scalability of participatory methods. Small-scale workshops may succeed in localized contexts, but extending these models to national or international deployments is considerably more complex. For example, AI-based border screening systems affect millions of passengers across multiple jurisdictions. Designing participatory frameworks that meaningfully incorporate this diversity remains an unsolved challenge [25]. Similarly, cybersecurity applications that operate globally face difficulties in defining which communities have standing to participate and how their voices can be systematically incorporated.

Finally, there are institutional and political resistances. Participatory approaches redistribute power by giving affected communities a voice in security decision-making. This redistribution can be perceived as threatening by agencies accustomed to unilateral authority [30]. Political leaders may fear that participatory deliberations expose them to criticisms of weakness or indecisiveness. Overcoming these resistances requires cultural change within institutions, alongside legal frameworks that mandate participatory practices rather than leaving them to discretionary adoption.

As Figure 3 demonstrates, the trade-off between benefits and challenges is not merely technical but deeply institutional. Each benefit such as increased fairness comes at the cost of potential delays or institutional resistance. The challenge is therefore not whether to pursue participatory security AI, but how to design frameworks that mitigate these obstacles while preserving the clear benefits outlined earlier. Recognizing this duality creates a balanced foundation for developing evaluative criteria and governance structures, which will be explored in the subsequent section.

7. TOWARD A FRAMEWORK FOR PARTICIPATORY SECURITY AI

7.1. Proposed Multi-Layered Framework

Designing a multi-layered framework for participatory integration into security AI requires acknowledging the intertwined nature of technical processes, governance structures, and community oversight. At the data level, community members can help identify which data categories are relevant and which may inadvertently introduce bias. This reduces risks of over-policing particular populations while enhancing contextual fidelity [29]. For example, in pilot programs where residents contributed to refining surveillance datasets, false alarm rates declined because participants highlighted locally specific patterns overlooked by automated systems. Such interventions reveal that community voices are not just ethical add-ons but practical tools for operational improvement.

At the model level, participatory approaches can shape how algorithms are trained, validated, and adjusted. Mechanisms like joint labeling workshops or deliberative review boards ensure that models reflect collective priorities rather than narrow technical imperatives [30]. Beyond technical accuracy, this fosters transparency since participants can observe where their input directly affects algorithmic outcomes. The introduction of participatory audits into model pipelines also creates an external accountability layer, ensuring developers remain responsive to end-user concerns. Without such involvement, systems risk perpetuating opaque decision-making processes that undermine legitimacy.

The deployment level requires governance structures capable of sustaining community engagement after rollout. Oversight councils, including regulators, civil society groups, and affected communities, can review AI system performance periodically. These councils act as anchors for accountability, mandating corrective action where misprofiling persists [31]. This institutionalization transforms ad-hoc consultation into structural practice. Moreover, integrating feedback loops into operational dashboards allows real-time adjustments, reinforcing the adaptability of deployed models.

The framework is best visualized in Figure 4, which illustrates a participatory ecosystem of security AI. The diagram maps interconnections between users, developers, regulators, and communities, highlighting continuous engagement channels across all lifecycle stages. This multi-actor ecosystem shows how oversight is embedded, not bolted on, ensuring participatory standards are treated as baseline requirements.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 75 – 89, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1008

Figure 4: Participatory Ecosystem of Security AI

Finally, sustainability requires building capacity among both technical actors and communities. Governments can fund participatory literacy programs, training citizens to meaningfully engage in oversight, while developers receive guidance on embedding inclusion into coding practices [32]. The framework emphasizes balance: maintaining operational efficiency while respecting democratic accountability. When deployed effectively, such a structure allows AI systems to remain both adaptive and socially legitimate.

7.2. Evaluation Metrics

Measuring the effectiveness of participatory security AI demands metrics that extend beyond technical accuracy to include fairness, trust, and inclusion. At the technical layer, fairness metrics evaluate whether false positives and false negatives are equitably distributed across demographic groups. This guards against systemic misprofiling where particular communities bear disproportionate burdens [33]. Metrics such as equalized odds or disparate impact ratios can be adapted to security contexts, ensuring both technical and ethical performance.

Equally important are trust indicators, which gauge the extent to which stakeholders perceive AI systems as legitimate. Trust can be measured through periodic surveys among communities affected by surveillance or policing tools. A system may achieve high accuracy but still fail if it generates distrust that erodes cooperation with authorities. Embedding such perception-based indicators ensures that evaluation captures social, not just computational, success.

Participatory success also hinges on representation and inclusion metrics. These measure the diversity of groups consulted during data collection, model validation, and deployment oversight. For instance, did oversight boards reflect gender, ethnic, and socioeconomic diversity? Were marginalized groups given meaningful influence in shaping system parameters? Documenting these factors avoids the pitfalls of tokenistic consultation, which reduces legitimacy and fails to capture community heterogeneity [34].

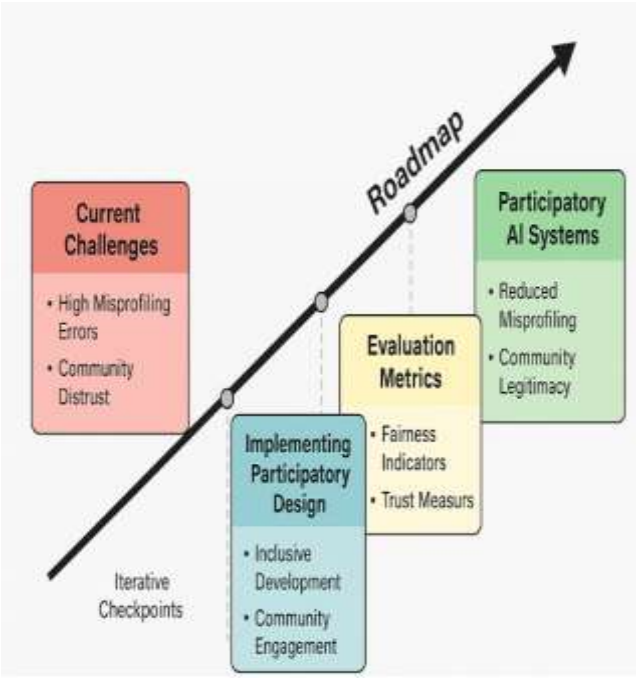

Figure 5: Roadmap from Misprofiling Challenges to Participatory AI Systems

Figure 5 illustrates a roadmap linking current misprofiling challenges to participatory-designed, fairer AI systems. The diagram shows how applying fairness and trust metrics can progressively reduce errors while strengthening community legitimacy. It highlights iterative checkpoints where evaluation is embedded into the lifecycle rather than applied post-hoc.

Finally, evaluation must remain adaptive. Security environments evolve quickly, and metrics must track shifts in both technical performance and community perception. Co-developing dashboards with stakeholders provides transparency, allowing regulators and the public to see progress and challenges in real time. In this way, evaluation metrics serve not only as measurement tools but as governance instruments that maintain accountability.

7.3. Future Integration with Policy

The long-term viability of participatory security AI rests on its integration with policy and regulatory frameworks. Embedding participatory standards into AI ethics guidelines ensures they become enforceable requirements rather than voluntary aspirations [35]. Governments can mandate participatory audits for high-risk AI systems, akin to environmental impact assessments, where societal implications are reviewed before deployment. This institutionalizes oversight, reducing the risk of unchecked technological expansion.

At the international level, harmonizing participatory standards through regional alliances can prevent fragmented practices. For example, cooperative frameworks across neighboring states could share best practices, aligning oversight structures with transnational security needs. This avoids gaps where authoritarian regimes exploit weaker governance environments to deploy opaque AI tools.

Table 3 summarizes proposed framework elements, identifies key stakeholders (developers, regulators, civil society, and communities), and links each element to measurable outcomes. By translating abstract principles into actionable policies, the table provides a roadmap for embedding participatory governance into security AI.

Ultimately, policy integration bridges theory and practice, ensuring participatory AI design is not confined to experimental pilots but becomes the norm in security governance. This sets the stage for future research on scaling participatory frameworks globally.

Table 3: Proposed framework elements, key stakeholders, and measurable outcomes for participatory governance in security AI

Framework Element	Key Stakeholders	Measurable Outcomes
Inclusive Data Governance	Developers, regulators, communities	Increased demographic representation in datasets; reduction in bias-related false positives/negatives
Transparent Model Auditing	Developers, regulators, civil society	Independent algorithmic audits published; higher public trust scores in security AI surveys
Participatory Design Reviews	Communities, civil society, developers	Documented community feedback loops; evidence of design adjustments based on participatory consultations
Accountability Mechanisms	Regulators, civil society, developers	Established redress systems for misprofiling cases; public reporting of corrective actions taken
Ethical Oversight Committees	Regulators, civil society, academic experts	Regular publication of ethical impact assessments; measurable decline in governance-related controversies
Capacity-Building Programs	Communities, civil society, regulators	Training workshops delivered; percentage increase in stakeholder literacy on AI system operations
Policy Integration Standards	Regulators, developers, policymakers	Adoption of participatory AI standards in national security guidelines; integration into regulatory codes

8. CONCLUSION

The persistent issue of misprofiling within security-focused artificial intelligence systems demands urgent attention, not only for its technical shortcomings but also for the human consequences it creates. From predictive policing to border surveillance and cybersecurity, the documented failures of AI-driven profiling illustrate a recurring pattern: systems trained and deployed without meaningful consideration of context, diversity, and community oversight often exacerbate rather than mitigate risks. Misclassification of individuals based on race, socioeconomic status, travel behavior, or digital activity does not just create false alarms; it erodes public trust, deepens societal inequities, and undermines the legitimacy of security institutions. This reality positions participatory design not as an optional add-on, but as a vital remedy for ensuring responsible, accurate, and fair security AI systems.

At its core, participatory design reframes AI from being a closed technological domain into one that integrates the lived experiences and knowledge of those most impacted by its outcomes. Engaging communities in defining what data is collected, how models are trained, and how deployment is monitored ensures that blind spots are identified early, biases are corrected, and fairness is prioritized alongside efficiency. Importantly, such involvement shifts the perception of security AI from an externally imposed tool of surveillance to a collaboratively designed system of protection. The result is not only improved technical accuracy but also enhanced trustworthiness and legitimacy in the eyes of the public.

Equally, the ethical dimensions of participatory approaches cannot be overstated. Misprofiling does not exist in a vacuum; it intersects with histories of systemic discrimination and present-day disparities in access to justice, privacy, and security. When communities are excluded from shaping these technologies, the risks of perpetuating those inequities multiply. By contrast, structured participation embodies an ethical commitment to transparency, accountability, and inclusivity. It ensures that marginalized voices are not just subjects of surveillance but active contributors to systems that affect their safety and freedom. This dual role both technical and ethical illustrates why participatory AI must be treated as a necessity rather than an experimental option.

The path forward requires embracing collaboration across domains that traditionally operate in silos. AI engineers bring expertise in algorithms, data pipelines, and system integration; policymakers contribute the regulatory frameworks, ethical guidelines, and governance standards; communities supply the contextual insight, lived experiences, and real-world feedback essential for equitable deployment. Together, these groups form a triad of responsibility that balances innovation with accountability. Without this cross-disciplinary collaboration, even the most advanced security AI risks repeating cycles of error and mistrust. With it, however, the potential emerges for systems that are not only intelligent but also just and socially responsive.

Looking ahead, the vision for participatory AI extends beyond isolated case studies or pilot projects. The aspiration is to normalize these practices as embedded standards in the development of security technologies. Frameworks that mandate participatory involvement at key stages data curation, model validation, deployment oversight, and feedback mechanisms should become a defining feature of responsible AI pipelines. Similarly, evaluation metrics must evolve to capture not just false positives or detection accuracy but also indicators of inclusivity, fairness, and public trust. These are not abstract ideals; they are practical necessities for ensuring that AI serves as a protective rather than punitive force.

Ultimately, the challenge of misprofiling reveals both the limitations of conventional AI and the transformative potential of participatory remedies. The former highlights what happens when technology is divorced from social realities, while the latter demonstrates how inclusive practices can foster accuracy, fairness, and legitimacy. The choice facing governments, corporations, and developers is therefore stark: continue down a path where efficiency is prioritized at the expense of equity, or embrace participatory design as the blueprint for responsible security AI.

The conclusion is clear. Building participatory AI is not simply about better algorithms; it is about reimagining the relationship between technology, governance, and society. It is about creating systems that reflect the values of fairness and accountability as much as they deliver on promises of safety and efficiency. By centering participation, the future of security AI can be one where innovation aligns with justice, and where communities no longer fear being misprofiled, but instead take confidence in systems designed with them and for them.

9. REFERENCE

1. Kannan K, Saha RL, Khern-am-nuai W. Identifying perverse incentives in buyer profiling on online trading platforms. Information Systems Research. 2022 Jun;33(2):464-75.
2. Onabowale Oreoluwa. Innovative financing models for bridging the healthcare access gap in developing economies. *World Journal of Advanced Research and Reviews*. 2020;5(3):200–218. doi: https://doi.org/10.30574/wjarr.2020.5.3.0023
3. Noh KW, Buettner R, Klein S. Shifting gears in precision oncology—Challenges and opportunities of integrative data analysis. Biomolecules. 2021 Sep 4;11(9):1310.
4. Romero F, Zhao M, Yadwadkar NJ, Kozyrakis C. Llama: A heterogeneous & serverless framework for auto-tuning video analytics pipelines. InProceedings of the ACM symposium on cloud computing 2021 Nov 1 (pp. 1-17).
5. Moeller J, Löecherbach F, Möller J, Helberger N. Out of control?: Using interactive testing to understand user agency in news recommendation systems. InNews Quality in the Digital Age 2023 Mar 9 (pp. 117-133). Routledge.
6. Wang Y, editor. Statistical techniques for network security: modern statistically-based intrusion detection and protection: modern statistically-based intrusion detection and protection. Igi Global; 2008 Oct 31.
7. Baruwa A. Redefining global logistics leadership: integrating predictive AI models to strengthen competitiveness. *International Journal of Computer Applications Technology and Research*. 2019;8(12):532-547. doi:10.7753/IJCATR0812.1010.
8. Sieron-Galusek D, Galusek L. Borderland: On Reviving Culture. LIT Verlag Münster; 2020.
9. Esan O. Dynamic pricing models in SaaS: a comparative analysis of AI-powered monetization strategies. *International Journal of Research Publication and Reviews*. 2021 Dec;2(12):1757-1772.DOI : https://doi.org/10.5281/zenodo.16879905
10. Anderson J, Rainie L. The future of human agency. Pew Research Center. 2023 Feb 24.
11. Ra S. Extraterritoriality in a Nevada Shipping Container: Accountability for Drone Warfare through the Post-Nestlé Alien Tort Statute. Columbia Human Rights Law Review. 2023 Mar 14;51.
12. Chai Z, Chen Y, Anwar A, Zhao L, Cheng Y, Rangwala H. FedAT: A high-performance and communication-efficient federated learning system with asynchronous tiers. InProceedings of the international conference for high performance computing, networking, storage and analysis 2021 Nov 14 (pp. 1-16).
13. Zhang T, Lee D, Jung C. Txrace: Efficient data race detection using commodity hardware transactional memory. InProceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems 2016 Mar 25 (pp. 159-173).
14. Saad MM, Mohamedin M, Ravindran B. {HydraVM}: Extracting Parallelism from Legacy Sequential Code Using {STM}. In4th USENIX Workshop on Hot Topics in Parallelism (HotPar 12) 2012.
15. Romero, Francisco, et al. "Llama: A heterogeneous & serverless framework for auto-tuning video analytics pipelines." *Proceedings of the ACM symposium on cloud computing*. 2021.
16. Guo Z, He Z, Zhang Y. Mira: A program-behavior-guided far memory system. InProceedings of the 29th Symposium on Operating Systems Principles 2023 Oct 23 (pp. 692-708).

17. Agrawal HK, Jain S, Bhadouria PS, Jain R. RECRUITMENT PROCESS: THE „HEART" OF HUMAN RESOURCES MANAGEMENT. Journal of Management Value & Ethics.:40.
18. Chan ED, Heifets L, Iseman MD. Immunologic diagnosis of tuberculosis: a review. Tubercle and Lung Disease. 2000 May 1;80(3):131-40.
19. Munoz A, Mackay J. An online testing design choice typology towards cheating threat minimisation. Journal of University Teaching and Learning Practice. 2019 Mar;16(3):1-8.
20. Jennings BM, Sandelowski M, Mark B. The nurse's medication day. Qualitative health research. 2011 Oct;21(10):1441-51.
21. Chai Z, Chen Y, Anwar A, Zhao L, Cheng Y, Rangwala H. FedAT: A high-performance and communication-efficient federated learning system with asynchronous tiers. InProceedings of the international conference for high performance computing, networking, storage and analysis 2021 Nov 14 (pp. 1-16).
22. Zhang M, He X, Yang Q. A unified, low-overhead framework to support continuous profiling and optimization. InConference Proceedings of the 2003 IEEE International Performance, Computing, and Communications Conference, 2003. 2003 Apr 9 (pp. 327-334). IEEE.
23. Mun AK. The psychology of investors' investment decision-making process: the role of emotion regulation and rumination in investment return. University of Nottingham (United Kingdom); 2023.
24. Haritha P, Uchil R. Conceptual framework on market factors affecting investor's sentiments and the effect of behavioral pitfalls on investment decision making. IOSR Journal of Economics and Finance. 2016;1(1):29-4.
25. Dietvorst E, Hiemstra M, Maciejewski D, van Roekel E, Ter Bogt T, Hillegers M, Keijsers L. Grumpy or depressed? Disentangling typically developing adolescent mood from prodromal depression using experience sampling methods. Journal of Adolescence. 2021 Apr 1;88:25-35.
26. Han JJ, Jang W. Information asymmetry and the financial consumer protection policy. Asian Journal of Political Science. 2013 Dec 1;21(3):213-23.
27. Gonzalez-Igual M, Santamaría TC, Agustín PC. Prevailing behavioral biases and investor profiles: a survey of professional investors. The Journal of Wealth Management. 2017 Dec 1;20(3):10.
28. Li D, Bissyandé TF, Kubler S, Klein J, Le Traon Y. Profiling household appliance electricity usage with n-gram language modeling. In2016 IEEE International Conference on Industrial Technology (ICIT) 2016 Mar 14 (pp. 604-609). IEEE.
29. Chan ED, Reves R, Belisle JT, Brennan PJ, Hahn WE. Diagnosis of tuberculosis by a visually detectable immunoassay for lipoarabinomannan. American journal of respiratory and critical care medicine. 2000 May 1;161(5):1713-9.
30. Balatel A, Boero R, Jonaityte I, Monti M, Novarese M, Pacelli V. Beyond the MiFID: Envisioning cognitively suitable and representationally supportive approaches to assessing investment preferences for more informed financial decisions.
31. Esan O. Strategic intelligence for SaaS innovation: leveraging business analytics to drive global competitiveness. *International Journal of Computer Applications Technology and Research*. 2018;7(12):473-488. doi: 10.7753/IJCATR0712.1009.
32. Hou X, Hao L, Li C, Chen Q, Zheng W, Guo M. Power grab in aggressively provisioned data centers: What is the risk and what can be done about it. In2018 IEEE 36th International Conference on Computer Design (ICCD) 2018 Oct 7 (pp. 26-34). IEEE.
33. Xenidis R. Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. Maastricht Journal of European and Comparative Law. 2020 Dec;27(6):736-58.
34. Kannan K, Saha RL, Khern-am-nuai W. Identifying perverse incentives in buyer profiling on online trading platforms. Information Systems Research. 2022 Jun;33(2):464-75.