DATA FOR POLICY .ORG

DATA & POLICY

Universiteit Leiden
The Netherlands

DATA FOR POLICY 2025 EUROPE

Twin Transitions in Data and Policy for a Sustainable Future

BOOK OF ABSTRACTS

12- 13 June, 2025

Leiden University, The Hague

CENTRE FOR BOLD CITIES

TNO Vector
Centre for Societal Innovation and Strategy

CAMBRIDGE UNIVERSITY PRESS

A Privacy-focused Data Solution for Understanding and Improving Indoor Environmental Quality in Social Housing From the SHINE Project.

Valesca Lima[1], Joseph Mullally[1], Tracy Mae Ildefonso[1] and Stephen Daniels[1]

1. Dublin City University

Keywords: Social housing, Sustainability, Mould, Sensors, Privacy

Abstract

The Irish social housing sector faces major challenges in improving home environments and sustainability. Ageing infrastructure, harsh weather, and inadequate management responses contribute to poor living conditions, leading to mould growth and worsening health. In a County Dublin social housing block, children and vulnerable individuals suffer from bronchiolitis, breathing issues, chest infections, and mental health decline due to mould exposure (Conneely, 2025). Despite calls for relocation, their health has already deteriorated, highlighting a widespread issue that harms residents and incurs high costs.

The Sustainable Homes Integrating Non-Intrusive Environmental Sensors Research Project (SHINE) aims to improve living conditions by identifying root causes and solutions. Through interviews with 28 stakeholders, including housing officials and residents, SHINE explores the use of non-intrusive environmental sensors in social homes. These sensors provide real-time insights, warning residents of mould risks by monitoring condensation over time. This proactive approach helps prevent issues, reducing management costs, hospital visits, and energy use. Long-term, SHINE seeks to integrate these technologies into social housing policy, promoting sustainability and better health outcomes.

Research Problem

Low-cost environmental sensors, when combined with expert-system mathematical algorithms, can be used by users to get a clear understanding of important living conditions

and the energy efficiency of their home, along with actionable recommendations to improve them. The same type of sensor systems can also be used by building management to receive notifications of different aspects of the premises that need to be repaired. However, when this proposal was presented to our stakeholders, we discovered that data privacy is amongst the top concerns of residents when it comes to indoor environmental monitoring.

As adversarial data harvesting and analytics become increasingly sophisticated, it is crucial for citizens to understand and control the information that exits their homes. Sensor readings collected within households contain sensitive privileged information. However, user data privacy in networked sensor systems is frequently overlooked in favour of over-collection and ease of implementation (Fei et al., 2023). Raw sensor readings are often transmitted to cloud servers, which analyse and disseminate information to other systems. The affordability of sensors, internet connectivity, and storage has led to a rise in the remote harvesting of sensor telemetry from household consumer electronics, contributing to large corporate datasets. While robust legal protections such as the GDPR exist, the average user is still confronted with complex and ever-changing data privacy agreements (van der Schyff et al., 2023). Additionally, user data may be vulnerable to interception in transit by uninvolved third parties. From an information security perspective, once a user's data leaves their household, it should be regarded as beyond their control.

To AI and other machine learning techniques, every bit of information collected from a user's sensors can hold statistical significance, enabling the inference of additional information about the individuals in their vicinity, their behaviours, and their environment - far beyond the original intended purpose of the sensor system. For instance, spikes in room CO_2 levels can indicate presence detection (Cali et al., 205), while pseudo-anonymization can be compromised through sensor fingerprinting (Ahmed & Mathur, 2017). When this data is fused with other datasets from grey-market data brokers (Kröger, 2019), the potential for further de-anonymization increases, providing richer insights into the user and their surroundings. In the wrong hands, this information can be used adversarially against the user —for example, through remote surveillance, manipulation via targeted advertising, or threats of eviction. Similarly, management organisations may face scrutiny due to demonstrated privacy violations against their tenants and allegations of data misuse. Hence, data privacy concerns among our stakeholders, based on this information alone, are warranted. In light of these concerns, a pertinent research question arises: How can we effectively address the challenges of data privacy and ethical usage of sensor data while simultaneously advancing our research goals?

Key Discussion

The SHINE team leveraged our stakeholders' insights in the design of a sensor, aiming to address their concerns while ensuring the effectiveness of the sensor for potential integration into an enhanced social housing management policy. This research outlines a design methodology focused on maximising user privacy in residential IoT sensor systems. By deploying analytical algorithms at the edge, the approach minimises unnecessary information transmission and storage. Furthermore, it ensures users have full transparency and local control over the capture and analysis of their sensitive sensor data, as well as control and visibility over what information is shared with external stakeholders.

The team utilises a non-intrusive sensor suite along with goal-oriented, privacy-focused analytics to continuously monitor various environmental factors such as temperature, humidity, particle counts, energy usage, VOCs, CO_2 levels, light levels, sound levels, and more within social housing. This system generates user-visible reports and recommendations, offering residents the option to share selected, minimal-information-content report data with researchers and housing authorities. By enhancing the understanding of critical parameters that affect residents' well-being and the sustainability of housing units, our research results aim to strengthen the social housing sector. The outcomes of this project are designed to inform policy interventions and facilitate the integration of smart and sustainable technologies, empowering government bodies, local authorities, and social housing tenants to tackle the intricate challenges posed by health, well-being, economic factors, and environmental concerns.

This approach acknowledges that for goal-oriented monitoring, raw sensor measurements hold limited direct value and can pose security risks that need careful management. What truly matters to residents and policy stakeholders are the outputs derived from goal-specific, long-term analytical models that they can choose to engage with (e.g., Mould Risk, Excessive Heat Loss, Over-stimulating Environment). Our design ensures that raw sensor measurements are neither stored or transmitted; instead, they are processed directly by local on-board analytical models, which generate infrequent, low-information-content high-level reports (e.g., a score ranging from 0-4 every seven days). The algorithms employed are sourced from peer-reviewed academic literature, with their implementation and behaviour within the system fully documented, transparent, and accessible to users and stakeholders alike. By ensuring that this openly auditable path is the only way that environmental data can move through the system, we aim to reassure residents that their sensitive sensor information remains within the household and that the algorithms generating environmental reports do not inadvertently exfiltrate additional hidden data signals. This system is strictly designed to produce opt-in high-level assessments and actionable recommendations aligned with policy objectives. We also apply machine learning and other statistical methods to evaluate how effectively these models avert any inferences beyond the specified measurement goals.

Conclusion

The SHINE project prioritizes health improvements while ensuring strong privacy protections to build trust and support sustainable, healthy social housing. Its data analysis policy focuses on evidence-based strategies that drive sustainable development through technology and resident collaboration. Emphasizing an interdisciplinary and cooperative approach, SHINE aims to address environmental and social challenges effectively. This strategy ensures practical implementation with measurable outcomes, ultimately improving citizens' well-being.

Reference

Calì, D., Matthes, P., Huchtemann, K., Streblow, R., & Müller, D. (2015). CO2 based occupancy detection algorithm: Experimental analysis and validation for office and residential buildings. Building and Environment, 86, 39-49.

Conneely, A. (2025, January 2021). 'It's really tough' - Tenants struggle with mould in homes. RTE Brainstorm. Accessed on: 21 February 2025.

Fei, W., Ohno, H., & Sampalli, S. (2023). A systematic review of IoT security: Research potential, challenges, and future directions. ACM computing surveys, 56(5), 1-40.

Kröger, J. (2019). Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In Internet of Things. Information Processing in an Increasingly Connected World: First IFIP International Cross-Domain Conference, IFIPIoT 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-19, 2018, Revised Selected Papers 1 (pp. 147-159). Springer International Publishing.

van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online Privacy Fatigue: A Scoping Review and Research Agenda. Future Internet, 15(5), 164.

Ahmed, C. M., & Mathur, A. P. (2017, July). Hardware identification via sensor fingerprinting in a cyber physical system. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 517-524).