Elder Law
2025, VOL. 9, NO. 2, 5-8
DOI: 10.47297/wspelWSP2515-824401.20250902

Research on the Protection of User Privacy Rights in Smart Elderly Care Models

Chuanyong Chen

School of Credit Management, Guangdong University of Finance, Guangzhou, Guangdong, 510521, China

ABSTRACT
Against the backdrop of an era where population ageing intersects with digital transformation, smart elderly care service models are accelerating their development due to their potential to enhance the quality of life and health management efficiency for the silver-haired generation. This paper focuses on the construction of privacy security systems for data subjects within smart elderly care scenarios. It first clarifies the connotations of the smart elderly care service framework, the specific privacy elements and their enabling functions within particular domains, and the unique value of their safeguarding. It then systematically deconstructs existing governance challenges: obstacles to informed consent arising from holistic data collection, risks of undermining information autonomy through algorithmic decision-making, and the absence of remedial mechanisms due to regulatory lag. A sustainable equilibrium between technological innovation and privacy rights protection can be achieved by establishing a collaborative governance framework that integrates technical defence capabilities, institutional constraints, and legal remedies.

KEYWORDS
Smart elderly care; User privacy; Privacy rights protection

1 Introduction

Human civilisation is undergoing a historic transformation toward comprehensive datafication. The penetration of digital technology has transcended economic boundaries to reshape the fundamental structure of social life, fundamentally altering individual existence and social governance paradigms. Concurrently, profound demographic shifts and the global spread of ageing are accelerating changes in intergenerational relationships and the allocation of social resources. The convergence of these two macro-historical currents has catalysed the emergence and evolution of the "smart elderly care" practice system. This model seeks to systematically resolve resource misallocation and supply-demand disconnects in traditional elderly care services through the technological integration of IoT sensing layers, big data analytics layers, and AI decision-making layers. It aims to construct a technology-enabled living landscape centred on safeguarding the dignity of older people. Yet the path to realising this technological vision is fraught with ethical challenges. The operational mechanism of smart elderly care is rooted in the continuous monitoring of elderly users' vital signs, real-time analysis of behavioural patterns, and dynamic mapping of social networks. Its functioning inherently relies on the integrated utilisation of highly sensitive personal information flows. During the implementation of this technological architecture, the silver-haired generation—a group doubly disadvantaged in terms of digital access capabilities and algorithmic resistance—faces systemic risks of drastically weakened privacy protection.

2 Foundations for Protecting User Privacy Rights in Smart Elderly Care

2.1 Definition, Models, and Evolution of Smart Elderly Care

Smart elderly care refers to an ageing services system that integrates Internet of Things (IoT) sensing technologies, edge computing resources, multi-source data modelling, and intelligent decision-making algorithms through cyber-physical systems. Its essence lies in establishing a non-physical service paradigm that achieves precision in health interventions and proactive allocation of daily living services through continuous environmental perception and biological signal capture. This system follows a dynamic evolutionary trajectory: transitioning from discrete emergency response devices (e.g., fall detectors) to integrated care networks; shifting from function-oriented hardware development to service ecosystem construction centred on older people's living environment. Typical modalities include three foundational configurations: wearable health monitoring systems, community virtual care platforms, and multidimensional management systems for smart institutions. Technological approaches are undergoing a fundamental shift: Deep learning-driven health prediction models are gradually replacing passive response mechanisms; cross-service aggregation platforms are accelerating the replacement of single-point technical solutions; and cognitive assistive technologies are enhancing user decision autonomy. Future paradigms will focus on modelling long-term health trajectories coupled with social support networks, constructing a seamless service continuum [1].

2.2 The Implications of User Privacy in Smart Elderly Care Contexts

Strengthening privacy rights protection in smart elderly care scenarios is essential across key dimensions: ethical foundations, market mechanisms, and social governance. The moral necessity stems from the equality of individual rights. As legally recognised rights holders, older people retain full autonomy over their personal information, unaffected by age or health status. Privacy protection fundamentally safeguards the basic freedom from digital surveillance and unauthorised identity labelling, reflecting a baseline respect for human dignity. Market necessity hinges on the sustainability of technological trust. Research indicates that users' confidence in data security directly impacts technology adoption rates. If elderly users and their families exhibit systemic distrust in service platforms, service abandonment rates will significantly increase, undermining the industry's foundation. Smart elderly care models lacking adequate privacy safeguards cannot operate sustainably. The necessity for social governance involves preventing and controlling new social risks. The large-scale aggregation of sensitive information, such as elderly health data and behavioural patterns, objectively makes relevant data storage systems more vulnerable targets for cyberattacks. Should a data breach occur, it could trigger chain reactions of social issues like targeted fraud and physical harm, posing substantial threats to public safety and order. Therefore, privacy protection systems hold institutional value as a source of preventive measures.

2.3 Analysis of the Necessity to Safeguard User Privacy Rights

The imperative to strengthen privacy protections in smart elderly care services manifests as an intertwining of multidimensional social values, with ethical considerations grounded in fundamental individual rights serving as the core driver. The right to self-determination over personal information, legally guaranteed to older people, remains unchanged despite physiological ageing. Safeguarding this right fundamentally involves regulating electronic surveillance practices and eliminating stereotypical data labelling to ensure equal access to dignity and rights. The United Nations Nairobi Declaration on Ageing explicitly states that the primary manifestation of age discrimination in the digital age is the deprivation of data autonomy. The sustainability of industry development is deeply intertwined with trust-building. Some silver-haired households cite privacy leakage risks as their primary reason for rejecting services. The spread of this trust deficit ultimately creates a dual market dilemma: shrinking end-user acceptance and sharply rising commercial costs for service providers, rendering the industry value chain unsustainable. From a public interest perspective, smart elderly care systems embed novel risk factors. Databases aggregating health records, daily activity patterns, and residential information are widely recognised as prime targets for cybercriminals. Data breaches often trigger multi-tiered consequences: initial theft enables precision fraud, which evolves into targeted attacks on vulnerable seniors, ultimately spreading social panic. This necessitates regulatory frameworks with proactive prevention capabilities, rather than relying on reactive remedies.

3 Core Challenges to User Privacy Rights in Smart Elderly Care

3.1 Data Leakage Risks Across the Entire Lifecycle

Substantial privacy leakage risks exist during the data collection phase of smart elderly care services. To support intelligent functionality, systems rely on densely deployed environmental sensing devices and wearable terminals to implement continuous, panoramic monitoring. This round-the-clock, ubiquitous data capture model renders traditional informed consent mechanisms—based on one-time authorisation—largely formalistic. Elderly users often encounter cognitive barriers when initially reviewing agreement texts, struggling to accurately comprehend the scope of data collection, its duration, and final application scenarios—significantly diminishing their substantive control. During data transmission and storage, inadequate implementation of encryption protocols and access control layers leaves highly sensitive information vulnerable to unauthorised interception over public networks or illegal access due to storage facility security flaws. Data application processes harbour multi-party interaction risks. Without granular permission allocation and operational traceability systems, diverse entities—including service providers, hardware vendors, and operators—may trigger unauthorised access, unpermitted replication, or even data circulation within black-market supply chains [2].

3.2 Discrimination and Fairness Issues in Algorithmic Decision-Making

Intelligent decision systems driven by large-scale data analysis induce novel risks of fairness rights violations. Algorithmic models in elderly care scenarios construct user profiles based on health metrics, economic capability maps, and behavioural pattern logs—a process that may trigger systemic exclusion. A typical example involves categorising elderly individuals with low activity levels and weak social connections as low-priority service recipients, thereby restricting their access to care resources. Such decision-making processes essentially constitute opaque black-box

operations. Individuals face cognitive barriers: they cannot understand the logic behind decision formation, lack the basis to question or evaluate outcomes, and lose effective channels for appeal or redress. Deeper risks stem from structural biases in training data—the absence of chronic disease patient samples leads to algorithmic outputs with systemic discrimination, amplifying marginalised groups' exclusion through technological means. Such technological alienation not only violates procedural justice principles but also becomes a digital enabler of real-world social inequality [3].

3.3 Lagging and Inadequate Existing Legal and Ethical Norms

The current privacy governance challenges in smart elderly care stem from the slow iteration of regulatory frameworks. While existing legal frameworks establish foundational principles for personal information protection, there are significant gaps in rules tailored to specific scenarios. Spatial behavioural fusion data generated by home sensor networks lack statutory criteria for determining sensitivity levels; derivative data assets required for AI training remain unregulated in terms of rights attribution. Legal mandates for algorithmic transparency lack concrete parameter systems, leaving the scope of service providers' decision-making autonomy ambiguous. The ethical dimension reveals a dual deficiency: neither has an ethical assessment paradigm specific to service scenarios been established, nor does an industry-consensus behavioural code provide a binding framework. This institutional vacuum enables a technology-driven model to prevail in corporate practices, relegating privacy security to a secondary consideration in commercial value rankings. The effectiveness of this self-regulation-dominated safeguarding model remains questionable.

4 Strategy Development for Protecting User Privacy Rights in Smart Elderly Care

4.1 Formulating Detailed Privacy Policies and Industry Standards for Smart Elderly Care

Precision-oriented institutional regulations must be established for the smart elderly care service system. It is recommended that industry regulators collaborate with enterprises, academic organisations, and user groups to develop a legally binding, specialised privacy governance framework. This system should be built upon privacy-by-design principles, mandating service providers to integrate privacy protection as a core architectural element during initial technical development. Implementation plans must encompass these key dimensions: First, establish necessary boundaries for data collection, prohibiting the gathering of non-functional, non-essential information. Second, age-friendly authorisation protocols using multimodal declarations should be developed to enhance elderly users' informed consent capabilities. Third, implement a three-tier classification system for sensitive data, applying risk-based differentiation in encryption strength, access control matrices, and audit requirements. Standardised operational paradigms should govern the entire data processing lifecycle [4].

4.2 Strengthening the Data Security Technical Protection System

The effective realisation of institutional efficacy requires a comprehensive technical implementation pathway. A defence system covering sensing endpoints, transmission layers, and application platforms should be constructed: Terminal device layer: Mandatory integration of security baseline capabilities, including device authentication mechanisms, firmware signature verification, and local data encryption modules.Transmission channel layer: Deployment of quantum key distribution or homomorphic encryption technologies to achieve transmission non-repudiation in dynamic network environments. At the cloud platform layer, adopt a zero-trust architecture model combined with distributed ledgers to build cross-domain audit trail capabilities. The core breakthrough lies in strengthening privacy-enhancing technology integration: employ differential privacy injection schemes to ensure group analysis feasibility, utilise federated learning architectures for cross-domain knowledge sharing, and leverage secure multi-party computation for data value extraction. This technical framework fundamentally creates data obfuscation, achieving a dialectical unity between analytical requirements and privacy protection.

4.3 Enhancing Legal and Regulatory Support for User Privacy Rights Protection

The sustainable development of smart elderly care requires judicial systems to provide definitive safeguards. At the legal empowerment level, regulations should be enacted to establish core institutional innovations, including deterrent mechanisms such as strict liability attribution principles for service providers, double punitive damages benchmarks, and mandatory third-party privacy certification. Regarding regulatory implementation, establish a Smart Elderly Care Data Ethics Committee to exercise four statutory functions: comprehensive review of privacy impact assessments, verification of algorithmic decision-making explainability, monitoring of data compliance operations, and dispute mediation. Remedial pathways should focus on judicial process improvements, including establishing expedited class action

channels for elderly groups, prosecutorial public interest litigation support mechanisms, and specialised data arbitration tribunals. This multidimensional framework achieves closed-loop protection of privacy rights through the synergistic integration of legislative empowerment, administrative oversight, and judicial remedies [5].

5 Conclusion

As a technological solution to population ageing, smart elderly care exhibits a structural symbiosis between developmental prospects and privacy risks, rooted in technology's inherently value-laden nature. When sensing devices and algorithmic decision-making become deeply embedded in the living environments of older people, the societal consequences of technology are fundamentally determined by institutionally constructed ethical calibration systems. Current practices reveal systemic flaws—including lack of data control, algorithmic opacity, and lagging regulatory frameworks—that constitute critical bottlenecks hindering the realisation of technological dividends. This necessitates: Reshaping data sovereignty through age-friendly authorisation mechanisms. Building defensive resilience with cryptographic systems and privacy-enhancing technologies. Reducing rights enforcement costs via legal innovation. Ultimately, achieving the dialectical unity of intelligent extension and dignity preservation.

About the Author

Chuanyong Chen, Ph.D., Lecturer. Research Interests: Civil Law, Health Law.

References

[1] Zhang Donglin. Research on the Development of "Smart Elderly Care" in the Context of the Silver Economy [C]//China Bandy Federation (CBF), Macau Sports Conditioning Association (MSCA), Guangdong Sports Conditioning Association (GSCA). Proceedings of the 15th National Conference on Sports Conditioning Science (Part II). School of Physical Education, Yunnan University; 2025:352-355.

[2] Luo Zhangwei. Research on Smart Elderly Care Service Models and Development Pathways in Urban Communities from an Ecosystem Theory Perspective [J]. Heilongjiang Science, 2025, 16(01): 1-6.

[3] Long Jianhui. Ethical Challenges of Artificial Intelligence in Smart Elderly Care and Governance Strategies [J]. Guangdong Economy, 2025, (01): 24-28.

[4] Shi L. Y., Li Q., Guliziba J. M., et al. Development Challenges and Pathways for Rural Smart Elderly Care in the Context of Digital Intelligence: A Case Study of a Village in Central China [J]. Rural Economy and Technology, 2025, 36(14): 162-165.

[5] Guo Yuhang, Du Zhengqiang, Chen Jie, et al. Exploring the "AI+" Smart Elderly Care Service Model in the Chengdu-Chongqing Economic Circle [J]. Chinese Journal of Sanatorium Medicine, 2025, 34(08): 20-26.