

Structural Design of the Market-Based Personal Data Protection Industry

Yeji Choi¹ and Hangbae Chang^{2,*}

Abstract

The rise of the data economy has dramatically expanded the use of personal data and intensified the need for secure data management and protection. To address this, we developed a taxonomy that systematically defines and analyzes the structure and functions of the personal data protection industry. Using a top-down approach, we first compared classification systems from major institutions to establish an upper framework. We then applied this framework to classify actual market cases of personal data protection products and services and refined the taxonomy through expert validation. The final model categorizes the industry into two primary divisions—Personal Data Protection Solutions and Personal Data Protection Services—with detailed subcategories, including Safe Utilization Solutions, Data Subject Rights Assurance Solutions, and Security Assurance Solutions. This taxonomy not only reflects the technical and managerial mechanisms applied in practice but also aligns with regulatory standards such as South Korea's Personal Information Protection Act (PIPA), enabling it to provide practical guidelines for organizations and policymakers seeking to enhance data protection strategies.

Keywords

Data Protection Solutions and Services, Industry Taxonomy, Market-Based Classification, Personal Data Protection Industry

1. Introduction

The advent of the data-driven economy has made personal data protection a critical socioeconomic issue globally. As data has become a key asset driving economic growth, the secure and efficient use of personal data has become an urgent priority. This is especially important because personal data accounts for the majority of data handled across industries. The widespread adoption of generative artificial intelligence (AI) and resulting incidents have heightened public concern regarding the safe handling and use of personal data. Indeed, the accelerating pace of technological advancement makes the development and implementation of legal, policy, and technical approaches to personal data protection even more urgent.

Despite its importance in developing effective strategic responses, a comprehensive taxonomy of the personal data protection industry is still lacking. Previous studies have attempted various approaches but have not successfully built a systematic model that captures the overall structure of the industry and the diversity of solutions available in the market. To fill this gap, this study analyzes the actual products and services currently available in the market and uses this real-world market data to develop a top-down

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Manuscript received September 9, 2025; first revision November 19, 2025; accepted March 5, 2026.

*Corresponding Author: Hangbae Chang (hbchang@cau.ac.kr)

¹ Department of Convergence Security, Chung-Ang University, Seoul, Korea (yji9783@cau.ac.kr)

² Department of Industrial Security, Chung-Ang University, Seoul, Korea (hbchang@cau.ac.kr)

framework-based structured taxonomy of the personal data protection industry.

In this study, we designed a taxonomy that classifies the overall structure of the personal data protection industry. First, we compared and analyzed existing technology classification systems to extract relevant criteria applicable to this domain. Based on the derived criteria, we developed an upper-level framework, which we then used to collect and categorize real-world personal data protection product and service market data. We then conducted expert interviews to refine and ensure the validity of the resulting taxonomy. This process enabled a final taxonomy that effectively represents the industry's overall structure.

Applying a top-down framework grounded in market realities, this study defines the structure and functions of the personal data protection industry. This market-oriented approach generated a model that should serve as a practical and systematic foundation for advancing the industry and developing related policies. Indeed, our exploratory analysis should deepen scholarly understanding of the field and provide a theoretical and practical basis for future empirical research and policy decisions. In addition, our findings may serve as a useful reference for the development of relevant technologies and services and foster international collaboration in the personal data protection industry.

2. Related Work

2.1 Related Industries

The Oxford English Dictionary [1] defines the term “industry” as “a particular form or sector of productive work, trade, or manufacture.” Similarly, the Cambridge English Dictionary [2] describes industry as “the companies and activities involved in the process of producing goods for sale, especially in a factory or special area.” These definitions emphasize the structural nature and economic role of industries.

Thus, an industry can be defined as a group of firms that engage in economic activities of a similar nature. From a structural perspective, every industry creates economic value through the efficient allocation of labor, capital, and technology, and promotes technological innovation [3]. However, the passage of time and shifts in the economic environment alter the scope and boundaries of industries, as technological advances and changes in market demand and policy necessitate reorganization or expansion [4]. For example, the shift from film to digital technology has redefined the structure of the photography industry. This shows that technological advances and consumer demand can significantly influence how an industry is defined and understood [5].

In the early stages of the information age, the information security industry was regarded as part of the broader information industry. However, advances and market expansion in security-related fields led to the division of the information industry and the information security industry into independent, separately managed sectors. A similar shift is now occurring in the personal data protection industry. Long treated as a subdomain of information security, the advent of the data-driven economy has led to a rapid increase in demand for privacy. This shift has highlighted the need to categorize and manage the personal data protection industry as a distinct sector [6,7]. When the personal data protection industry is incorporated into other sectors, it becomes difficult to define its scope and manage it effectively. This approach also fails to fully reflect the industry's growth and distinct characteristics. From a policy perspective, the independent management of the personal data protection industry is both reasonable and necessary; it clarifies the boundaries between industries and supports the development of targeted policies and management strategies aligned with each industry's specific features.

This historical background and policy evolution provide an important foundation for the analysis in this section. By systematically examining the similarities and differences between the personal data

protection industry and other sectors, we aim to establish a clear rationale for managing the personal data protection industry as an independent industry.

2.1.1 Data industry

The data industry comprises a broad set of activities that generate economic value through the collection, storage, processing, analysis, and use of data. Recent technological advances have reduced the cost of data collection, leading to a rapid increase in data volume and a corresponding expansion in its range of applications [8]. These developments have paved the way for the active utilization of data across various sectors. In parallel, the emergence of data marketplaces has fueled more sophisticated development in the industry [9]. These data industries build efficient ecosystems that support data trading and data-driven economic activities, facilitate collaboration among enterprises by optimizing data sharing, and create a more efficient economic structure by facilitating cross-industry data exchange [10].

A key feature of the data industry is its coverage of the full data lifecycle: generation, collection, storage, processing and analysis, and utilization. This integrated process enables the industry to enhance data-driven decision-making and improve overall competitiveness [11]. In particular, the data industry is closely linked to advanced technologies such as the Internet of Things, cloud computing, big data analytics, and AI—technological advances that continue to expand data processing and utilization abilities.

In terms of both data use and data protection, the data industry is closely related to the personal data protection industry. While the data industry prioritizes the maximization of data's economic value, the personal data protection industry focuses simultaneously on ensuring the safe use of data and preserving individual privacy. Thus, for instance, projects that use big data analytics to predict consumer behavior or deliver personalized services should also emphasize privacy protection and data de-identification [6]. Indeed, this fundamental divergence in priorities demonstrates that, despite their independence, the two industries can have a complementary relationship.

The data industry plays a key role in the modern economy, serving as a foundation for the advancement of a wide range of technologies and industries, and a personal data protection industry that ensures a balance between data utilization and privacy is essential for the sustainable growth of the data industry [12].

2.1.2 Information security industry

The information security industry encompasses a range of technologies, services, and infrastructures designed to ensure the confidentiality, integrity, and availability of information. Aiming primarily to protect data from unauthorized access, data breaches, and cyber threats [12,13], the industry's main components include network security, application security, cloud security, data protection, and security operations [14].

The industry offers tools and services to prevent data leakage, damage, and unauthorized access, and is generally divided into three areas: information security, physical security, and convergence security. Information security focuses information in computer and network systems from leaking or being compromised. Its products and services include physical or software-based tools that safeguard organizational data, networks, and systems, and professional support for security operations, monitoring, incident response, and consulting, respectively [15].

The physical security industry includes products and services that prevent disasters, crimes, and other risks across physical environments. Physical security products and services include hardware and technical solutions for protecting buildings, facilities, and assets, and personnel-based protection and monitoring of facilities and assets, along with the deployment and upkeep of security systems, respectively [16].

Finally, the convergence security industry includes products and services that facilitate the convergence of IT and non-IT industries, such as automotive security, aviation and maritime security, as well as convergence markets between non-IT industries [17,18]. However, security technologies embedded in non-IT industries within the convergence security industry are difficult to measure and may be overestimated depending on the scope of market analysis. Therefore, the information security industry is generally divided into the information security and physical security industries [19].

Although the information security industry and the privacy industry may appear similar, their protective emphases and aims differ [20]. The information security industry aims to protect organizations' entire information infrastructures by ensuring confidentiality, integrity, and availability. It employs technologies such as encryption, intrusion detection systems (IDS), firewalls, and security operation centers (SOCs) [15]. In contrast, the personal data protection industry focuses on protecting privacy throughout the data lifecycle—including the collection, storage, processing, and use of personal data. This industry deploys solutions such as data anonymization, privacy-enhancing technologies (PETs), and consent management systems, developed in response to legal requirements such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Personal Information Protection Act (PIPA) [21-23].

The information security industry provides the technical foundation for the personal data protection industry. Some privacy solutions are implemented using encryption, access control, and more, all of which fit the category of information protection technologies. Therefore, effective personal data protection requires the integration of information security capabilities [24].

Despite their close technical relationship, the two industries differ in focus and scope. The information security industry emphasizes the protection of systems and networks through technical means, whereas the personal data protection industry prioritizes the safeguarding of individual privacy and regulatory compliance. Thus, while the two industries are interrelated, they require distinct strategies and management frameworks tailored to their specific goals and operational contexts.

2.2 Personal Data Protection Industry

Personal data includes any information relating to an identified or identifiable natural person, including information that can directly (e.g., name, identification number, location data) or indirectly (e.g., biometric, cultural, or economic data) identify an individual [25]. Personal data protection technologies are designed both to prevent breaches, leaks, and misuse during the processing of personal data and to support data subjects' right to informational self-determination. Examples include data de-identification techniques, consent management systems, and access audit mechanisms. Unlike general information security tools, these technologies prioritize the management of user consent and preferences and the secure storage, transfer, and processing of data. They also support legal compliance and enable anonymization, minimizing the risk of re-identification while maintaining data utility [23,24,26].

Collectively forming the functional basis for personal data protection, these technologies are packaged into solutions and services. Accordingly, the personal data protection industry refers to the development, production, and provision of products and services that focus on protecting personal data throughout its lifecycle—collection, use, storage, transfer, and disposal—while preventing unauthorized access or exposure [27, 28].

According to Gartner [29], 75% of the global population is now subject to privacy regulations. In this regard, data localization, privacy-preserving computation, AI governance, centralized user experiences, and human-centered approaches to privacy are expected to shape the personal data protection industry. These changes increase the need for organizations to strengthen both managerial and technical measures to protect personal data.

However, previous studies have tended to analyze privacy-related industries as part of the broader information security industry, limiting its independent scope and classification. Jentzsch [27] emphasized

that research on cybersecurity and privacy markets has been fragmented, and systematic examinations of the personal information product market are notably lacking. Meanwhile, the Future of Privacy Forum [28] pointed out that the lack of common terminology for privacy technologies and inconsistencies in defining which technologies and services belong in the privacy tech sector make market analysis and policymaking significantly more difficult. This highlights the urgent need to define the privacy technology industry as an independent industry and develop a consistently applicable industry classification system. In addition, a market-oriented approach that classifies privacy technologies based on the business needs they address may help clarify their functions and provide a more effective foundation for policymaking and industry support.

3. Methodology

3.1 Research Design

Top-Down Analysis is an approach that identifies the structural characteristics of an entire system by taking high-level theoretical knowledge as a starting point and applying it step-by-step to lower-level elements [30]. For example, Hanna [31] employed a top-down analysis to recursively classify bull and bear market states, thereby identifying stable turning points. Similarly, Callon et al. [32] used a top-down approach grounded in existing SDM coding systems and theoretical models to systematically extract key elements and missing domains in clinical decision-making dialogues.

In this study, we employed a top-down analysis to develop a systematic classification of the personal data protection industry by first establishing an upper framework and then applying it to real-world market data. Our research design consists of three main stages: (1) Establishing the Upper Concept (Theoretical Framework), (2) Lower-level Case Classification, and (3) Deriving the Personal Data Protection Industry Taxonomy. This sequential approach enables us to integrate theoretical and practical data and thereby develop a comprehensive understanding of the industry's overall structure. Fig. 1 illustrates the full research workflow, showing the linkages and integration processes across all stages.

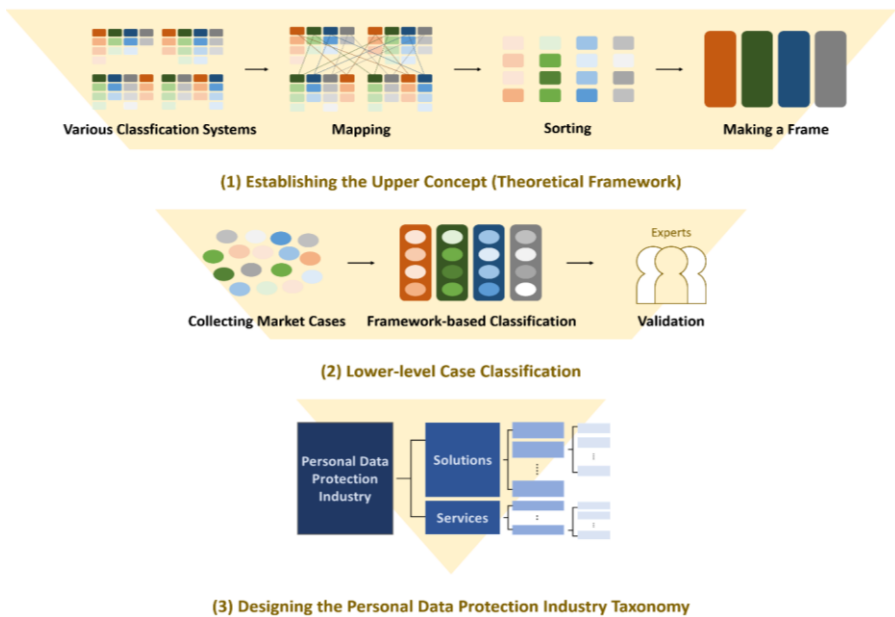


Fig. 1. Research workflow using a top-down approach.

3.2 Research Procedure

In this study, we applied the three-stage top-down analysis outlined in Fig. 1 to develop a taxonomy of the personal data protection industry. In the (1) Establishing the Upper Concept (Theoretical Framework) stage, we compared and analyzed relevant literature and existing technology classification systems to identify key classification criteria applicable to the personal data protection industry. In constructing the preliminary classification framework (Upper Framework), we drew on existing classification systems that have been systematically developed to operationalize the data protection laws and policies of various jurisdictions. As this framework is grounded in legal and institutional arrangements rather than in specific technologies, it provides a stable point of reference despite changes in the technological environment and furnishes a basis on which the taxonomy can be flexibly elaborated by refining and expanding its functional categories as new technologies and services emerge. This process involved a review of academic papers, policy reports, and industry analyses, from which we synthesized the technical and functional elements emphasized in each source. We then selected and systematized the core elements that appeared consistently across sources into an upper-level concept capable of representing the overall structure of the personal data protection industry. This resulted in the development of a theoretical framework that captures the industry's main structural and functional dimensions.

Next, in the (2) Lower-level Case Classification stage, we used the Upper Framework established in stage (1) to collect and classify real-world data on personal data protection products and services. We gathered market examples from sources such as company announcements, industry reports, and official websites and used the major classifications defined in the framework to review and categorize their technical characteristics and functions. During this process, we evaluated each case for alignment with the theoretical structure and refined subcategories as needed based on functional distinctions. To enhance the validity of the preliminary taxonomy, we also conducted in-depth interviews with experts in the privacy and security fields. These experts provided feedback on the appropriateness of the classification criteria, the consistency of the results, and the extent to which the taxonomy reflected the overall industry. Based on their feedback, we revised and clarified ambiguous or insufficiently defined categories. This process strengthened the validity of the initial classification and ensured closer alignment between theoretical standards and practical needs.

Finally, in the (3) Designing the Personal Data Protection Industry Taxonomy stage, we developed the finalized taxonomy by integrating the Upper Framework, the classified market cases, and the expert-validated preliminary taxonomy. After reviewing each classification item to assess how the relationships between the categories and the industry roles and functions they represent, we established a comprehensive taxonomy that clearly defines the structure and functions of the personal data protection industry.

In sum, through the sequential execution of (1) Establishing the Upper Concept, (2) Lower-level Case Classification, and (3) Designing the Personal Data Protection Industry Taxonomy stages, we systematically developed a taxonomy that should contribute to the advancement of policies and technologies for the secure use and protection of personal data in the data-driven economy.

4. Results and Discussion

4.1 Establishing the Upper Concept (Theoretical Framework)

In the Establishing the Upper Concept (Theoretical Framework) stage, we analyzed and compared classification systems related to the personal data protection industry across five major institutions: Organization for Economic Co-operation and Development (OECD) [23], Personal Information Protection

Commission (PIPC) [33], Federal Reserve Bank of San Francisco [34], Office of the Privacy Commissioner of Canada (OPC) [35], and European Union Agency for Cybersecurity (ENISA) [24].

We initially grouped the subcategories derived from each classification system based on their functional purposes and roles, incorporating elements commonly emphasized across the institutions. As shown in Table 1, we thereby established a theoretical framework comprising nine groups.

Table 1. Top-down analysis result

Group	Item
(A) Data De-identification and Synthesis	Anonymization / Pseudonymization
	Synthetic data
	Differential privacy
	Foundational Technologies
	Anonymization
	Pseudonymization
	Differential Privacy
	Synthetic Data
	K-Anonymity and its extensions
	Differential privacy and related models
	Masking
(B) Data Encryption and Secure Computation	Synthesis
	Zero-knowledge proofs
	Homomorphic encryption
	Multi-party computation (including private set intersection)
	Trusted execution environments
	Federated learning
	Distributed analytics
	Threshold secret sharing
	Foundational Technologies
	Encryption
	Homomorphic Encryption
	Multi-party Computation
	Data Dispersion
	Database encryption
	Property preserving encryption
	Structured encryption
	Homomorphic encryption
	Secure multi-party computation
(C) Data Protection Governance Management	Accountable systems
	Protection System Throughout the Personal Data Lifecycle
	Management Interfaces
	Sticky policies
	Websites not collecting personal info
	Private browsing mode
	Platform for Privacy Preferences Project (P3P)
	Policy aware web
	Privacy policy enforcement
	Privacy preferences and sticky policies

Continued on the next page.

Table 1. Continued

Group	Item
(D) Personal Data Disposal	Disposal Privacy eraser
(E) Identity Management and Access Control	Data Subject Identity Authentication and Information Management Digital Identity Attribute-Based credentials Enterprise digital rights management Granular access control
(F) Data Subject Rights Assurance	Personal data stores / Personal information management systems Data Subject Rights Protection System Data Subject Consent Data Subject Control Rights Personal Data Protection in MyData Self-sovereign identity Personal Information Management Systems (PIMS) Web transparency tools Access My Info (AMI) Consent mechanisms Personal data stores
(G) Personal Data Collection and Detection	Collection Data tagging Transparent accountable datamining initiative
(H) Secure Use of Personal Data	Safe Utilization System Use and Provision Privacy Protection in Data Convergence Service Applications Privacy Protection in AI Services Ephemeral communication tools Trust Mark Tor
(I) Personal Data Breach Prevention	Response to Personal Data Breaches Planning and Design Applying the PbD Principle Security Assurance Privacy Enhanced Hardware Network monitoring Endpoint event detection Oblivious RAM Accountability and audit mechanisms Data provenance

4.2 Lower-level Case Classification

In the Lower-level Case Classification stage, we used the previously established Upper Framework to classify real-world market data. After collecting 365 personal data protection products and services from corporate reports, industry publications, and official websites, we carefully analyzed the technical features, functions, and areas of application of each case. Our analysis identified 94 distinct functions, which we grouped into 14 preliminary categories based on functional similarity. This process involved

evaluating the technical and functional characteristics of each product and service to assess their alignment with the criteria defined in the Upper Framework. Based on this evaluation, we derived the initial industry taxonomy presented in Fig. 2.

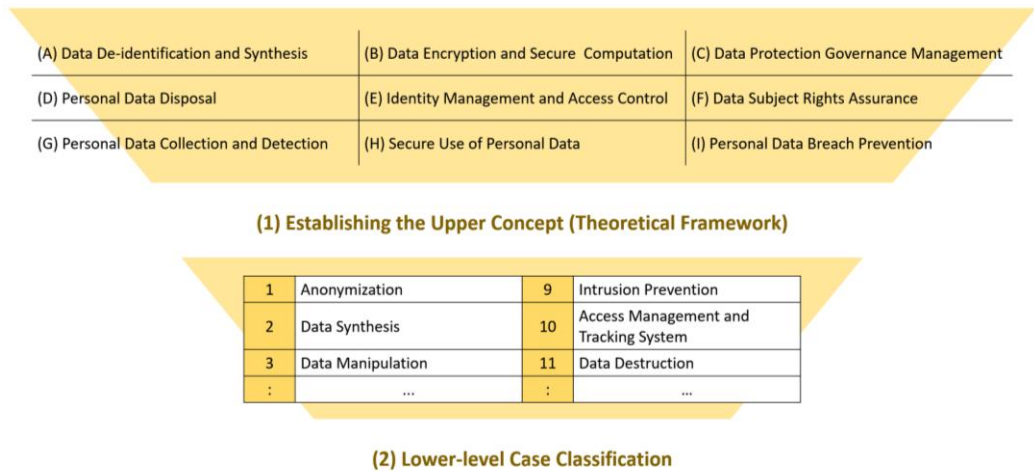


Fig. 2. Initial industry taxonomy result.

During the classification of real-world market data, we reorganized the Upper Framework’s initial nine categories—using processes of refinement, integration, and segmentation—to better reflect market realities. Since the market analysis indicated that separating solutions from services allows for clearer categorization by product group and function, we added Management Services and Technical Services as distinct classifications (see Fig. 3).

- (A) Data De-identification and Synthesis initially encompassed techniques for removing or modifying personal identifiers to reduce re-identification risk and for generating synthetic data. However, our analysis of real-world market cases revealed that many solutions offered pseudonymization and anonymization as distinct features, often alongside data synthesis capabilities using similar techniques. In addition, data merging—combining different data sources—emerged as a key function in several solutions. Accordingly, we refined category (A) into four specific subcomponents: Pseudonymization, Anonymization, Data Synthesis, and Data Merging.
- (B) Data Encryption and Secure Computation initially covered both encryption and secure computation techniques. However, our market analysis revealed encryption to be the most widely adopted technology in the market and indicated that secure computation is embedded within encryption-based or AI-powered privacy protection solutions rather than existing as a separate category. As a result, we redefined (B) to emphasize Data Encryption as the core function, with Secure Computation integrated into associated technical services.
- (C) Data Protection Governance Management originally encompassed overall privacy management and policy compliance within organizations. However, our market analysis showed that Consent Management for data collection and use and User-Centric Data Management for data subject control are distinct functions. We also found that Privacy Management Services frequently serve as organizational tools for overseeing comprehensive privacy programs. Accordingly, we divided (C) into two subcategories: Consent Management and User-Centric Data Management.
- (D) Personal Data Disposal initially referred to the secure deletion of personal data [36]. In practice, this function is commonly labeled Data Destruction, an adjustment of terminology that leaves the concept

itself unchanged.

- (E) Identity Management and Access Control originally combined identity verification and access control. However, our analysis of real-world cases revealed a clear distinction between Authentication and Access Management and Tracking Systems. As a result, we split (E) into two separate categories to better reflect the functional characteristics of each solution.
- (F) Data Subject Rights Assurance initially defined covered the full scope of data subject rights. However, in practice, we found that consent management and user control are offered as separate solutions. Since we already reclassified these functions under category (C), we removed (F) as an independent category and integrated it into the relevant subcategories.
- (G) Personal Data Collection and Detection initially included both data collection and detection functions. However, in the market, collection is typically addressed through consent management tools, while detection is embedded in solutions such as Intrusion Prevention or AI-based Privacy Protection. As a result, we eliminated (G) as an independent category and integrated it into other relevant groups.
- (H) Secure Use of Personal Data initially encompassed solutions for the safe use of personal data. However, our market analysis revealed a stronger focus on applying technical safeguards such as Data Encryption and Access Management, as well as AI-based Privacy Protection tools for real-time monitoring and protection. As a result, we did not retain (H) as a standalone category but instead integrated it into relevant technical groups or reframed it under AI-based solutions.
- (I) Personal Data Breach Prevention originally included breach prevention capabilities. In practice, however, we found that this function is primarily implemented through network and system-level Intrusion Prevention. Access Management and Tracking Systems, as defined in category (E), and robust Data Encryption also play complementary roles in preventing breaches. Accordingly, we broke (I) down into more specific technical functions such as Intrusion Prevention, replacing the broad concept of breach prevention with implementable categories.

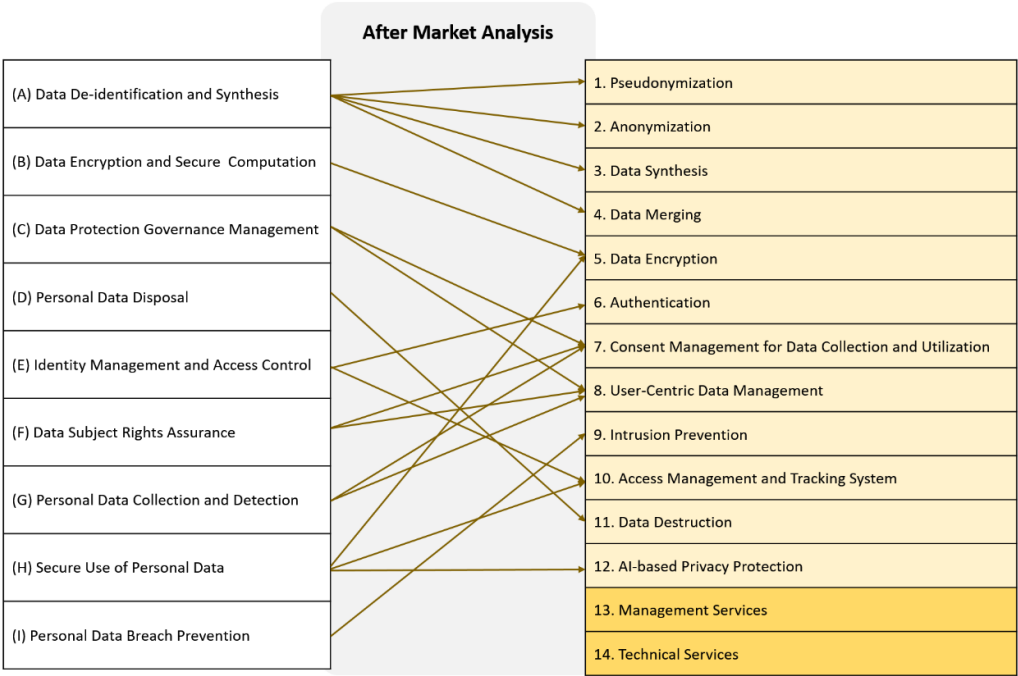


Fig. 3. Changes in the classification framework based on market analysis.

Subsequently, we conducted in-depth interviews with three experts who have extensive personal data protection experience: Expert A from the private sector with over 30 years of experience, Expert B from academia with over 20 years, and Expert C from a government agency with more than 15 years. To mitigate potential bias arising from reliance on a single sector, the expert panel was deliberately composed to encompass perspectives from the private, academic, and public/regulatory domains, which collectively represent the major stakeholder groups in the personal data protection market. During the interviews, the experts evaluated the validity of the 14 preliminary categories derived from the Lower-level Case Classification as actual personal data protection products or services. They also assessed whether the grouping based on functional similarity appropriately reflected shared purposes and roles. For items deemed misclassified, the experts provided suggestions for more appropriate categorization. They also shared broader feedback on the overall taxonomy and proposed ways to enhance its practical relevance by aligning it more closely with the Enforcement Decree of the PIPA.

4.3 Designing the Personal Data Protection Industry Taxonomy

In this study, we designed a final taxonomy that represents the overall structure and functions of the personal data protection industry by synthesizing the established Upper Framework, classification results from real-world market cases, and expert validation. In the drafting stage, we reexamined the relationships among key functional elements of the industry based on the theoretical framework and real market data. We also incorporated feedback from expert interviews to refine the definitions and categorization criteria. The experts provided insights regarding how well each category reflected field requirements by mapping them to the Enforcement Decree of the PIPA, enabling us to revise and clarify redundant or ambiguous items in the initial taxonomy.

As a result, we reorganized the 14 preliminary items from the Upper Framework and market classification into 8 subcategories. To reflect the nature of offerings in the personal data protection industry, we divided the top-level categories into two groups: Personal Data Protection Solutions and Personal Data Protection Services. This distinction was based on the fundamental differences in the roles and delivery methods of solutions and services, as well as the legal separation of technical and managerial measures defined in PIPA.

In the next step, we consolidated subcategories identified as overlapping or highly similar into unified classifications. We grouped technologies supporting safe data use, such as de-identification, under Safe Utilization Solutions in alignment with PIPA's safety measures. Meanwhile, we consolidated functions related to consent management and data access rights into Data Subject Rights Assurance Solutions. In the service domain, we unified subcategories related to consulting under Consulting & Advisory Services and grouped training-related items into Training & Education Services, simplifying similar service types into single classifications.

Finally, we either retained or created as separate categories areas the expert reviewers identified as having clear market demand. In particular, the growing need for privacy-related certification and evaluation highlighted by the experts led us to establish Certification Evaluation Services as a distinct category. Following this reorganization, we confirmed our final taxonomy, which consists of seven subcategories structured under the two domains of solutions and services, as presented in Table 2.

The final taxonomy of the personal data protection industry developed in this study is structured as follows:

Personal Data Protection Solutions

- **Safe Utilization Solutions:** These solutions apply technologies such as de-identification (including pseudonymization and anonymization), data synthesis, and data encryption to prevent the identification of sensitive personal information when data is shared. For example, solutions that safely de-identify patient data in hospital settings fall into this category. These practices align with Articles

21 and 30 of the Enforcement Decree of the PIPA, which require the encryption of passwords and identifiers using secure algorithms to minimize the risk of data breaches.

- **Data Subject Rights Assurance Solutions:** This category includes identity management, authentication, and user-centered data management functions that enable data subjects to actively exercise their rights to access, rectify, and delete their personal data. These functions relate to Article 17 of the Enforcement Decree, which specifies methods for obtaining consent, and Article 29-5, which prescribes safety measures for pseudonymized data.
- **Security Assurance Solutions:** These solutions integrate security and management technologies such as breach prevention, access control and monitoring, and data disposal to protect personal data. In particular, data disposal functions align with Article 16 of the Enforcement Decree, which requires electronic files to be permanently deleted in a manner that prevents recovery and other records to be shredded or incinerated.

Personal Data Protection Services

- **Personal Data Management Services:** These services help organizations systematically manage personal data, including outsourced system operations and lifecycle monitoring.
- **Consulting & Advisory Services:** These services analyze compliance requirements under privacy laws, regulations, and international standards, and provide organizations with customized consulting. For example, large financial institutions may work with security and legal experts to comply with international standards such as the GDPR.
- **Training & Education Services:** In accordance with Article 28(2) of PIPA, this category includes training programs and hands-on courses to help personal information handlers strengthen organizational capabilities in personal data protection.
- **Certification Evaluation Services:** These services help organizations objectively assess and certify their levels of personal data protection in accordance with Article 34-2 of the Enforcement Decree. For instance, this category includes specialized firms that support ISMS-P (Personal Information & Information Security Management System) certification preparation and post-certification management.

As such, the final taxonomy reflects the comprehensive structure and functions of the personal data protection industry, refined through top-down analysis, real market case classification, and expert validation. We expect that this taxonomy will serve as a practical foundation for the development of policies and technologies that enable the safe use and protection of personal data in the data-driven era.

Table 2. Personal data protection industry taxonomy

Category	Details
Personal Data Protection Solutions	
Safe Utilization Solutions	De-identification Data Synthesis Data Encryption
Data Subject Rights Assurance Solutions	Identity Management & Authentication User-Centered Data Management
Security Assurance Solutions	Breach Prevention Access Control & Monitoring Data Disposal
Personal Data Protection Services	
Personal Data Management Services	-
Consulting & Advisory Services	-
Training & Education Services	-
Certification Evaluation Services	-

5. Conclusion

As data utilization increases in the data economy era, socioeconomic demand for the secure and effective use of personal data—the majority of all data—is growing. Against this backdrop, we developed a final taxonomy by comparing existing classification systems proposed by major institutions, classifying real market products and services based on the derived framework, and refining the structure through expert validation.

We employed a three-stage top-down approach to systematically define the overall structure and functions of the personal data protection industry. First, we analyzed classification systems from institutions such as the OECD, PIPC, Federal Reserve Bank of San Francisco, OPC, and ENISA to extract the core functions and technical elements of the industry, which we then organized into a nine-group theoretical framework. Next, we analyzed 365 real-world cases and mapped them to the framework to construct an initial taxonomy, which we then refined based on expert interviews. The resulting final taxonomy consists of seven subcategories structured under two domains: Personal Data Protection Solutions and Personal Data Protection Services.

The final taxonomy divides the industry into two sub-industries: Personal Data Protection Solutions and Personal Data Protection Services. Each division includes detailed subcategories such as Safe Utilization Solutions, Data Subject Rights Assurance Solutions, and Security Assurance Solutions. Not limited to the theoretical model, our taxonomy reflects technical and managerial mechanisms currently implemented in practice. This approach should contribute to the development of a standardized framework that aligns with various regulatory environments such as South Korea's PIPA.

Elucidating the structural characteristics of the personal data protection industry, the proposed taxonomy should serve as both a data-driven decision-making tool for companies and policymakers and a foundational framework for academic research and practical application. Although we developed the taxonomy based on PIPA, its alignment demonstrates its applicability as a standardized model at the international level. It should thus contribute both to global policy and standardization efforts and to theoretical advancements and the identification of future academic research directions in the personal data protection industry. From an industry perspective, the taxonomy offers practical guidelines for companies and governments seeking to develop effective security and personal data protection strategies.

At the same time, this study is subject to several limitations that should be acknowledged. The proposed taxonomy was derived from market data collected at a specific point in time and therefore may not fully capture subsequent developments in the personal data protection industry. Nevertheless, the upper-level framework was constructed with reference to existing classification systems that have been systematically developed to implement national data protection laws and policies, and the market cases, including AI-based privacy protection products, were classified according to their primary functional roles rather than specific technologies. Accordingly, the taxonomy demonstrates structural scalability, in that it can be extended as the industry evolves by further specifying existing functional categories or introducing additional subcategories to accommodate emerging technologies and services.

Future studies should empirically validate the effectiveness and practical utility of this taxonomy across diverse industries and application contexts. For instance, it could be employed as an analytical framework to measure industry performance, assess market structure, or evaluate the effectiveness of specific policy instruments related to personal data protection. In addition, future research should examine how emerging technologies such as AI, big data, and cloud computing can be mapped onto the existing categories and whether they call for refinements, extensions, or dynamic updates to the taxonomy.

Conflict of Interest

The authors declare that they have no competing interests.

Funding

This work was supported by the MSIT (Ministry of Science and ICT), Korea, under the Convergence security core talent training business support program (IITP-2026-RS-2023-00266605) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

- [1] Oxford English Dictionary, "Industry, n., sense 5.a.," Oxford University Press, 2024 [Online]. Available: <https://doi.org/10.1093/OED/1171082780>.
- [2] Cambridge English Dictionary, "Industry," Cambridge University Press, 2023 [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/industry>.
- [3] J. Nightingale, "On the definition of 'Industry' and 'Market'," *Journal of Industrial Economics*, vol. 27, no. 1, pp. 31-40, 1978. <https://doi.org/10.2307/2098116>
- [4] K. A. Munir and N. Phillips, "The concept of industry and the case of radical technological change," *Journal of High Technology Management Research*, vol. 13, no. 2, pp. 279-297, 2002. [https://doi.org/10.1016/S1047-8310\(02\)00046-9](https://doi.org/10.1016/S1047-8310(02)00046-9)
- [5] C. M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston, MA: Harvard Business School Press, 1997.
- [6] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442-492, 2016. <https://doi.org/10.1257/jel.54.2.442>
- [7] R. P. Romansky and I. S. Noninska, "Challenges of the digital age for privacy and personal data protection," *Mathematical Biosciences and Engineering*, vol. 17, no. 5, pp. 5288-5303, 2020. <https://doi.org/10.3934/mbe.2020286>
- [8] P. Koutroumpis, A. Leiponen, and L. D. W. Thomas, "Markets for data," *Industrial and Corporate Change*, vol. 29, no. 3, pp. 645-660, 2020. <https://doi.org/10.1093/icc/dtaa002>
- [9] K. Rahul, R. K. Banyal, and N. Arora, "A systematic review on big data applications and scope for industrial processing and healthcare sectors," *Journal of Big Data*, vol. 10, article no. 133, 2023. <https://doi.org/10.1186/s40537-023-00808-2>
- [10] A. E. Abbas, W. Agahari, M. van de Ven, A. Zuiderwijk, and M. de Reuver, "Business data sharing through data marketplaces: a systematic literature review," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, no. 7, pp. 3321-3339, 2021. <https://doi.org/10.3390/jtaer16070180>
- [11] S. I. H. Shah, V. Peristeras, and I. Magnisalis, "DaLiF: a data lifecycle framework for data-driven governments," *Journal of Big Data*, vol. 8, article no. 89, 2021. <https://doi.org/10.1186/s40537-021-00481-3>
- [12] L. N. Valli, S. Narayanan, M. Mech, and S. Lokesh, "Ethical considerations in data science: balancing privacy and utility," *International Journal of Scientific Research Archive*, vol. 11, no. 1, pp. 11-22, 2024. <https://doi.org/10.30574/ijrsra.2024.11.1.1098>
- [13] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of cyber security," *Journal of Digital Forensics, Security and Law*, vol. 12, pp. 53-74, 2017. <https://doi.org/10.15394/jdfsl.2017.1476>
- [14] W. S. Jeong, K. S. Min, and S. W. Chai, "Analysis of economic effects for information security industry in Korea," *Journal of Korea Institute of Information Security and Cryptology*, vol. 24, no. 2, pp. 385-396, 2014. <https://doi.org/10.13089/KJIISC.2014.24.2.385>
- [15] M. Nieves, K. Dempsey, and V. Y. Pillitteri, "An Introduction to Information Security," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-12 Revision 1, 2017. <https://doi.org/10.6028/NIST.SP.800-12r1>

- [16] S. Moses and D. Rowe, "Physical security and cybersecurity: reducing risk by enhancing physical security posture through multi-factor authentication and other techniques," *International Journal of Information Security Research*, vol. 6, pp. 77-85, 2016. <https://doi.org/10.20533/ijisr.2042.4639.2016.0077>
- [17] L. Schneller, C. N. Porter, and A. Wakefield, "Implementing converged security risk management: drivers, barriers, and facilitators," *Security Journal*, vol. 36, no. 2, pp. 333-349, 2023. <https://doi.org/10.1057/s41284-022-00341-6>
- [18] D. Beck, M. Gips, and B. McFarland Pierce, *The State of Security Convergence in the United States, Europe, and India*. Alexandria, VA: ASIS Foundation, 2019.
- [19] Ministry of Science and ICT, Korea Information Security Industry Association, "Survey for Information Security Industry in Korea: Year 2024," 2024 [Online]. Available: <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=99&mPid=74&bbsSeqNo=79&nnttSeqNo=3173643>.
- [20] D. E. Bambauer, "Privacy versus security," *Journal of Criminal Law and Criminology*, vol. 103, no. 3, pp. 667-684, 2013. <https://scholarlycommons.law.northwestern.edu/jclc/vol103/iss3/2>
- [21] J. Henriksen-Bulmer, C. Yucel, S. Faily, and I. Chalkias, "Privacy goals for the data lifecycle," *Future Internet*, vol. 14, no. 11, article no. 315, 2022. <https://doi.org/10.3390/fi14110315>
- [22] S. Stalla-Bourdillon, G. Thuermer, J. Walker, L. Carmichael, and E. Simperl, "Data protection by design: Building the foundations of trustworthy data sharing," *Data & Policy*, vol. 2, article no. e4, 2020. <https://doi.org/10.1017/dap.2020.1>
- [23] OECD, "Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches," OECD, Paris, France, Digital Economy Papers No. 351, 2023. <https://doi.org/10.1787/bf121be4-en>
- [24] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y. A. de Montjoye, and A. Bourka, "Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics," European Union Agency for Network and Information Security, 2015 [Online]. Available: <https://data.europa.eu/doi/10.2824/641480>.
- [25] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): Article 4(1)," 2016 [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [26] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A taxonomy for privacy enhancing technologies," *Computers & Security*, vol. 53, pp. 1-17, 2015. <https://doi.org/10.1016/j.cose.2015.05.002>
- [27] N. Jentzsch, "Horizontal and vertical analysis of privacy and cyber-security markets," Waterford Institute of Technology, Waterford, Ireland, IPACSO D4.2, 2015. <http://dx.doi.org/10.2139/ssrn.2671296>
- [28] Future of Privacy Forum, "Privacy tech's third generation: a review of the emerging privacy tech sector report," 2021 [Online]. Available: <https://fpf.org/resource/new-fpf-report-highlights-privacy-tech-sector-evolving-from-compliance-tools-to-platforms-for-risk-management-and-data-utilization/>.
- [29] Gartner, "Gartner identifies top five trends in privacy through 2024," 2022 [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024>.
- [30] N. Aleixosa, P. Company, and M. Contero, "Integrated modeling with top-down approach in subsidiary industries," *Computers in Industry*, vol. 53, no. 1, pp. 97-116, 2004. [https://doi.org/10.1016/S0166-3615\(03\)00122-2](https://doi.org/10.1016/S0166-3615(03)00122-2)
- [31] A. J. Hanna, "A top-down approach to identifying bull and bear market states," *International Review of Financial Analysis*, vol. 55, pp. 93-110, 2018. <https://doi.org/10.1016/j.irfa.2017.11.001>
- [32] W. Callon, M. C. Beach, A. R. Links, C. Wasserman, and E. F. Boss, "An expanded framework to define and measure shared decision-making in dialogue: a 'top-down' and 'bottom-up' approach," *Patient Education and Counseling*, vol. 101, no. 8, pp. 1368-1377, 2018. <https://doi.org/10.1016/j.pec.2018.03.014>

- [33] Personal Information Protection Commission, “Personal Information Protection and Utilization Technology R&D Roadmap,” 2021 [Online]. Available: <https://dl.nanet.go.kr/SearchDetailView.do?cn=MONO12022000014656>.
- [34] Federal Reserve Bank of San Francisco, “Privacy enhancing technologies: categories, use cases, and considerations,” Fintech Edge Special Report, 2021 [Online]. Available: <https://www.frbsf.org/research-and-insights/publications/fintech-edge/2021/06/privacy-enhancing-technologies/>.
- [35] Office of the Privacy Commissioner of Canada, “Privacy enhancing technologies – a review of tools and techniques,” 2017 [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/.
- [36] Q. Zhang, S. Jia, B. Chang, and B. Chen, “Ensuring data confidentiality via plausibly deniable encryption and secure deletion—a survey,” *Cybersecurity*, vol. 1, article no. 1, 2018. <https://doi.org/10.1186/s42400-018-0005-8>



Yeji Choi <https://orcid.org/0009-0000-8307-7094>

She received the B.S. degree in sociology from Chung-Ang University, Seoul, South Korea, in 2022, and the M.S. degree in convergence security from Chung-Ang University in 2024. She is currently pursuing the Ph.D. degree in convergence security at Chung-Ang University. Her current research interests include personal data protection, privacy-enhancing technologies, and security data analytics.



Hangbae Chang <https://orcid.org/0000-0001-6098-1419>

He received the B.S. and M.S. degrees in computer engineering from Chung-Ang University, Seoul, South Korea, in 1997 and 1999, respectively, and the Ph.D. degree in information systems from Yonsei University, Seoul, in 2006. He is currently a Professor in the Department of Industrial Security, Chung-Ang University. His current research interests include privacy-enhancing technologies, security data analytics, and industrial security.