[PBL5] 연구분야 동향조사 보고서

A Report on Privacy Security Trends

Han, A-Lim

Introduction

Since the advent of the 21st century, technological advancements such as the internet, mobile devices, cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) have undergone rapid development.

These technologies have facilitated the collection, storage, and analysis of substantial quantities of personal data, thereby enhancing convenience in daily life, business efficiency, and the quality of healthcare and public services.

Concurrently, a multitude of risks persist, encompassing violations of personal privacy, data breaches, data processing without user consent, and the misuse of sensitive information. These environmental changes demand serious measures not only in technological responses but also in institutional and ethical aspects.

The present report is an examination of recent major technological trends, practical cases, institutional changes, and future challenges in the field of privacy security.

I. Technical Trends

1. Privacy Enhancing Technologies (PETs)

- ✓ Differential Privacy(차등 프라이버시)
  : This technique involves the insertion of noise to prevent inferences about individual users' contributions. Companies such as Google and Apple employ this method when analyzing user data at the operating system or service level, achieving a balance between protecting user privacy and enabling useful statistical analysis and model training.

- ✓ Homomorphic Encryption(동형 암호)
  : This facilitates the execution of computations on encrypted data, thereby enabling analysis

and processing without the need for decryption. However, there are still practical limitations in terms of computational cost and latency. Researchers are working to improve this through lightweight techniques, efficient hardware support, and parallel processing methods.

2. Federated Learning and Distributed Data Processing

- ✓ Case Study 1: The application of Federated Learning in the field of healthcare

  For instance, studies have been published that demonstrate the efficacy of training models without the need to share raw data, a method employed by hospitals that utilize electronic health records (EHRs). This approach has been shown to enhance prediction accuracy while ensuring privacy protection.

- ✓ Case Study 2: The Intersection of the Internet of Things (IoT) and Smart Healthcare

  The data generated by sensors and devices on medical Internet of Things (IoMT) networks is characterized by its high degree of sensitivity. The aggregation of this data on a centralized server poses significant privacy concerns. Research has been conducted on methods for defending against malicious poisoning attacks, including approaches such as combining blockchain technology with secure aggregation and secure multi-party computation (SMPC).

3. The evolution of attack types and defense techniques is a subject of considerable interest.

Privacy attacks targeting artificial intelligence models, such as model extraction attacks, membership inference attacks, and model inversion attacks, are increasing.

The following countermeasures have been implemented:

- ✓ Model output restriction (output perturbation or clipping)
- ✓ Differentially private learning
- ✓ The design of loss functions is considered in the context of regularization and privacy guarantees.

- ✓ The present study will examine the development of systems designed for the detection of anomalies and the execution of audits of models.
- ✓ The present study is in the preliminary research phase.

II. Regulatory and Legal Trends

1. GDPR and Enforcement Cases in Europe

The General Data Protection Regulation (GDPR) of the European Union (EU) imposes stringent requirements on data processing, including transparency, user consent, data minimization, and implementation of security measures. Non-compliance with this regulation can result in substantial fines, and numerous companies have faced enforcement actions as a consequence.

- ✓ TikTok Case

  : The Irish Data Protection Commission (DPC) imposed a fine of €530 million on TikTok for transferring European users' data to China in violation of the GDPR. (The Verge)

- ✓ Meta (Facebook) International Data Transfer Case

  : Meta was fined €1.2 billion by the Irish DPC for insufficient compliance with regulations regarding the transfer of user data to the United States. (CMS Law)

- ✓ Clearview AI Case

  : The Dutch Data Protection Authority (DPA) levied a fine of €30.5 million on Clearview AI for creating a biometric database by scraping European citizens' facial images from publicly accessible websites without legal authorization. (DPO India)

- ✓ Criteo Case

  : The French National Commission on Informatics and Liberty (CNIL) imposed a fine of €40 million on Criteo due to inadequate prior consent procedures for user tracking and ad-target profiling. (EQS Group, CookieYes)

2. Country- and Region-Specific Regulatory Developments

In multiple countries, including South Korea, efforts have been made to strengthen personal data protection laws, regulate cross-border data transfers, and expand data subject rights such as access and erasure. Additionally, guidelines for ethical use of artificial intelligence have been introduced.

For instance, regulations regarding the destruction of personal data by public institutions and companies are becoming increasingly strict, with administrative fines and criminal penalties for violations.

Furthermore, requirements related to the clarity of user consent, completeness of disclosure, and mandatory reporting obligations in the event of security breaches are being increasingly enforced.

III. Lessons Learned from Real-World Cases

1. Importance of Transparency

It is essential to clearly inform users about what data is being collected, why it is collected, how it will be used, and with whom it will be shared. For example, LinkedIn was fined €310 million by the Irish Data Protection Commission (DPC) due to insufficient legal grounds for processing personal data for advertising purposes. In this case, deficiencies in advertising data processing methods and user consent procedures were identified as the main issues.

2. Handling of Sensitive and Biometric Data

Biometric information, such as facial recognition data, is classified as particularly sensitive under GDPR. As illustrated by the Clearview AI case, collecting or processing such data without proper consent or in a non-transparent manner can result in substantial penalties.

3. Child Data Protection

In the case of TikTok, issues were raised because children’s accounts were set to public by default, and age verification procedures were inadequate. Personal data of children requires a higher standard of protection than that of adult users.

4. Data Responsibility in Corporate Acquisitions

During the acquisition of Starwood Hotels by Marriott, insufficient due diligence regarding system security and data processing practices exposed vulnerabilities in legacy systems, resulting in significant fines.

Conclusion and Recommendations

The field of privacy and security is rapidly evolving due to technological advancement, increasing value of user data, strengthened regulations, and heightened societal awareness. The traditional paradigm of "collecting as much data as possible is a competitive advantage" is shifting toward questions such as "how to collect, store, and use data safely" and "how to obtain user consent and ensure control over personal information."

Based on this context, the following recommendations are proposed:

- ✓ Establish Strategies Integrating Technology and Regulation

  : Privacy cannot be ensured solely through technology. Techniques such as differential privacy, federated learning, encrypted communications, and model security verification should be implemented strategically, while simultaneously reinforcing user notifications, transparency policies, consent procedures, audits, and accountability mechanisms.

- ✓ Implement Privacy by Design

  : Privacy principles (e.g., data minimization, limited retention, purpose limitation, data security) should be incorporated at the system and service design stage. This proactive approach minimizes the need for costly retroactive modifications.

- ✓ Continuous Evaluation of Threat and Attack Models

  : AI-related attacks, including membership inference and model extraction, are continuously evolving. Existing security models are insufficient; threat models must be regularly updated, and safety verification procedures must be established.

- ✓ Recognize the Importance of Legal Compliance and Invest Accordingly

  : As major privacy regulations such as GDPR and CCPA have global implications, organizations should seek legal counsel, appoint internal Data Protection Officers (DPOs), and conduct Privacy Impact Assessments (PIAs). Enforcement cases demonstrate that non-compliance can result in substantial fines and significant reputational damage.

- ✓ Ensure Ethics and Societal Trust

  : Beyond technical and legal measures, organizations must communicate how data is used and what risks exist, while enabling user feedback mechanisms. Special attention should be given to sensitive information, biometric data, and data concerning children, applying stricter protection standards where necessary.

References

Fatehi, Farhad and Burton-Jones, Andrew and Hynd, Andrew and Hassandoust, Farkhondeh, Learning from Enforcement Cases to Manage GDPR Risks (2021). MIS Quarterly Executive, 20 (3), 4, 199-218.DOI:10.17705/2msqe.00049., The University of Auckland Business School Research Paper Series, Available at SSRN: https://ssrn.com/abstract=4738548

Wenlong Li, Zihao Li, Wenkai Li, Yueming Zhang, Aolan Li,

Mapping the empirical literature of the GDPR's (In-)effectiveness: A systematic review,

Computer Law & Security Review, Volume 57, 2025, 106129, ISSN 2212-473X

Haperen, Olaf. (2025). GDPR Enforcement Beyond EU-Borders — The Dutch Data Protection Authority’s Fine on Clearview AI and the Future of AI Regulation & Enforcement. Computer Law Review International. 26. 10-13. 10.9785/cri-2025-260103.

Maciej Pichlak, Klaudia Gaczoł, Simple and advanced reflexivity in GDPR enforcement: empirical evidence from DPA activity, International Data Privacy Law, Volume 13, Issue 4, November 2023, Pages 267–283, https://doi.org/10.1093/idpl/ipad018

[Okta] Data Privacy vs. Security: Maintaining Privacy and Security in the Digital Age

(https://www.okta.com/identity-101/privacy-vs-security/)

[Meta] Privacy Tools and Information Security

(https://www.meta.com/ko-kr/actions/protecting-privacy-and-security/?srsltid=AfmBOoodhNzm_wMiLNxIWa7giWAO0rz7x1W6kSIGB4jYlNXlYZSQikOT)

[An Coimisiun um Chosaint Sonrai Data Protection Commisson] Irish Data Protection Commission fines LinkedIn Ireland €310 million

(https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million)

[EDPB] Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition

(https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en)

[EDPB] 1.2 billion euro fine for Facebook as a result of EDPB binding decision

(https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en)

[EBPD] Personalised advertising: French SA fined CRITEO EUR 40,000,000

(https://www.edpb.europa.eu/news/national-news/2023/personalised-advertising-french-sa-fined-criteo-eur-40000000_en)

[Herbeat Smith Freehills Kramer] ICO fines Marriott £18.4 million in relation to Starwood Hotel's 2014 data breach

(https://www.hsfkramer.com/notes/data/2020-11/the-other-not-so-mega-mega-fine-ico-fines-marriott-18-4-million-in-relation-to-starwood-hotels-2014-data-breach)