sciendo

Explaining the unexplainable: data sharing and privacy in Web 3.0

Jieun Shim
Jieun Kim[1]

Graduate School of Technology & Innovation Management
Hanyang University
222 Wangsimni-ro, Seongdong-Gu
Seoul, Republic of Korea
uouttl73@hanyang.ac.kr
jkim2@hanyang.ac.kr

Abstract: Web 3.0 transforms data ownership by empowering users to monetize their personal information, yet this shift amplifies complex privacy challenges. Understanding the features influencing data-sharing decisions in this evolving context aligns with the proactive philosophy of designing legal frameworks that anticipate and mitigate conflicts. This study leverages explainable AI (XAI) to analyze user privacy behaviors and other privacy attributes, using data from 682 individuals in Korea within a personalized app scenario. The findings reveal a privacy paradox: users with low perceived data value but high privacy concerns often share their data, whereas those with higher trust in services are more hesitant, prioritizing long-term privacy and service continuity. These insights demonstrate that a one-size-fits-all legal or regulatory approach cannot adequately address the nuances of Web 3.0 data-sharing dynamics. Instead, this study advocates for a proactive law framework that integrates user research and XAI insights to anticipate conflicts and opportunities. By understanding individual intentions and concerns, proactive law can deliver tailored, context-sensitive solutions that balance privacy, user autonomy and economic opportunity, ensuring equitable and sustainable outcomes in the decentralized Web 3.0 ecosystem.

Keywords: *explainable AI (XAI), privacy design, privacy paradox, proactive law, user decision-making, Web 3.0*

[1] Corresponding author.

https://doi.org/10.2478/bjes-2025-0008 *TalTech Journal of European Studies*, 15(1(41))
Tallinn University of Technology (ISSN 2674-4619)

1. Introduction

The Web 3.0 environment is evolving rapidly, introducing new technologies, economic models and privacy challenges that demand innovative approaches (Bruwer and Rudman, 2015). Proactive law emphasizes flexibility and adaptability, allowing legal frameworks to respond effectively to these dynamic changes. By ensuring ongoing relevance, principled compliance and conflict management, proactive law not only prevents potential conflicts but also anticipates and addresses future challenges through thorough analysis and preparation (Schartum, 2006; Solarte-Vásquez, Järv and Nyman-Metcalf, 2016). Unlike traditional legal approaches, which are often reactive, proactive law aligns legal logic with real-world requirements, promoting interdisciplinary collaboration to achieve practical and context-specific outcomes (Pohjonen, 2006). These qualities make it particularly well-suited to address the emerging complexities of Web 3.0.

Among these complexities, privacy has emerged as a critical concern in digital ecosystems, amplified in Web 3.0 by the shift toward user-centric data ownership and monetization (Bouchagiar, 2018). This paradigm grants users greater control over their data as an asset, demanding fair practices and transparent governance (Rudman and Bruwer, 2016). However, decentralization technologies such as blockchains and cryptocurrencies introduce significant trade-offs between data-sharing and the personalized services or financial benefits that users seek, which can lead to disputes over rights, responsibilities and misuse of data.

In this context, the privacy paradox—the gap between privacy attitudes and behaviors—becomes particularly pronounced (Kokolakis, 2017; Barth and de Jong, 2017). While users express concern about their privacy, they often prioritize immediate convenience over long-term risks, leaving them vulnerable to potential misuse of their data by third parties (Bouchagiar, 2018).

The complexities of privacy in Web 3.0 are further compounded by evolving global data privacy regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Personal Information Protection Act (PIPA) of the Republic of Korea, which seek to address the challenges posed by decentralization (Pavelek and Zajíčková, 2021; 'Directive (EU) 2022/1925', 2022). Despite these efforts, navigating the relationships between users, service providers and third parties remains a

critical challenge (Rudman and Bruwer, 2016). Addressing these challenges requires not only reactive regulatory updates but also proactive frameworks that empower users and anticipate future needs.

In this context, this study investigates how user research and explainable AI (XAI) can inform privacy design to address emerging privacy concerns and support proactive legal frameworks. Using data from personalized app usage scenarios, we examine the factors influencing users' willingness to share personal data with third parties. XAI provides interpretable insights into users' privacy decision-making, uncovering paradoxical behaviors such as prioritizing immediate service benefits over privacy. Drawing on the principles of proactive law, the study concludes with tailored privacy design improvements and proactive legal frameworks to balance user autonomy, economic opportunities and privacy protection in the evolving Web 3.0 landscape.

2. XAI in supporting privacy decision-making

With the increasing integration of artificial intelligence (AI) in personalized digital services, automated decision-making systems pose risks of uncertainty as users are left uncertain when making privacy decisions (Jones, Kaufman and Edenberg, 2018; Mazur, 2019). Individuals may not fully understand how those decisions are made, highlighting the need to regulate automated systems to address transparency issues (Larsson and Heintz, 2020) and improve transactional design practices from legal and technical perspectives (Solarte-Vásquez and Nyman-Metcalf, 2017).

In practical deployments of AI, explainable AI (XAI) refers to machine-learning techniques aimed at providing explainability for AI decisions (Arrieta *et al.*, 2020). Some pioneers have attempted to integrate XAI by helping users understand their complex decision-making and visualize the trade-offs between service utility and privacy protection (Wijesekera *et al.*, 2018; Ghalebikesabi *et al.*, 2024). For example, privacy-conscious assistants (Ghalebikesabi *et al.*, 2024) are AI systems that adjust information-sharing behaviors to align with user privacy expectations while providing interpretable insights, demonstrating principles that align with XAI. Another example of privacy-aware reinforcement learning systems, adaPARL (Taherisadr, Stavroulakis and Elmalaki, 2023) allows users to balance data utility and privacy by analyzing their usage patterns and

guiding them to make informed decisions without sacrificing privacy for convenience. Building on the research of Wijesekera *et al.* (2018), XAI can be utilized to predict future issues in user decision-making regarding personal data access, providing preventative measures.

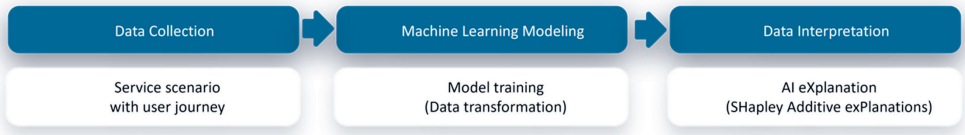
The above studies demonstrate the potential application of XAI in the growth of the Web 3.0 data market, ultimately mitigating unfairness between users and services in regulating automated privacy systems. The integration of XAI into privacy decision-making processes not only enhances transparency but also empowers users to make informed choices in the evolving digital landscape, which partially addresses fundamental concerns about the concept of consent in legal and ethical domains (Jones, Kaufman and Edenberg, 2018; Bongard-Blanchy *et al.*, 2021).

3. Case study

This case study investigates how user research can inform privacy design by examining the features that influence users' willingness to share personal data with third parties. To analyze these complex decision-making processes, we take into account the combined taxonomy of usability factors for transactional design (Solarte-Vásquez, Järv and Nyman-Metcalf, 2016) and employ an approach to explainable artificial intelligence (XAI), which provides transparent and interpretable insights into the privacy attributes that drive users' decisions to sell or not sell their data to third parties within the context of the personalized service journey. The findings uncover key determinants of data-sharing behavior, including paradoxical patterns in which users prioritize immediate service benefits over long-term privacy considerations.

3.1 Protocol

Figure 1: Case study protocol



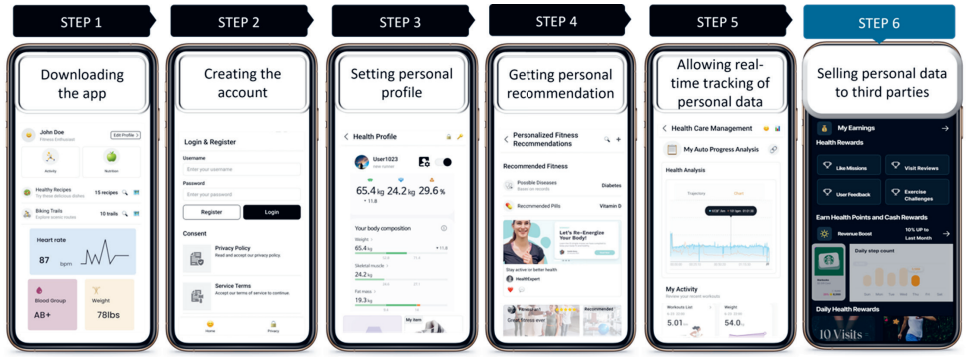
3.1.1 Data collection

First, a total of 682 users (among which 53.9% were female) from the Republic of Korea, aged 20s to 30s, were recruited through an online survey platform. The participants were paid $10 for approximately 10 minutes of their time, and the survey was conducted throughout May 2024. Most of the participants were college graduates, with the highest frequency of recent usage being once per week.

The privacy paradox is characterized by the complexity arising from users' irrational decision-making, which is influenced by individual, social and situational factors across the service usage context. This paradox manifests through diverse privacy attributes, highlighting the intricate dynamics of user behavior. Addressing the privacy paradox requires comprehensive user research and a nuanced understanding of factors such as demographics, risk perception and perceived service utility (Acquisti *et al.*, 2017; Schomakers, Lidynia and Ziefle, 2019).

Schomakers, Lidynia and Ziefle (2019) proposed addressing this issue by exploring classification models that segment users into clusters based on their behavioral traits, thereby accommodating the complexity of user characteristics. Similarly, Acquisti *et al.* (2017) introduced objective scales to quantitatively measure user attitudes, enhancing the validity of data collection efforts. Building on these prior studies, research methodologies have been synthesized to capture privacy attributes comprehensively throughout the user journey.

Figure 2: Example of a user journey in a personalized healthcare app service



Throughout the study, users were asked to decide which data they would share in exchange for personalized service features. As the study progressed,

the data requested became increasingly sensitive, including potentially risky personal data such as GPS locations and heart rate data, to receive more tailored service benefits and recommendations. After completing Step 5, the participants were asked to confirm their privacy attitudes by answering questions on the importance of privacy and security and their intention to continue using the service. Finally, in Step 6, the users evaluated how they perceived the value of their data based on the list of data they had decided to share in the earlier steps. Considering a referential monetary return (i.e., $22.5 per person, based on Facebook Ads Revenue 2020), they were then asked whether they were willing to sell their personal data to third parties.

3.1.2 Machine-learning modeling

The protocol begins by collecting data from 682 users through a personalized app service scenario (Figure 2). Based on the studies of Barth and de Jong (2017) and Schomakers, Lidynia and Ziefle (2019), the following privacy attributes were selected: User Characteristics, Privacy Attitudes, Perceived Service Benefits, Privacy Behaviors and Privacy Decisions. User Characteristics reflect demographic traits that define each user's personal context. Privacy Attitudes represent the comprehensive perception of privacy intentions that users hold prior to making any specific decisions. Perceived Service Benefits—especially evident in mobile environments where applications are downloaded and engaged— assess the advantages users have in a given service context. Privacy Behaviors emerge as concrete actions, captured in decisions about whether to disclose personal information. Finally, the process culminates in Privacy Decisions, encompassing the value users assign to their exposed privacy after they have taken specific privacy-related steps and resolved to continue using the service.

After collecting user data, an XGBoost classification model (Chen and Guestrin, 2016) was developed to evaluate the impact of privacy attributes on users' decision-making. Unlike other machine learning models, XGBoost of decision tree models have the advantage of visually representing the variables that significantly influence a specific outcome (target variable) and their contributions.

Table 1: Privacy attributes and variables (features) examined in the user journey

User journey	Privacy attributes	Variables (n=25)
Step 1: Downloading the app	User Characteristics	- Age - Gender - Level of education
	Perceived Service Benefits	- Service type - Usage frequency
	Privacy Attitudes	- General privacy concerns
Step 2: Creating the account	Privacy Attitudes	- Social norms - Perceived privacy concerns - Personal information infringement
	Perceived Service Benefits	- Trust in service - Convenience of service - Interest in service
Step 3: Setting personal profile	Privacy Behaviors	- Disclosure of date of birth - Disclosure of gender - Disclosure of email address
Step 4: Getting personal recommendations	Privacy Behaviors	- Disclosure of friend lists on social network service (SNS) - Disclosure of medical records from insurance - Disclosure of income information from banking accounts
Step 5: Allowing real-time tracking of personal data	Privacy Behaviors	- Disclosure of viewing history on YouTube - Disclosure of location data from GPS - Disclosure of stress index from Biosensors
	Privacy Attitudes	- Importance of privacy and security
	Perceived Service Benefits	- Intention to continue to use
Step 6: Selling personal data to third parties	Privacy Decisions	- Perceived data value - Willingness to sell personal data to third parties

SHapley Additive exPlanations (SHAP) (Lundberg and Lee, 2017), when used with the XGBoost model, provides a more sophisticated and objective understanding than other variable importance measurement techniques (Bhattacharya, 2022). By leveraging the Shapley values from game theory, SHAP accurately calculates the contribution of each variable by considering all the possible combinations of variables (Lundberg and Lee, 2017).

XAI machine-learning model employed a classification approach, referencing studies by Kenny *et al*. (2020) and Bhattacharya (2022), to analyze complex interactions between various influencing factors in unstructured data through intuitive visualizations. As shown in Table 1, the model utilized a total of 25 variables (or features) based on its classification, each with its own class definition and collection method.

The features related to Privacy Attitudes were analyzed by conducting a scale-based survey. For example, regarding Social Norms, respondents were asked to rate their level of agreement with the statement, "Many people around me disclose their real personal information on this service", across different intervals. To measure the perceived value of information disclosure, participants responded to survey items such as "The value I gain from using this app is worth the information I give away".

Using the XGBoost model, we achieved a high accuracy of 0.8372, demonstrating strong performance in predicting user decisions on data sharing to sell their data.

3.1.3 Interpretation of data

Figure 3 illustrates the explanations of the SHAP results using two visualization types—summary and waterfall plots. The summary plot and the waterfall plot were selected from various SHAP plot libraries. The summary plot allows us to examine the key factors influencing decisions across the entire dataset, whereas the waterfall plot provides insight into the significant factors in individual users' decision-making processes.

In the summary plot (see the top left of Figure 3), the Y-axis displays features in the order of importance. Through the summary SHAP plot, we can identify key features in the order of Feature A, B, and C, as well as observe their corresponding patterns. The X-axis represents the SHAP values where positive values contribute positively to the result and negative values contribute negatively. The color spectrum represents the feature values, with the values increasing as the color approaches red. The distribution of dots reveals distinct patterns; for example, in the case of Feature A, the blue dots have a positive impact on the decision. For Feature B, relatively dense red dots influence the decision positively with high SHAP values. The trend for Feature C is split into two, with red and purple dots showing negative impacts, indicating that feature values from medium to high negatively influence the decision.

Figure 3: XAI model explanations using the SHAP's summary plot and waterfall plot



In the waterfall plot (see the top right of Figure 4), each bar represents the contribution of a feature to an individual user's decision, showing how specific features impact the decision. The SHAP value of +1.55 (in red) for class 5 of Feature D shows that this feature class positively influences the decision. In contrast, a SHAP value of -1.64 (in blue) for class 3 of Feature E indicates that this feature class negatively impacts the decision. By summing up the individual feature contributions, the waterfall plot visually explains how each feature affects the overall decision outcome for a specific user.

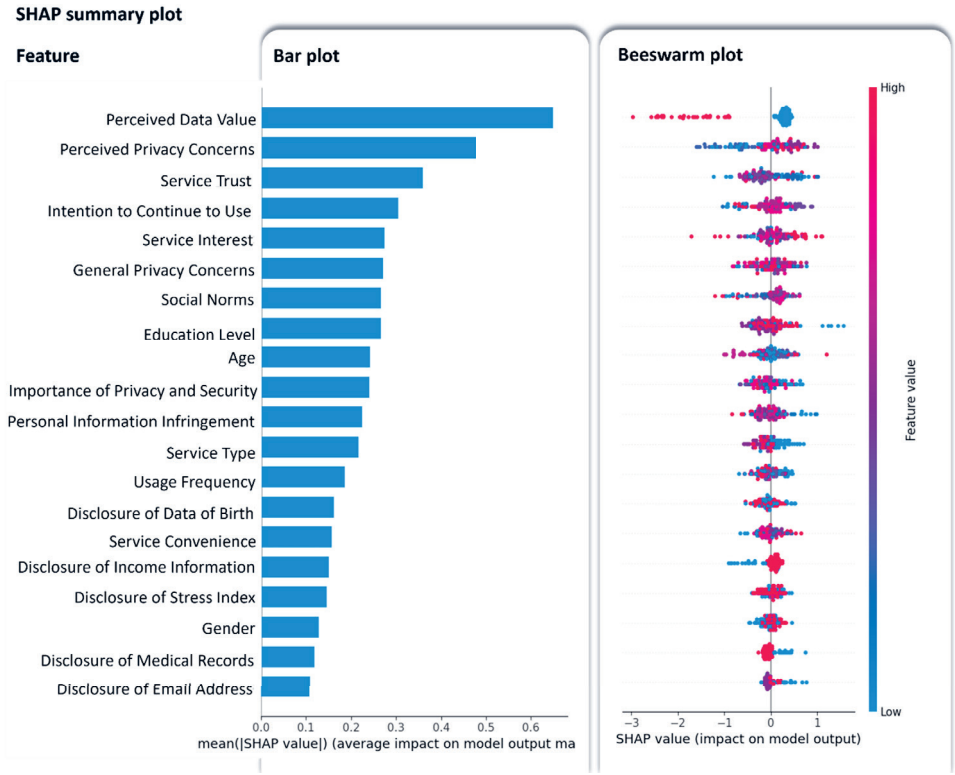
3.2 Key features influencing users' decision-making

The analysis starts with delineating the importance of key influencing features and then examines how each feature affects the user's decision-making process. Following the study of XAI interpretation (Kenny *et al.*, 2020; Bhattacharya, 2022), we decided to focus on the top three features that illustrate how each feature affects the user's decision-making process. Figure 4 illustrates the most important features in the following order: Perceived Data Value, Perceived Privacy Concerns and Service Trust.

The summary plot on the left side of Figure 4 shows the importance of Perceived Data Value, identified as the most important feature contributing

to the decision with a SHAP value of 0.6. The SHAP value difference between Perceived Data Value and Perceived Privacy Concerns indicates that these two features have the most significant impact on the decision to sell their data to third parties compared to other factors. This suggests that users weigh the perceived value of data assets and their privacy concerns as the primary determinants in their decision-making process.

Figure 4: Summary plots for users' decision-making, which include two types: bar plot (left) and beeswarm plot (right)



In the distribution of dots, Perceived Data Value is clustered with blue dots in the positive direction on the x-axis (see the beeswarm plot in Figure 4). The distinct user patterns in Perceived Data Value show a greater effect on the decision to accept when the feature's value is low (i.e., lower than "invaluable"). The second most influential feature, Perceived Privacy Concerns, has a positive effect on the decision when it is high. Owing to these two key factors, the user patterns suggest a tendency to sell their data when Perceived Data Value is considered less valuable and Perceived Privacy Concerns are high. In contrast, Service Trust indicates that users

who trust the service (feature values are medium or high) negatively impact their decision to accept it.

The results show that in personalized service journeys, the overall patterns of users reveal a contradiction between their privacy attitudes and privacy decisions, which is not resolved even when financial benefits are offered in exchange for their data. Importantly, users face different privacy paradox aspects, trading off their data and perceiving it as low in value or by not seeking additional service benefits, even when they have high trust in the service with high privacy concerns.

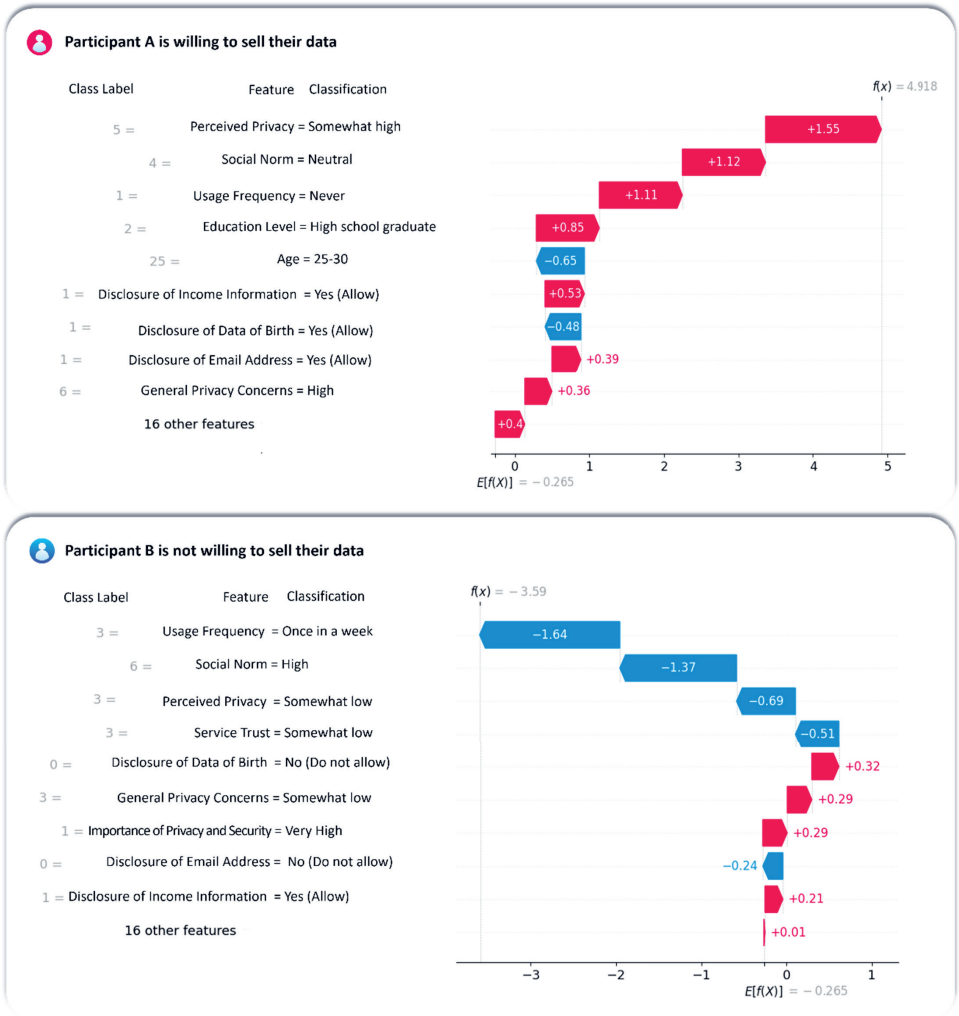
3.3 Comparing different individuals' decision-making profiles

A waterfall plot (see Figure 5) was extracted for Participant A and Participant B, who had opposing decisions, to understand how different factors contribute to an individual's decision-making process. The key factors influencing both decisions were Perceived Privacy Concerns, Social Norms (specifically, the belief that many people share their authentic personal information on the app), and Usage Frequency (how often the app is used).

Participant A, who is willing to sell their data, was influenced primarily by Perceived Privacy Concerns, with a SHAP value of +1.55, indicating that this factor had a 1.55 times greater influence than the other factors. Despite having somewhat high privacy concerns, these led Participant A to sell their data to third parties. Additionally, their neutral stance on Social Norms—the belief that "many people share their authentic personal information on the app"—also contributed significantly (+1.12). This neutrality suggests that while they did not strongly believe in widespread data sharing by selling, they were not opposed to it either. Finally, Participant A's lack of prior experience with the app positively influenced their decision to sell (+1.11).

By contrast, Participant B, who chose not to sell their data, was influenced primarily by Usage Frequency, with a SHAP value of -1.64. Familiarity with the app (rated as "once a week") led to a more cautious approach regarding data selling. Additionally, Participant B's strong belief in Social Norms—that others frequently share real, authentic information on the app—contributed negatively (-1.37). This might suggest that Participant B values their real personal data more and, since they too share authentic information, they are more reluctant to sell it to third parties. Finally, Perceived Privacy Concerns, although rated somewhat low, still had a negative impact (-0.69), reflecting a cautious attitude toward data sharing to sell despite having lower privacy concerns overall.

Figure 5: Waterfall plots for individual's decision-making profiles for Participant A (top) and Participant B (bottom)



A comparison between Participant A and Participant B shows that although both were influenced by Perceived Privacy Concerns and Social Norms, their reactions to these factors differed. Participant A, with a neutral belief in Social Norms was not particularly swayed by whether others were sharing real information, leading them to sell their data despite privacy concerns. Meanwhile, Participant B, with a strong belief in Social Norms, was more protective of their data, likely because they perceived their own information to be authentic and therefore more valuable. This distinction highlights the importance of considering how users' perceptions of data authenticity and social behavior influence their decisions.

This analysis emphasizes the need to understand personalized privacy concerns when designing legal frameworks or data market platforms, as different users weigh risks and benefits in unique ways. This will be further discussed in the next section.

4. Considerations on proactive legal design frameworks

The proactive law framework effectively highlights the importance of fostering fairness, transparency and trust to address emerging legal challenges proactively (Schartum, 2006; Pohjonen, 2006). This study does that by considering the key features of privacy attributes, focusing on monetized data-sharing and presenting proactive priorities, including tailored legal frameworks and XAI-driven solutions. By integrating explainable AI (XAI), it explores how proactive legal strategies can enhance user autonomy and promote human-centric and equitable data management in the evolving Web 3.0 ecosystem.

4.1 Addressing the privacy paradox and the impact of service trust

Our study revealed an intensified privacy paradox in monetarily incentivized data-sharing scenarios. When financial rewards were offered, users with greater Privacy Concerns but lower Perceived Data Value were paradoxically more willing to sell their data. This emphasizes the need for proactive and human-centric transactional design to address this paradox by ensuring that users are fully informed of the potential risks and implications of selling behavior, even when financial incentives are involved.

At the same time, Service Trust emerged as a critical factor in users' reluctance to share data, with highly trusting users preferring to retain their data within the service due to confidence in its inherent value and security. While this behavior aligns with responsible data-sharing practices, it could limit the growth of the Web 3.0 data market, where exchanges are essential to the ecosystem's development.

These findings demonstrate that a one-size-fits-all legal or regulatory approach cannot adequately address the nuances of Web 3.0 data-sharing dynamics. Instead, this study advocates for a proactive law framework that

anticipates and prevents potential conflicts by leveraging insights from prior legally relevant usability factors and user behavior research and XAI. Legal tools for data privacy must evolve based on those principles, to address the complex interplay of user trust, privacy attitudes and economic incentives.

Privacy laws can balance and support economic opportunities in Web 3.0 data sharing by fostering trust through transparency and dynamic consent models, supporting fairness and trust. This study builds on Jackson and Wang's (2018) work by advancing from a reactive model to a proactive approach.

4.2 Incorporating XAI to address future privacy challenges

A crucial element of this study is the integration of XAI to interpret the factors influencing users' data sharing decision to sell their data as a digital asset. XAI plays a pivotal role in providing users with transparent explanations of the risks and benefits associated with selling their data, which is especially important in a landscape where privacy attitudes can be inconsistent or paradoxical. SHAP models are particularly useful in visualizing and interpreting these factors, allowing for a deeper understanding of user behaviors and how privacy attitudes shift over time and across individuals, significantly improving the usability assessment of systems (Oviedo *et al.*, 2024).

The analysis advances the integration of legal application with technological design, applying some of the integrated usability notions proposed by Solarte-Vásquez, Järv and Nyman-Metcalf, 2016. Given that the weighing of risks and benefits varies for each user, various advanced automation technologies can be discussed to assess this balance.

This study broadens the understanding of *the interdisciplinary nature of proactive law*, as mentioned by Berger-Walliser (2012). By evolving privacy management systems with XAI, compliance with privacy protection laws can be personalized for individual users. Early researchers, including Klitou (2014) and Rossi *et al.* (2019), have explored design approaches in digital contexts by integrating artificial agents. Consequently, Hagan's (2020) concept of *human-centered systems in a proactive approach* progresses from user participation to understanding through XAI. As illustrated in Xi's (2024) research discussing the global application of proactive regulation for emerging AI, new regulations for XAI-driven privacy protection can be proposed.

For example, the comparison of two distinct users' privacy decision-making (Participant A and Participant B in Figure 5) reveals how individual factors influence choices in different ways. Participant A, despite having somewhat high Perceived Privacy Concerns and a neutral stance on Social Norms, chose to share their data. Additionally, Participant A's lack of usual experience with the app positively influenced their decision, as they might be more open to selling data in a market service context. Conversely, Participant B, who used the app relatively frequently (once a week), took a more cautious approach to selling the data. Interestingly, Participant B's strong belief in Social Norms—that others share authentic, valuable information—made them more protective of their own data, likely perceiving it as too valuable to sell to third parties, even though Participant B had relatively low Perceived Privacy Concerns.

This comparison highlights the complexity of privacy in decision-making, where users' perceptions of social norms, data value and authenticity significantly shape their behavior. Explainable AI (XAI) offers a deeper understanding of these personalized and nuanced decisions by making the underlying factors transparent, thus enabling more informed choices. Moreover, XAI facilitates a collaborative approach, underscoring the need for regulators, industry stakeholders and policymakers to work together to create a legal environment that balances user autonomy with economic opportunities.

A proactive approach to privacy by leveraging XAI holds global potential by addressing individual users' needs without being restricted by regional boundaries. Building on prior research by Pavelek and Zajíčková (2021) and Razmetaeva (2020), it emphasizes the importance of establishing a global regulatory framework based on sound methodological foundations that fosters fairness and equity in the data economy. Personalization, when integrated into proactive legal frameworks, could enable a cohesive, global data privacy market that aligns with users' expectations while addressing emerging regulatory challenges.

5. Conclusion

The evolution of Web 3.0 grants users increased control over their personal data and the ability to monetize it, making it essential to understand the factors influencing privacy decision-making to shape proactive legal frameworks. This study explored these dynamics within a potential data marketplace, an intensified privacy paradox in monetarily incentivized data-sharing scenarios: users with higher Privacy Concerns and lower Perceived Data Value paradoxically became more willing to sell their data to third parties, while those with higher Service Trust were more reluctant.

Resolving this paradox requires adopting a proactive law strategy that anticipates and prevents legal issues while fostering fairness and trust. Tailored consent mechanisms, informed by user profiles such as Privacy Attitudes and Behaviors, and fair data compensation models are essential for balancing user autonomy with economic incentives. Furthermore, integrating explainable AI into these processes can enhance transparency, enabling users to make informed decisions in a complex data economy.

Our approach is crucial for balancing the economic opportunities of data monetization with the need for robust privacy care. By fostering transparency, trust and fairness, this study offers a pathway for Web 3.0 stakeholders—service providers, regulators and policymakers—to develop sustainable frameworks that empower users while supporting the growth of equitable data markets.

Jieun Shim is a PhD candidate at the Graduate School of Technology and Innovation Management, Hanyang University. She holds a BA in media communication from the same university. With ten years of practical experience in the media-IT field, her research focuses on empirical studies that bridge human-centered interaction and privacy design through the application of technology.

Jieun Kim is a full professor at the Graduate School of Technology and Innovation Management, Hanyang University and co-director of Imagine X Lab. With an MS and PhD in industrial engineering from Arts et Métiers ParisTech, she pioneers legal design studies, exploring how design methodologies transform legal systems to be more human-centered and innovative. Author of Patent analytics: transforming IP into intelligence (Springer, 2021) and Legal design workbook: innovating the law for a human-centred future (2023), she advances interdisciplinary

research, bridging law, design and technology to address modern legal and societal challenges.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S (2017) 'Nudges for privacy and security: understanding and assisting users' choices online', *ACM Computing Surveys*, 50(3), article 44, pp. 1–41. Available at: https://doi.org/10.1145/3054926

Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R. and Herrera, F. (2020) 'Explainable artificial intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI', *Information Fusion*, 58(1), pp. 82–115. Available at: https://doi.org/10.1016/j.inffus.2019.12.012

Barth, S. and de Jong, M.D.T. (2017) 'The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review', *Telematics and Informatics*, 34(7), pp. 1038–1058. Available at: https://doi.org/10.1016/j.tele.2017.04.013

Berger-Walliser, G. (2012) 'The past and future of proactive law: an overview of the development of the proactive law movement. Proactive law in a business environment', in Berger-Walliser, G. and Østergaard, K. (eds) *Proactive law in a business environment*. Copenhagen: DJØF Publishing, pp. 13–31. Available at: https://ssrn.com/abstract=2576761 (Accessed: 18 December 2024).

Bhattacharya, A. (2022) *Applied machine learning explainability techniques: make ML models explainable and trustworthy for practical applications using LIME, SHAP, and more*. Birmingham: Packt Publishing Ltd.

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V. and Lenzini, G. (2021) '"I am definitely manipulated, even when I am aware of it. It's ridiculous!"—Dark patterns from the end-user perspective', in *Proceedings of the 2021 ACM Designing Interactive Systems Conference (DIS '21)*. New York: Association for Computing Machinery, pp. 763–776. Available at: https://doi.org/10.1145/3461778.3462086

Bouchagiar, G. (2018) 'Privacy and Web 3.0: implementing trust and learning from social networks', *Review of European Studies*, 10(4), pp. 16–28. Available at: https://doi.org/10.5539/res.v10n4p16

Bruwer, R.H.J. and Rudman, R. (2015) 'Web 3.0: governance, risks and safeguards', *Journal of Applied Business Research*, 31(3), pp. 1037–1056. Available at: https://doi.org/10.19030/jabr.v31i3.9241

Chen, T. and Guestrin, C. (2016) 'XGBoost: a scalable tree boosting system', *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 22, pp. 785–794. Available at: https://doi.org/10.1145/2939672.2939785

'Directive (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector'. *Official Journal* L 265, 14 September, pp. 1–66.

Ghalebikesabi, S., Bagdasaryan, E., Yi, R., Yona, I., Shumailov, I., Pappu, A., Shi, C., Weidinger, L., Stanforth, R., Berrada, L., Kohli, P., Huang, P-S. and Balle, B. (2024) 'Operationalizing contextual integrity in privacy-conscious assistants', *ArXiv*, article 2408.02373. Available at: https://doi.org/10.48550/arXiv.2408.02373

Hagan, M. (2020) 'Legal design as a thing: a theory of change and a set of methods to craft a human-centered legal system', *Design Issues*, 36(3), pp. 3–15. Available at: https://doi.org/10.1162/desi_a_00600

Jackson, C.B. and Wang, Y. (2018) 'Addressing the privacy paradox through personalized privacy notifications', *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2), article 68, pp. 1–25. Available at: https://doi.org/10.1145/3214271

Jones, M.L., Kaufman, E. and Edenberg, E. (2018) 'AI and the ethics of automating consent', *IEEE Security & Privacy*, 16(3), pp. 64–72. Available at: https://doi.org/10.1109/msp.2018.2701155

Klitou, D. (2014) *Privacy-invading technologies and privacy by design: safeguarding privacy, liberty and security in the 21st century*. The Hague: T.M.C. Asser Press. Available at: https://doi.org/10.1007/978-94-6265-026-8

Kokolakis, S. (2017) 'Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon', *Computers & Security*, 64(1), pp. 122–134. Available at: https://doi.org/10.1016/j.cose.2015.07.002

Larsson, S. and Heintz, F. (2020) 'Transparency in artificial intelligence', *Internet Policy Review*, 9(2), pp. 1–16. Available at: https://doi.org/10.14763/2020.2.1469

Lundberg, S.M. and Lee, S.-I. (2017) 'A unified approach to interpreting model predictions', *Advances in Neural Information Processing Systems*, 30, pp. 4765–4774. Available at: https://doi.org/10.48550/arXiv.1705.07874

Mazur, J. (2019) 'Automated decision-making and the precautionary principle in EU law', *TalTech Journal of European Studies*, 9(4), pp. 3–18. Available at: https://doi.org/10.1515/bjes-2019-0035

Kenny, E.M., Ford, C., Quinn, M. and Keane, M.T. (2020) 'Explaining black-box classifiers using post-hoc explanations-by-example: the effect of explanations and error-rates in XAI user studies', *Artificial Intelligence*, 294, article 103459. Available at: https://doi.org/10.1016/j.artint.2021.103459

Oviedo, J., Rodriguez, M., Trenta, A., Cannas, D., Natale, D. and Piattini, M. (2024) 'ISO/IEC quality standards for AI engineering', *Computer Science Review*, 54, article 100681. Available at: https://doi.org/10.1016/j.cosrev.2024.100681

Pavelek, O. and Zajíčková, D. (2021) 'Personal data protection in the decision-making of the CJEU before and after the Lisbon Treaty', *TalTech Journal of European Studies*, 11(2), pp. 167–188. Available at: https://doi.org/10.2478/bjes-2021-0020

Pohjonen, S. (2006) 'Proactive law in the field of law', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49. Stockholm: Stockholm Institute for Scandinavian Law, pp. 53–70. Available at: https://www.scandinavianlaw.se/pdf/49-4.pdf (Accessed: 12 September 2024).

Razmetaeva, Y. (2020) 'The right to be forgotten in the European perspective', *TalTech Journal of European Studies*, 10(1), pp. 58–76. Available at: https://doi.org/10.1515/bjes-2020-0004

Rossi, A., Ducato, R., Haapio, H. and Passera, S. (2019) 'When design met law: design patterns for information transparency', *Droit de la consommation*, 122–123(5), pp. 79–121.

Rudman, R. and Bruwer, R. (2016) 'Defining Web 3.0: opportunities and challenges', *The Electronic Library*, 34(1), pp. 132–154. Available at: https://doi.org/10.1108/EL-08-2014-0140

Schartum, D.W. (2006) 'Introduction to a government-based perspective on proactive law: a proactive approach', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49, Stockholm: Stockholm Institute for Scandinavian Law, pp. 35–51. Available at: https://www.scandinavianlaw.se/pdf/49-3.pdf (Accessed: 12 September 2024).

Schomakers, E.M., Lidynia, C. and Ziefle, M. (2019) 'A typology of online privacy personalities: exploring and segmenting users' diverse privacy attitudes and behaviors', *Journal of Grid Computing*, 17(4), pp. 727–747. Available at: https://doi.org/10.1007/s10723-019-09500-3

Solarte-Vásquez, M.C., Järv, N. and Nyman-Metcalf, K. (2016) 'Usability factors in transactional design and smart contracting', in T. Kerikmäe and A. Rull (eds) *The future of law and eTechnologies*, Cham: Springer, pp. 149–176. Available at: https://doi.org/10.1007/978-3-319-26896-5_8

Solarte-Vásquez, M.C. and Nyman-Metcalf, K. (2017) 'Smart contracting: a multidisciplinary and proactive approach for the EU digital single market', *Baltic Journal of European Studies*, 7(2), pp. 208–246. Available at: https://doi.org/10.1515/bjes-2017-0017

Taherisadr, M., Stavroulakis, S.A. and Elmalaki, S. (2023) 'AdaPARL: adaptive privacy-aware reinforcement learning for sequential decision making human-in-the-loop systems', in *IoTDI '23: Proceedings of the 8th ACM/IEEE Conference*

on Internet of Things Design and Implementation, pp. 262–274. Available at: https://doi.org/10.1145/3576842.3582325

Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J., Good, N., Wagner, D., Beznosov, K. and Egelman, S. (2018) 'Contextualizing privacy decisions for better prediction (and protection)', in *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Montreal QC: ACM, pp. 1–25. Available at: https://doi.org/10.1145/3173574.3173842

Xi, R. (2024) 'On emerging technologies: the old regime and the proactivity', *Cardozo International & Comparative Law Review*, 8(1), pp. 3–57. Available at: https://doi.org/10.2139/ssrn.4952153