Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Privacy Conscious Integration of Artificial Intelligence and Management Information Systems for Secure and Sustainable Consumer Device Lifecycles in the United States

Latul Hasan
International American University
Md Abutaher Dewan
International American University
Mohammad Hasibul Hasan
International American University
Md Rashel Ahmmed
International American University
Md Didear Hossen
International American University
Muhammed Zakir Hossain
zakir@sub.edu.bd

State University of Bangladesh

Research Article

Keywords: Artificial Intelligence, Management Information Systems, Consumer Devices, Lifecycle Management, Cybersecurity

Posted Date: August 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10408218/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Modern consumer devices are converging into connected product-service systems that encompass tangible products, embedded software, mobile applications, cloud platforms, user profiles, telemetry data, and a network of after-sales support systems. This synergy also presents opportunities for operational value but entails greater risks to privacy, cybersecurity, reparability, and end-of-life (EOL) sustainability. Focus on investigating the relationship of the privacy-oriented lifecycle governance, AI–enabled lifecycle intelligence and MIS-driven lifecycle operation integration, and the secure and sustainable performance of the lifecycle of consumer devices in the U.S. The sample consists of 300 employees from the consumer products business dimension who were examined in a quantitative, cross-sectional manner. The examination of the complete dataset involves an analysis of reliability, a factor analysis, and the computation of correlations and regressions. Regression indicates 42.9% of the variance in secure & sustainable lifecycle performance is explained. MIS-based operational integration has the highest standardized regression coefficient (β = .377) with lifecycle performance, followed by privacy-oriented lifecycle governance (β = .326) and AI-powered lifecycle intelligence (β = .152). These outcomes reveal that the device firms can't operate the privacy, AI, MIS, cybersecurity, and circularity projects independently. Rather, the key to secure and maintainable lifecycle performance lies in the integration of lifecycle privacy accountability, responsible AI–driven decision support, and converged MIS systems integrating records of product, firmware, warranty, repair, security, reverse logistics, and recycling. The business and information systems literature will benefit from this work through an empirical test of a lifecycle-based framework for the digital governance of consumer device ecosystems.

JEL Classification: M15, M10, O33, Q56, K24

1. Introduction

The life cycle management of consumer devices has become a critical business issue because these devices are no longer merely pieces of hardware. The products range from cell phones, smart home devices, routers, wearable, and game consoles to household appliances and Consumer electronic goods are now implemented as interconnected product-service systems of hardware, software, firmware, mobile apps, cloud services, device accounts, telemetry, and service providers' networks *(*Brous et al., 2020; Porter & Heppelmann, 2014; Sicari et al., 2015). Therefore, lifecycle management cannot be restricted to manufacturing and sales only. The problem also touches on secure configuration, consent & account management, data collection, software updates, warranty service, repair, refurbishment, reselling, recycling, and final disposal *(*Fagan et al., 2020; Fagan et al., 2022; Lee & Lee, 2021*)*.

The US is also a useful real-world environment for studying these issues. The US Device market is technologically complex, significant in terms of sales volume and subject to increasing pressures regarding privacy and data security guarantees, right to repair, and the treatment of e-waste. The Federal Trade Commission stated that data collected from network products is subject to privacy and security obligations (Federal Trade Commission, 2015; California State Legislature, 2023; California Department

of Justice, Office of the Attorney General, *2024; New York State Governor's Office (2022)*. The Federal Communications Commission is moving ahead with the voluntary United States Digital Trust Mark program for U.S. Internet of Things (IoT) consumer electronics that voluntarily participate *(*Federal Communications Commission, 2024*)*. The centrality of governance to cybersecurity risk management has also been emphasized in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, which links security performance to management responsibility rather than solely to technical controls *(NIST, 2024)*.

The privacy element is at the core of this lifecycle problem since connected devices may acquire personal, behavioural, contextual, audio-visual, biometric, locational, household, and usage-pattern data. Device use is not the only time a privacy risk may be created. A risk may be present when the device is set up, transferred to another account, repaired, data is moved between devices, refurnished, sold, the cloud is deactivated, components are stripped, discarded, or recycled *(*Cavoukian, 2011; Lee & Lee, 2021; Saura et al., 2024). The ability to securely repair, reassign, or repurpose a device from which sensitive data can still be recovered poses a privacy risk and constitutes an environmental failure. Privacy–conscious lifecycle governance can therefore be defined as a capability to operate in a trusted, compliant-ready and circular-reusable way.

The only thing that remains to be determined is whether the problem is still present today, with 62 million tons of electronic waste produced in 2022, and 82 million tonnes predicted for 2030. On the contrary, an estimated 22.3% of e-waste is collected for recycling *(Balde et al., 2024)*. Recovery activities are a focus of circular economy approaches to resource scarcity and waste, and include product longevity, repair and refurbishment, remanufacturing, and materials retrieval and reuse. *(*Bocken et al., 2016; Geissdoerfer et al., 2017; Kumar & Putnam, 2008*)*. Yet with connected devices, reversing logistics through the physical domain alone is insufficient. There is a need for reliable information on device identity, firmware status, account reset, data deletion, vulnerability history, warranty eligibility, reparability, spare parts availability, and recycling outcomes.

Artificial intelligence (AI) and management information systems (MIS) are tools that enable companies to tackle the challenges of each life cycle stage, but only if their application is controlled. The uses of AI in predictive maintenance, anomaly detection, vulnerability prioritization, repair triage, take-back forecasting, refurbishment grading, spare parts planning, and recycling were analyzed *(*Mikalef & Gupta, 2021; Wamba et al., 2017). Also, AI may create new privacy, explain ability, fairness, accountability and security risks of models that are poorly designed or used without human monitoring *(NIST, 2023;* OECD, 2024*)*. Therefore, MIS capability is important due to the nature of the lifecycle decisions, which necessitate consolidated and auditable data related to product development, support, security and privacy management, warranty service, repair partners, reverse logistics, and recycling data (Bharadwaj, 2000; Laudon & Laudon, 2022; Melville et al., 2004).

Privacy governance, AI capability, MIS capability, cybersecurity, and the circular economy are extensively studied areas, though in isolation from one another. This compartmentalization of knowledge impedes

understanding of how to manage privacy, AI, information systems, repair, cybersecurity, and sustainability together throughout a device's entire life cycle. This study fills this gap and proposes an empirically tested lifecycle framework of operation. This study examines how privacy-conscious lifecycle governance, AI-enabled lifecycle intelligence, and MIS-driven operational integration are associated with secure and sustainable consumer device lifecycle performance in the United States.

This paper makes three main contributions to the literature. Firstly, the paper also adds to the body of literature on privacy by design and privacy risk management by describing privacy governance as an end-to-end capability. Secondly, it connects the capabilities of AI and responsible AI to device life-cycle decisions, such as prediction and repair, security update prioritization, repair decisions, and reverse logistics. Thirdly, it provides evidence that MIS-driven operational integration is a key enabler of the transformation of disparate lifecycle data into safe, reliable and accountable performance outcomes. In the subsequent sections, we will review and discuss the literature, hypotheses, methodology, results, conclusions, recommendations, and limitations, as well as the references.

2. Literature review and hypotheses development

2.1 Consumer device lifecycle management

The management of consumer devices through planning, control, monitoring, and improvement throughout their lifecycle is known as consumer device life cycle management. In a traditional product view, lifecycle management encompasses the design, production, distribution, sales, service, and replacement stages. This expanded socio-technical perspective is necessary for connected consumer devices, since value generation stems from interactions among hardware, software, data, users, cloud services, and ecosystem partners *(*Brous et al., 2020; Porter & Heppelmann, 2014*).* According to the NIST definition, post-purchase services for consumer IoT devices include: identifying the device, configuring the device, ensuring security, controlling the interface, updating firmware, managing cyber state, and maintaining documentation (Fagan et al., 2022).

Lifecycle management is also related to sustainability. The environmental effects are directly related to the extraction of raw materials from the earth, the production processes, energy consumption during device use, reparability, product durability, product reusability, device recycling, and device disposal *(*Bocken et al., 2016; Geissdoerfer et al., 2017). We might also suppose that, through the circular economy, the company acknowledges the durability of its product, closing resource loops and preventing overconsumption of materials through product design, reverse logistics, remanufacturing, and resource recovery *(*Ellen MacArthur Foundation, 2015; Kumar & Putnam, 2008*).* Information transparency is necessary in these operations, as the product's sustainability value cannot be determined without data on product condition, security support, repair capability, spare parts availability, data erase state, and disposal path.

Lifecycle management within connected device markets also encompasses cybersecurity issues. Devices might remain in homes and offices for years, even if the vendor no longer supports them or ownership has changed hands. Lack of update continuity, failure to reset passwords/credentials and delete data, and inadequate device security against threats mean that these devices may pose privacy/security risks *(*Fagan et al., 2020; Sicari et al., 2015). Therefore, secure and sustainable product life cycle management depends on a synchronized strategy of extended product life, continuous cybersecurity, consumer data security, reparability and end-of-life traceability.

2.2 Privacy-conscious lifecycle governance

Privacy-conscious lifecycle governance refers to the policies, practices, accountability mechanisms, and technological solutions firms apply to manage privacy risk across device design, use, service, reuse, and end-of-life. Privacy by Design asserts that organizations proactively embed privacy, keep it inherent, focus on users, set privacy as the default, and ensure security, rather than treat it as an afterthought *(*Cavoukian, 2011*).* NIST's privacy framework frames privacy risk management as an enterprise-level process that encourages innovation while safeguarding people *(NIST, 2020).* In the consumer device ecosystem, this remains particularly important, as personal data often circulates among manufacturers, cloud service providers, application developers, retailers, repair and refurbishment companies, logistics providers, and recyclers.

The privacy lifecycle view is important because data leakage may occur at several stages. During onboarding (the initial account creation and device setup process), users set up accounts, accept privacy terms, and connect devices to networks. Devices may then collect telemetry (automated system data), diagnostics (device health data), images, voice commands, location data, or behavioural patterns during use. Technicians and partners may access device data or customer information during service or refurbishment. Data residues may remain unless proper procedures for deletion, reset, and account transfer are followed during resale or disposal (Lee & Lee, 2021; Weber, 2010*).* Privacy-aware lifecycle governance includes principles such as data minimization (collecting only necessary data), purpose limitation (using data only for specified reasons), consent management, access control (restricting data access), and retention rules (defining how long data is kept), secure deletion, third-party vendor supervision, and auditability (ability to review data handling practices).

Previous studies have found that trust in connected environments is affected by privacy and security concerns. Explicit control processes reduce the likelihood of data misuse or leakage (Sicari et al., 2015; Weber, 2010). Privacy governance may also benefit sustainability in consumer devices. Safe repair, resale, and refurbishment require strong procedures for data removal and access control. Insecure devices are more likely to be discarded. Privacy-aware lifecycle governance can therefore be expected to enhance safe and sustainable lifecycle outcomes.

H1

Privacy-conscious lifecycle governance is positively associated with secure and sustainable consumer device lifecycle performance.

2.3 AI-enabled lifecycle intelligence

AI-enabled lifecycle intelligence is a firm's capacity to use AI, machine learning, analytics, and automated decision support to detect, forecast, assess, and enhance lifecycle decisions. From the perspective of resources and the dynamic capabilities view, it is concluded that a firm's performance increases when it has the capability to recognize threats and opportunities, capture them, and reconfigure its resources in accordance with change *(*Barney, 1991; Teece, 2007*).* AI can assist device lifecycle management by aiding in predictive maintenance, warranty analytics, anomaly detection, vulnerability prioritization, service triage, take-back demand estimation, refurbishment classification and recycling strategies *(*Mikalef & Gupta, 2021; Wamba et al., 2017).

AI brings lifecycle intelligence by changing operational data into predictive insights. Device telemetry and service histories provide insight into the probable failure of components. Vulnerabilities can be prioritized using firmware and incident data. Product condition information can reveal if the product needs repair refurbishment, replacement or disposal. Records of returns and take-backs could aid reverse logistics planning. Nonetheless, AI-powered life cycle intelligence has its own caveats. In accordance with NIST's AI risk management framework, trustworthy AI is referred to as artificial intelligence that is reliable, secure, resilient, safe, dependable, responsible, transparent, explainable, privacy-preserving, and fair *(NIST, 2023).*

In a consumer-device context, Responsible AI is crucial because AI models can affect warranty claims, suggested repairs, the detection of fraudulent transactions, customer service, and lifecycle risk scoring. When these systems are opaque, inaccurate, or biased, or rely on excessive personal data *(*OECD, 2024; Saura et al., 2024), *they can erode trust and create legal or reputational risks. As a result*, organizations leveraging these capabilities need robust and transparent AI-powered lifecycle intelligence—not just as automation, but as a strategic safeguard for consumer trust and brand integrity.

H2

AI-enabled lifecycle intelligence is positively associated with secure and sustainable consumer device lifecycle performance.

2.4 MIS-driven operational integration

MIS is central to effective lifecycle management, providing the backbone for device operations from development through recycling. By supporting functions spanning manufacturing, sales, service, security, privacy, warranty, repairs, reverse logistics, refurbishment, and recycling, MIS enables companies to gather, archive, process, transfer, and analyze information to guide managerial decision-making and

performance (Bharadwaj, 2000; Laudon & Laudon, 2022; Melville et al., 2004). Without integrated information systems, the entire device lifecycle becomes fragmented, opaque, and difficult to control.

MIS-driven operations integration demonstrates how the system unifies lifecycle data, processes, dashboards, workflows, audit trails, and decision-making *(*Chen et al., 2012). This integration is critical for cross-border and cross-domain data exchange, supporting circularity and sustainability by enabling material reuse, repair, and refurbishment within a circular economy framework (Dragomir & Duțescu, 2022; Schumacher & Green, 2023; Babbitt et al., 2011).

To ensure lifecycle reliability, MIS should link product serials, firmware versions, vulnerability alerts, update histories, service times, warranty and repair records, data deletion logs, parts data, and external provider access. These features reinforce MIS's role in managing and tracking every aspect of the lifecycle.

Robust lifecycle management through MIS aligns with circular economy principles by extending product lifespans through repair, refurbishment, and remanufacturing. This is achieved through strong data governance, traceability, and standardization (Schumacher et al., 2023; Renckens, 2008; Khompatraporn, 2021). Data-rich MIS enables informed decisions on asset disposition, refurbishment, and compliance with regulatory and environmental standards (McMahon et al., 2023; Islam et al., 2022; Gaur et al., 2024).

Consistent with IT business value literature, MIS delivers performance benefits when paired with organizational capabilities (Bharadwaj, 2000; Melville et al., 2004). Digital transformation research highlights that firms require not only technologies but also process redesign and integrated data (Vial, 2019). Ultimately, MIS-driven integration makes privacy policies, AI intelligence, cybersecurity, and circular practices visible, auditable, and manageable, strengthening lifecycle control.

H3

MIS-driven operational integration is positively associated with secure and sustainable consumer device lifecycle performance.

2.5 Research framework

A framework is described to link three organizational competencies-privacy-aware lifecycle governance, AI-based lifecycle intelligence and MIS-driven operational integration- to safe and reliable consumer devices lifecycle performance. The framework diagram is illustrated in Fig. 1.

Table 1
Constructs and operational definitions

Construct	Code	Operational definition	Core dimensions
Privacy-conscious lifecycle governance	PCLG	The degree to which a firm governs risks about privacy across the device lifecycle.	Data minimization, Assessment of the privacy risk, Management of storage/removal, Access by repair-partner, Accountability of the life cycle.
AI-enabled lifecycle intelligence	AILI	Level of adoption of AI/analytics for predictive and responsible lifecycle decision-making.	Predictive maintenance, Prioritization of vulnerabilities, Recommendation of repairs/refurbishments, Forecasting returns, Responsible AI monitoring
MIS-driven operational integration	MISOI	The degree to which MIS links together lifecycle data, workflows, audit trails, and interdepartmental decisions.	Consolidated Product Records; Dashboards; Audit trails; Workflow automation; Reverse Logistics/Recycling visibility.
Secure and sustainable consumer device lifecycle performance	SSCDLP	The extent to which the firm can secure data, maintain data integrity, facilitate circularity, and build trust throughout the device's entire lifecycle.	Continuity for Updates, less exposure of data, effective for repair/refurbishment, traceable for recycling, consumer confidence.

Note. All of the previously stated constructs were measured using a five item measure that contained five choices on a **5-point Likert-scale.**

3. Methodology

3.1 Research design and sample

This paper explored correlations among privacy-oriented lifecycle governance, AI-driven lifecycle intelligence, MIS-driven operational integration, and secure, sustainable consumer device lifecycle performance using a quantitative cross-sectional survey. The study design is valid because it explores correlations between preconceived ideas using verified measurements. Target respondents were U.S. professionals working in areas related to the consumer-device life cycle, including MIS/IT, operations, cybersecurity/privacy, lifecycle service, repair and refurbishment, reverse logistics, and sustainability.

The final data set consists of 300 valid responses. Completeness was checked prior to analysis, revealing no missing data in demographics, scale items, or scale means. The sample focused on professionals involved in the product lifecycle and used a purposive professional sample rather than a consumer sample. This method is well-suited to organizational research, where respondents must understand device lifecycle processes, information systems, privacy processes, and operational performance.

3.2 Measurement instrument

The questionnaire consisted of demographic and organizational items, followed by 20 construct items. The privacy-aware lifecycle management was assessed through questions covering data minimization, privacy risk assessment, retention/deletion controls, and repair partner access and privacy responsibility for lifecycle management. AI lifecycle intelligence was assessed using items on predictive maintenance, prioritization of vulnerabilities, support for repair/refurbishment decision-making, prediction of returns, and AI-responsible monitoring. MIS-driven operational integration was examined using integrated records, dashboards, audit trails, automated workflows and reverse-logistics visibility. The life-cycle performance was ensured by update continuity, minimal data exposure, efficient repair/refurbishment, traceable recyclability, and consumer trust.

Each item of each construct was rated on a 5-point Likert scale (1 = strongly disagree, 5 = Strongly Agree). Artifacts were extracted from privacy by design, privacy risk management, AI capacity, AI risk management, information systems capacity, IT business value, IoT security and literature on the circular economy (Bharadwaj, 2000; Bocken et al., 2016; Cavoukian, 2011; Fagan et al., 2022; Hair et al., 2019; Mikalef & Gupta, 2021; *NIST, 2020; NIST, 2023;* Wamba et al., 2017). All of the questionnaire items are shown in Appendix A

3.3 Data analysis procedure

A staged data analysis approach was followed. Firstly, a descriptive profile of respondents based on demographic and organizational attributes was developed using frequency analysis. Secondly, descriptive statistics and Cronbach's alpha were computed for all constructs. Thirdly, the measurement model was assessed using the Kaiser-Meyer-Olkin statistic, the Bartlett test of sphericity, exploratory factor analysis, composite reliability, average variance extracted (AVE), the Fornell-Larcker criterion (Fornell & Larcker, 1981), and the heterotrait-monotrait (HTMT) ratio. Fourthly, common-method bias was assessed using Harman's single-factor test (Podsakoff et al., 2003). Finally, the hypothesis was tested through multiple regression and Pearson's correlations.

Multiple regressions were used to test how the three independent variables relate concurrently to the dependent variable. Standardized betas, t values, p values, confidence intervals, tolerance values and VIF values have been added to the output to assist interpretation. Multicollinearity was considered acceptable when the VIF was below 5.00, and the tolerance was above 0.2010 *(*Hair et al., 2019). The independence of the residuals was tested using the Durbin-Watson statistic. A second test for the degree of heteroscedasticity was performed with the Breusch-Pagan test. The fact that these data are self-reported and cross-sectional means we cannot infer causality and can only assume association.

3.4 Ethical considerations and data availability

Ethical approval

was obtained where needed, following best practices for anonymous, low-risk social science surveys. Only adult professionals participated; no clinical settings, deception, vulnerable populations, medical data, or sensitive identifiers were involved. Thus, formal institutional ethics approval was not required.

The questionnaire was given only after participants received an information sheet describing the research, voluntary participation, and a 15-minute duration. Participants could decline or withdraw at any point, and data from those who withdrew were excluded. Electronic consent was secured before the survey began. No personal, contact, device, employer, or other identifiable data were collected. The anonymised dataset is secured, accessible only for academic study, and results are reported only as aggregate summaries. No individual or organization can be identified. The anonymised data is available as an additional file or upon request.

4. Results

4.1 Respondent profile

The respondent's profile is outlined and presented in Table 2. The sample represents diverse age groups, functional positions, industry segments, work experience, firm size, and device classes, which are appropriate for investigating consumer device lifecycle management as a cross-functional business and IS problem.

Table 2
Respondent profile

Variable	Category	Frequency	Percentage (%)
Age group	18–29 years	55	18.3
	30–39 years	122	40.7
	40–49 years	76	25.3
	50 years and above	47	15.7
Gender	Male	164	54.7
	Female	123	41.0
	Prefer not to say	13	4.3
Professional role	MIS/IT manager or analyst	36	12.0
	Operations/supply chain manager	63	21.0
	Cybersecurity/privacy/compliance professional	42	14.0
	Product/service lifecycle professional	44	14.7
	Sustainability/reverse logistics professional	40	13.3
	Repair/refurbishment/warranty professional	43	14.3
	Other relevant professional	32	10.7
Industry segment	Consumer electronics manufacturing	74	24.7
	Smart-home/consumer IoT products	63	21.0
	Electronics retail/warranty services	37	12.3
	Repair/refurbishment services	49	16.3
	Reverse logistics/recycling services	23	7.7
	Cybersecurity, privacy, IT, or related services	44	14.7
	Other related consumer-device firm	10	3.3
Experience	1–5 years	64	21.3
	6–10 years	79	26.3
	11–15 years	82	27.3

Notes: **n = 300.** Labels used to denote categories correspond to those in the survey codebook accompanying the data file.

Variable	Category	Frequency	Percentage (%)
	More than 15 years	75	25.0
Firm size	Fewer than 100 employees	54	18.0
	100–499 employees	98	32.7
	500–999 employees	74	24.7
	1,000 employees or more	74	24.7
Device category	Smartphones, tablets, or wearables	66	22.0
	Smart-home or consumer IoT devices	83	27.7
	Routers or network devices	36	12.0
	Gaming or personal electronics	40	13.3
	Household electronic appliances	31	10.3
	Mixed consumer-device portfolio	44	14.7

Notes: **n = 300.** Labels used to denote categories correspond to those in the survey codebook accompanying the data file.

4.2 Descriptive statistics and reliability

Descriptive statistics and analyses for internal consistency for the four constructs appear in Table 3. Average scores are above the midpoint of the 5-point scale, suggesting a perception of medium-to-high implementation of lifecycle privacy governance, lifecycle intelligence powered by AI, integration of MIS, and lifecycle performance in terms of safety and sustainability. The range of Cronbach's alpha values was 0.843 to 0.896, all within the accepted threshold of > 0.70.

Table 3
Descriptive statistics and reliability

Construct	Items	Mean	SD	Cronbach alpha	Decision
Privacy-conscious lifecycle governance (PCLG)	5	3.451	1.007	0.884	Reliable
AI-enabled lifecycle intelligence (AILI)	5	3.393	0.921	0.843	Reliable
MIS-driven operational integration (MISOI)	5	3.402	0.977	0.875	Reliable
Secure and sustainable lifecycle performance (SSCDLP)	5	3.484	1.030	0.896	Reliable

Note. Likert Scale applied: 1 = Strongly Disagree 5 = Strongly Agree

4.3 Measurement validity and common method bias diagnostics

The measurement diagnostics provide evidence that the data are suitable for construct-level analysis. All number of samples are good- KMO value = 0.924, and Bartlett's test of sphericity is significant (Chi-square = 3185.77, df = 190, p<.001). All factors are factors. The exploratory factor analysis resulted within the desired 4-factor solution, and the four rotated factors accounted for 67.66% of the variance. Harman's single-factor test shows that only 38.08% of the variance is explained by the first unrotated factor. This is below the typical acceptable standard of 50%. These findings suggest that common method bias does not severely dominate other findings.

Table 4
Measurement validity summary

Construct	Rotated loading range	Composite reliability	AVE	Decision
Privacy-conscious lifecycle governance (PCLG)	0.755–0.828	0.916	0.686	Supported
AI-enabled lifecycle intelligence (AILI)	0.728–0.798	0.890	0.618	Supported
MIS-driven operational integration (MISOI)	0.761–0.786	0.911	0.672	Supported
Secure and sustainable lifecycle performance (SSCDLP)	0.741–0.823	0.924	0.710	Supported
Note. AVE = average variance extracted. The reliability measures, composite reliability and AVE were calculated using the standardized factor loadings of the items.				

The Fornell-Larcker discriminant reliability matrix is presented as shown in Table 5. The square root of AVE for all constructs is greater than the construct correlations. HTMT values range from 0.368 to 0.609, which are well below the rigorous threshold of 0.85. All four factors thus clearly distinguished themselves from one another.

Table 5
Fornell-Larcker discriminant validity matrix

Construct	PCLG	AILI	MISOI	SSCDLP
PCLG	0.828	0.348	0.324	0.502
AILI	0.348	0.786	0.372	0.406
MISOI	0.324	0.372	0.819	0.539
SSCDLP	0.502	0.406	0.539	0.843

Note. All the diagonal entries are sqrt of the AVE and the off-diagonal entries are Pearson correlations.

4.4 Correlation analysis

Table 6 presents the Pearson correlations among the constructs. Secure and sustainable lifecycle performance is significantly and positively correlated with privacy-sensitive lifecycle governance, AI-driven lifecycle intelligence and MIS-based operational integration. The strongest bivariate association exists between MIS-driven operational integration and lifecycle security and sustainability.

Table 6
Correlation matrix

Variable	Mean	SD	1	2	3	4
1. PCLG	3.451	1.007	1			
2. AILI	3.393	0.921	0.348**	1		
3. MISOI	3.402	0.977	0.324**	0.372**	1	
4. SSCDLP	3.484	1.030	0.502**	0.406**	0.539**	1

Note. ** P < .01. PCLG, privacy-conscious lifecycle governance; AILI, AI-enabled lifecycle intelligence; MISOI, MIS-driven operational integration; SSCDLP, secure and sustainable consumer device lifecycle performance.

4.5 Regression analysis and hypothesis testing

Three hypotheses were assessed using multiple regression analysis. The model is significant, $F(3,296) = 74.05$, $p < .001$, R-squared = .429, adjusted R-squared = .423, indicating that 42.9% of the variance in the secure & sustainable life cycle of consumer device performance can be explained by three variables. The value of Durbin-Watson = 2.024. This seems acceptable. VIF ranged from 1.198 to 1.244, and tolerance values ranged from 0.804 to 0.835, indicating no multicollinearity. The Breusch-Pagan test result ($p = 0.927$) is not significant, indicating no evidence of heteroscedasticity.

Table 7
Multiple regression results

Predictor	B	SE	Beta	t	p	95% CI LL	95% CI UL	Tolerance	VIF
Constant	0.402	0.217		1.849	0.065	-0.026	0.830		
Privacy-conscious lifecycle governance	0.334	0.049	0.326	6.790	< .001	0.237	0.431	0.835	1.198
AI-enabled lifecycle intelligence	0.170	0.055	0.152	3.108	0.002	0.062	0.278	0.804	1.244
MIS-driven operational integration	0.397	0.051	0.377	7.757	< .001	0.297	0.498	0.818	1.222
Note. Dependent variable: SSCDLP. R-squared = **0.429**, Adjusted R-squared = 0.423, F (3, 296) = 74.05, Durbin-Watson = 2.024									

The regression outcomes validate all three hypothesized effects. The association between privacy-responsive lifecycle governance and secure, sustainable lifecycle performance is positive and significant (β = .326, p < .001), which provides support for. AI-based lifecycle intelligence is positively and significantly related to safe and sustainable lifecycle performance (β = .152, p = .002), which supports. The relationship with MIS-based operational integration is the strongest positive one (β = .377, p < .001), which supports.

Table 8
Hypothesis-testing summary

Hypothesis	Standardized beta	p-value	Decision
H1: PCLG is positively associated with SSCDLP.	0.326	< .001	Supported
H2: AILI is positively associated with SSCDLP.	0.152	0.002	Supported
H3: MISOI is positively associated with SSCDLP.	0.377	< .001	Supported
Note. For all the hypotheses SSCDLP was regressed against using multiple regression.			

5. Discussion

The paper finds that privacy-conscious lifecycle governance, AI-enabled lifecycle intelligence, and MIS-driven operational integration each have a significant positive association on secure and sustainable lifecycle performance for consumer devices in the US, collectively explaining 42.9% of the variance. These findings provide strong empirical support for the proposed model. Notably, secure and sustainable lifecycle management cannot rely on isolated technical tools or compliance programs; it requires a unified capability that integrates governance, intelligence, and information systems.

The positive correlation between privacy-sensitive lifecycle management and lifecycle performance confirms H1. Companies that collect less data, evaluate privacy risks before shipping devices, manage retention and deletion controls, limit data access for repair partners, and assign privacy responsibility throughout the lifecycle are more likely to achieve good, secure, and sustainable lifecycle performance. This aligns with "privacy-by-design" principles, which state privacy should be integrated into systems and processes from the initial design (Cavoukian, 2011), and the NIST Privacy Framework, which identifies privacy risk management as an enterprise capability (NIST, 2020). The result also indicates that privacy governance may indirectly promote circularity: If data can be deleted or secured, devices can more easily transition into repair, resale, or refurbishment channels.

The positive relationship between AI-enhanced lifecycle intelligence and lifecycle performance supports this finding. Specifically, AI and analytics help firms anticipate device failures, prioritize security updates, inform repair and refurbishment decisions, predict reverse-logistics needs, and guide decision-making throughout the lifecycle. This aligns with AI capability literature, which claims that AI resources drive superior performance when combined with organizational capabilities and data (Mikalef & Gupta, 2021; Wamba et al., 2017). However, the smaller standardized coefficient compared to other predictors suggests that AI alone is insufficient. Value is generated when AI is integrated into operating systems and implemented with responsible governance. This view also aligns with the NIST AI Risk Management Framework principles for valid, secure, privacy-enhancing, transparent, and accountable AI (NIST, 2023).

The MIS-driven operation integration shows a high correlation with secure and sustainability lifecycle performance, providing backing for. This demonstrates that integrated information systems are crucial for life cycle improvement. Without MIS integration, privacy policies may not connect to repair processes, AI findings may not be disseminated to shop floor personnel, security update information may not be tied to warranty information, and recyclability performance cannot be readily audited. The integrated MIS links product identity to the following: firmware version, consent records, warranty claims, repair records, vulnerability issues, replacement parts, take-back information, refurbishment results, and recycling details. This finding aligns with the literature on IT business value, in which the value of information systems realized through its utilization in business processes and decision-making routines (Bharadwaj, 2000; Melville et al., 2004).

Overall, it indicates that safely and sustainably performing life cycle management of consumer devices is a multi-dimensional outcome. Privacy governance establishes rules, establishes accountability and protects consumer data. AI-powered lifecycle intelligence allows you to predict, prioritize, and optimize. A MIS-driven operational integration links the capabilities across departments and between partners. Consequently, the results confirm a lifecycle-centered view of digital governance in which privacy, AI, MIS, cybersecurity, and the circular economy interact positively.

6. Implications

6.1 Theoretical implications

The first theoretical consequence is that privacy management could be conceptualized as an operational capability, rather than purely a legal compliance function. By spanning the different phases of a system lifecycle-design, use, service, transfer, refurbishment, and disposal- privacy governance helps bridge privacy-by-design and privacy risk management to the lifecycle operations.

Second, AI capacity must be aligned with lifecycle governance and the integration of information systems. The results support the idea that AI-powered intelligence improves performance. However, its relationships are strongest when AI outputs are explainable, monitored, and linked to operations. This adds to research on AI capabilities and shifts the focus from firm performance to secure, sustainable lifecycle outcomes.

Finally, the third implication is that integrating MIS can turn fragmented lifecycle data into clear, auditable performance output. This integration applies IT business value theory to devices and shows how information systems manage privacy, cybersecurity, repairs, refurbishment, and end-of-life sustainability.

6.2 Managerial implications

Managers should view the consumer device lifecycle as an enabling capability, not just a post-sale activity. Firms must embed privacy controls at every stage—onboarding, support, repair, refurbishment, resale, recycling, and disposal—and ensure data minimization, consent tracking, limited data retention, deletion records, service-partner access controls, and lifecycle responsibility.

Similarly, managers must implement AI cautiously and responsibly. AI is applicable to predictive maintenance, vulnerability prioritization, repair triage, return forecasting, refurbishment grading, and recycling. Nonetheless, companies should also take measures to ensure that AI-powered lifecycle decisions are transparent to consumers regarding privacy, fairness, accuracy, and accountability. If a warranty claim is granted, or consumer confidence in a product is affected.

Lastly, companies should consider integrating their MIS platforms to consolidate product records, firmware history, warranty claims, repair tickets, privacy logs, vulnerability reports, parts-replacement inventory, reverse-logistics information, refurbishment success reports, and recycling data. This approach allows managers to achieve greater continuity of updates, reduce exposure to risk in data-safe devices, streamline repair and refurbishment processes, track end-of-life outcomes, and instil customer confidence in environmentally friendly and secure device management.

6.3 Policy implications

These are also policy-relevant. This demonstrates the overlap between data privacy legislation, cybersecurity labels, right-to-repair laws, and e-waste laws. This life cycle transparency should be incentivised by policymakers through proposals for standards on update maintenance support, safe data disposal, repair tracking, remanufacturing warranty, and e-waste tracking. Companies that treat these shifts as strategic signals rather than episodic compliance exercises will have a stronger advantage in fostering environments of consumer-device trust.

7. Limitations and future research

There are limitations inherent in each of these explanations of the results. First, the data are cross-sectional; thus, causal inferences cannot be made. Although regression analysis revealed statistically significant correlations among the variables, longitudinal research is necessary to determine whether privacy governance, AI-driven smart technologies, and MIS standardization enhance overall performance throughout the life cycle. Second, the study relies on self-report, making it susceptible to response bias. While measures and checks for common method bias were employed, future research may benefit from integrating survey and archival measures, such as time since up-deployment, repair cycle time, data-deletion logs, refurbishment yield, and recycling certificates.

Thirdly, US practitioners are included in the sample. Building on this, future research could undertake comparative analyses of the US, EU, Japan, Korea, and developing countries by examining divergent policies on privacy, right to repair, cybersecurity, and waste-treatment infrastructure. Fourthly, the current model includes three predictors. Future research may incorporate mediators such as consumer readiness, trust, resilience to cybersecurity threats, readiness for compliance, capacity for circular economy, or operational agility. Additionally, moderators such as firm size, product category, data sensitivity, regulatory pressure, and supply chain complexity may yield further insights. Fifthly, qualitative case studies could examine how leading device firms manage privacy controls, AI life-cycle intelligence, and MIS.

8. Conclusion

In this paper, we introduce and validate a privacy-aware, AI-enabled, MIS-driven framework for secure and sustainable consumer device lifecycle management in the U.S. A survey of 300 practitioners shows that privacy-oriented lifecycle governance, AI-supported lifecycle intelligence, and MIS-oriented operational integration are strongly and positively associated with safe and sustainable lifecycle performance. The closest relationship appears with MIS-driven operational integration, followed by privacy-aware governance and AI-driven intelligence.

The study demonstrates that relying only on technical cybersecurity controls or separate sustainability programs does not ensure sustainable, secure device lifecycle management. Achieving this goal requires aligning privacy accountability, responsible AI-driven lifecycle management, and MIS systems to connect lifecycle data across departments and partners. The main takeaway for consumer device companies is that lifecycle management should be viewed as a safe, privacy-friendly, AI-enabled, and MIS-integrated operational capability spanning from design to end-of-life.

Declarations

Author contributions

Muhammed Zakir Hossain: Conceptualization, methodology, supervision, project administration, validation, and writing—review and editing.

Latul Hasan: Conceptualization, investigation, data curation, formal analysis, visualization, and writing—original draft.

Md Abutaher Dewan: Conceptualization, investigation, methodology, validation, and writing—review and editing.

Mohammad Hasibul Hasan: Investigation, data curation, resources, visualization, and writing—original draft.

Md Rashel Ahmmed: Methodology, formal analysis, validation, and writing—review and editing.

Md Didear Hossen: Investigation, data curation, resources, visualization, and writing—original draft.

All authors reviewed and approved the final version of the manuscript and agreed to be accountable for their respective contributions to the work.

Funding

There was no specific fund for undertaking this work the paper authors.

Conflict of interest

The authors are unaware of any actual or potential conflicts of interest on the part of any of the parties involved in this agreement.

Data availability statement

The anonymised data are attached or can be requested from the corresponding author.

Ethics statement

The study protocol was reviewed and approved by the Ethical Review Committee of State University of Bangladesh (SUB) (approval reference SUB/PH/H-ERC/2025/19; approval date 1 December 2025). The research was conducted in accordance with the ethical guidelines and regulations prescribed by the committee.

Consent to participate

Freely given electronic informed consent to participate was obtained from all participants before they accessed the survey questionnaire. Participants received an information sheet explaining the purpose of the study, the expected duration of participation, the voluntary nature of participation, the confidentiality

and anonymity of their responses, and their right to decline participation or withdraw without penalty. Only adults who provided informed consent were permitted to participate in the study.

Acknowledgements

Thanks to all that have taken the survey. Any remaining mistakes are the responsibility of the authors.

References

1. Babbitt CW, Williams E, Kahhat R. Institutional disposition and management of end-of-life electronics. Environ Sci Technol. 2011;45(12):5366–72. https://doi.org/10.1021/es1028469.
2. Baldé CP, Kuehr R, Yamamoto T, McDonald R, D'Angelo E, Althaf S, Bel G, Deubzer O, Fernandez-Cubillo E, Forti V, Gray V, Herat S, Honda S, Iattoni G, Khetriwal DS, di Luda V, Lobuntsova Y, Nnorom I, Pralat N, Wagner M. The global e-waste monitor 2024. International Telecommunication Union; United Nations Institute for Training and Research; 2024. https://ewastemonitor.info/the-global-e-waste-monitor-2024/.
3. Barney J. Firm resources and sustained competitive advantage. J Manag. 1991;17(1):99–120. https://doi.org/10.1177/014920639101700108.
4. Bharadwaj AS. A resource-based perspective on information technology capability and firm performance: An empirical investigation. MIS Q. 2000;24(1):169–96. https://doi.org/10.2307/3250983.
5. Bocken NMP, de Pauw I, Bakker C, van der Grinten B. Product design and business model strategies for a circular economy. J Industrial Prod Eng. 2016;33(5):308–20. https://doi.org/10.1080/21681015.2016.1172124.
6. Brous P, Janssen M, Herder P. The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. Int J Inf Manag. 2020;51:101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008.
7. California Department of Justice, Office of the Attorney General. (2024, March 13). *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa
8. California State Legislature. (2023). *SB-244 Right to Repair Act (2023–2024).* California Legislative Information. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB244
9. Cavoukian A. (2011). Privacy by design: The 7 foundational principles—Implementation and mapping of fair information practices. Inform Priv Commissioner Ont. https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
10. Chen H, Chiang RHL, Storey VC. Business intelligence and analytics: From big data to big impact. MIS Q. 2012;36(4):1165–88. https://doi.org/10.2307/41703503.
11. Dragomir VD, Duţescu A. (2022). New business models in the circular economy. *Proceedings of the International Conference on Business Excellence, 16*(1), 792–804. https://doi.org/10.2478/picbe-2022-0074

12. Ellen MacArthur Foundation. (2015). *Towards a circular economy: Business rationale for an accelerated transition*. https://www.ellenmacarthurfoundation.org/towards-a-circular-economy-business-rationale-for-an-accelerated-transition
13. Fagan M, Marron J, Brady K, Cuthill B, Herold R, Hoehn B, Lemire D. (2022). *Profile of the IoT core baseline for consumer IoT products* (NIST IR 8425). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8425
14. Fagan M, Megas KN, Scarfone K, Smith M. (2020). *IoT device cybersecurity capability core baseline* (NIST IR 8259A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259A
15. Federal Communications Commission. Cybersecurity labeling for Internet of Things. Fed Reg. 2024;89(146):61242–79. https://www.federalregister.gov/documents/2024/07/30/2024-14148/cybersecurity-labeling-for-internet-of-things.
16. Federal Trade Commission. (2015, January). *Internet of Things: Privacy & security in a connected world*. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
17. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J Mark Res. 1981;18(1):39–50. https://doi.org/10.2307/3151312.
18. Gaur TS, Yadav V, Mittal S, Sharma MK. A systematic review on sustainable e-waste management: Challenges, circular economy practices, and a conceptual framework. Manage Environ Quality: Int J. 2024;35(4):858–84. https://doi.org/10.1108/MEQ-05-2023-0139.
19. Geissdoerfer M, Savaget P, Bocken NMP, Hultink EJ. The circular economy—A new sustainability paradigm? J Clean Prod. 2017;143:757–68. https://doi.org/10.1016/j.jclepro.2016.12.048.
20. Hair JF, Black WC, Babin BJ, Anderson RE. Multivariate data analysis. 8th ed. Cengage Learning; 2019.
21. Islam MT, Iyer-Raniga U, Trewick S. Recycling perspectives of circular business models: A review. Recycling. 2022;7(5). Article 79. https://doi.org/10.3390/recycling7050079.
22. Khompatraporn C. (2021). Circular supply chain management. In L. Liu and S. Ramakrishna, editors, *An introduction to circular economy* (pp. 419–435). Springer. https://doi.org/10.1007/978-981-15-8510-4_21
23. Kumar V, Putnam V. Cradle to cradle: Reverse logistics strategies and opportunities across three industry sectors. Int J Prod Econ. 2008;115(2):305–15. https://doi.org/10.1016/j.ijpe.2007.11.015.
24. Laudon KC, Laudon JP. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson.
25. Lee Y, Lee GY. Security management suitable for lifecycle of personal information in multi-user IoT environment. Sensors. 2021;21(22). Article 7592. https://doi.org/10.3390/s21227592.
26. McMahon K, Uchendu C, Fitzpatrick C. Characterizing IT asset disposition flows for the circular economy: A case study on export for reuse from Ireland. J Ind Ecol. 2023;27(4):1212–22. https://doi.org/10.1111/jiec.13406.

27. Melville N, Kraemer K, Gurbaxani V. Review: Information technology and organizational performance: An integrative model of IT business value. MIS Q. 2004;28(2):283–322. https://doi.org/10.2307/25148636.
28. Mikalef P, Gupta M. Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. Inf Manag. 2021;58(3). Article 103434. https://doi.org/10.1016/j.im.2021.103434.
29. National Institute of Standards and Technology. (2020). *NIST privacy framework: A tool for improving privacy through enterprise risk management* (Version 1.0). https://doi.org/10.6028/NIST.CSWP.01162020
30. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1
31. National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
32. New York State Governor's Office. (2022, December 29). *Governor Hochul signs the Digital Fair Repair Act into law*. https://www.governor.ny.gov/news/governor-hochul-signs-digital-fair-repair-act-law
33. OECD. (2024). *AI, data governance and privacy: Synergies and areas of international co-operation* (OECD Artificial Intelligence Papers No. 22). https://doi.org/10.1787/2476b1a4-en
34. Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: A critical review of the literature and recommended remedies. J Appl Psychol. 2003;88(5):879–903. https://doi.org/10.1037/0021-9010.88.5.879.
35. Porter ME, Heppelmann JE. How smart, connected products are transforming competition. Harvard Business Rev. 2014;92(11):64–88. https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition.
36. Renckens S. Yes, we will! Voluntarism in U.S. e-waste governance. Rev Eur Community Int Environ Law. 2008;17(3):286–99. https://doi.org/10.1111/j.1467-9388.2008.00605.x.
37. Saura JR, Škare V, Ozretić Došen Đ. Is AI-based digital marketing ethical? Assessing a new data privacy paradox. J Innov Knowl. 2024;9(4). Article 100597. https://doi.org/10.1016/j.jik.2024.100597.
38. Schumacher K, Last N, Morris K, Ferrero V, Hapuwatte B, Mathur N, Reslan M. Fostering a circular economy of manufacturing materials: Workshop report 2022. ASTM Int. 2023. https://doi.org/10.1520/. amcoe-economy-of-manufacturing-materials.
39. Schumacher KA, Green ML. Circular economy in a high-tech world. Circular Econ Sustain. 2023;3(2):619–42. https://doi.org/10.1007/s43615-022-00220-7.
40. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Comput Netw. 2015;76:146–64. https://doi.org/10.1016/j.comnet.2014.11.008.
41. Teece DJ. Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strateg Manag J. 2007;28(13):1319–50. https://doi.org/10.1002/smj.640.

42. Vial G. Understanding digital transformation: A review and a research agenda. J Strateg Inf Syst. 2019;28(2):118–44. https://doi.org/10.1016/j.jsis.2019.01.003.
43. Wamba SF, Gunasekaran A, Akter S, Ren SJ-F, Dubey R, Childe SJ. Big data analytics and firm performance: Effects of dynamic capabilities. J Bus Res. 2017;70:356–65. https://doi.org/10.1016/j.jbusres.2016.08.009.
44. Weber RH. Internet of Things—New security and privacy challenges. Comput Law Secur Rev. 2010;26(1):23–30. https://doi.org/10.1016/j.clsr.2009.11.008.

Figures

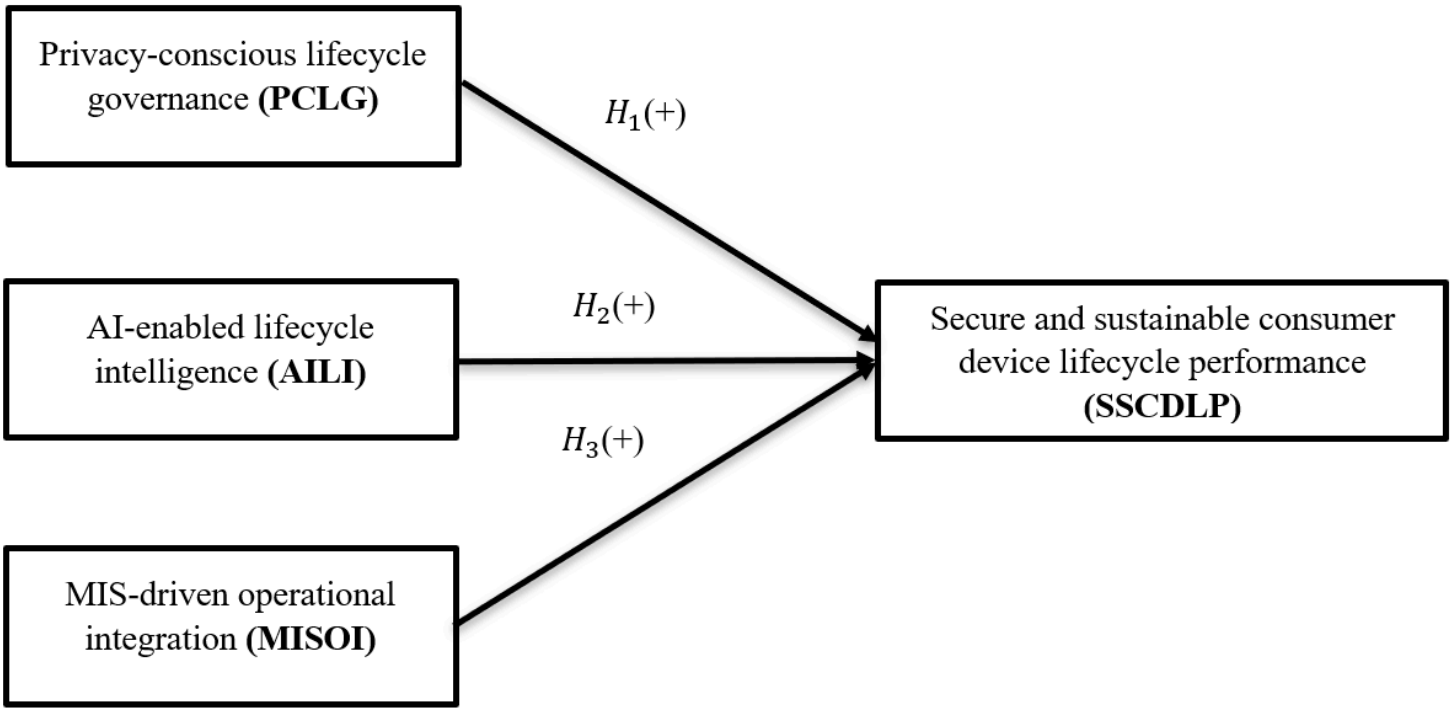


Figure 1

Conceptual research framework

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Appendix.docx