UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Digital Economics and Business

Biometric Data Governance and Consumer Trust: The Role of Storage Architecture in Digital Payment Adoption

Relatore: Prof. Andrea Perna

Rapporto Finale di: Mariam Motsikulashvili

Anno Accademico 2025/2026

INDEX

ABSTRACT 3

INTRODUCTION 4

CHAPTER I : BIOMETRICS AND THE CONSUMER: PRIVACY, TRUST, AND GOVERNANCE 6

I.1 BIOMETRICS IN DIGITAL PAYMENTS 6
I.2 CONSUMER TRUST, PRIVACY AND PERCEIVED CONTROL 8
I.2.1 Privacy Calculus and the Privacy Paradox 9
I.2.2 Perceived Risk and Non-Financial Vulnerabilities 9
I.2.3 Trust, Control, and Adoption Intention 10
I.3 BIOMETRIC DATA GOVERNANCE MODELS 11
I.3.1 Centralized Storage and Market Risk 11
I.3.2 The GDPR Constraint 12
I.3.3 Decentralized Storage as a Strategic Solution 13

CHAPTER II: CONCEPTUAL FRAMEWORK AND METHODOLOGY 15

II.1 PROPOSED CONCEPTUAL FRAMEWORK 15
II.2 MODEL PROPOSITIONS 16
II.3 RESEARCH APPROACH 17

CHAPTER III: DISCUSSION AND MANAGERIAL IMPLICATIONS 18

III.1 SYNTHESIS OF FINDINGS 18
III.2 MANAGERIAL RECOMMENDATIONS 19
III.3 LIMITATIONS AND FUTURE RESEARCH 20

CONCLUSION 21

Abstract

This thesis explores a crucial barrier to consumer adoption and purchase intention in biometric payment systems, corporate biometric data governance. Biometric authentication undoubtedly offers efficiency and convenience by reducing checkout friction, however, the irreversible and unique nature of biological traits (face, fingerprints, iris) raises severe security concerns and certain behavioural dilemmas. The main part of this thesis is a firm's data governance architecture, what effect does it have whether consumer data is held centrally by a company, or it is decentralized and kept locally on a user's device. My thesis argues that this architectural choice is what shapes risk perception and acts as a primary barrier to consumer trust and adoption in biometric technology. In doing so, it contributes to the broader marketing and consumer behaviour literature on barriers to online purchasing.

To analyze these dynamics, an important contribution of this thesis is the development of the pre-existing traditional trust-risk framework developed by Kim et al. (2008) by integrating a new "Governance Model" variable into the model to better demonstrate the factors that affect the biometric technology adoption and purchase intentions of a consumer.

Through a systematic literature review using databases such as Scopus, Google Scholar, and JSTOR, along with the analysis of real-world examples, such as the Suprema breach in 2019 and the discontinuation of Amazon One palm payments, the findings illustrate that the way firms make choices to store consumers' data heavily outweighs the convenience benefits it may offer. The thesis concludes that a company’s data governance model is a crucial deciding factor in consumer acceptance. Since centralized cloud storage increases perceived risk and reduces consumer trust, firms should strive to make the data governance architecture their priority to overcome the barriers that consumers face in the long-term adoption of biometric systems.

Keywords: Biometric Payments; Data Governance; Digital Marketing; Purchase, Consumer Behaviour

INTRODUCTION

What happens to trust in a system that asks for something a consumer can never take back? It's been a while since fingerprints and faces have quietly replaced passwords as the way for millions of people to prove their identity. As digital transformation accelerates, biometric verification is at the core of how organizations verify identity, secure access, and authorize transactions, with uses in areas ranging from finance to healthcare to border control. Biometrics undoubtedly make checkouts more efficient and convenient for consumers; however, since it relies on unique physical traits such as fingerprints, iris, and facial features that can't be replaced if compromised, it equally raises critical concerns regarding security, data privacy and potential misuse.

This thesis examines how the storage and governance of biometric data (centralized vs decentralized) act as a barrier to consumer trust and purchase intention in biometric payments in e-commerce. It also addresses the gap by exploring how corporate data governance methods influence perceived risk, trust, and consumer willingness to adopt biometric payments in digital commerce. This study provides insights into how these methods address the security challenges inherent in biometric authentication systems.

STATEMENT OF THE PROBLEM

This commercial push poses a critical management dilemma for digital commerce platforms and e-commerce application developers. On one hand, biometric authentication provides massive efficiency and convenience to consumers, reduces

shopping cart abandonment, and creates frictionless checkout experiences. On the other hand, it raises serious privacy anxieties and risks of data theft on the information that is irrevocable and a unique physical trait of the user.

At the heart of biometric adoption lies a fundamental behavioral paradox: consumers are ready to exchange their most unique and sensitive biological data for the convenience of performing immediate transactions, yet they possess a deep-rooted fear of corporate data security, which remains unaddressed.

RESEARCH OBJECTIVE

The primary objective of the thesis is to examine how the consumer perceptions of privacy risk, institutional trust and corporate data governance frameworks influence the adoption of biometric payment in digital commerce. Current research well establishes the benefits of accepting biometric authentication. My research explores how the unchangeable nature of biometric data affects consumer decision-making processes.

To better address the core objective of my thesis, the research is focused on the following research question:
How does the consumer perception of privacy risks and data governance architecture influence the trust and purchasing intentions of B2C e-commerce payment systems?

CHAPTER I : BIOMETRICS AND THE CONSUMER: PRIVACY, TRUST, AND GOVERNANCE

I.1 BIOMETRICS IN DIGITAL PAYMENTS

Authentication systems were created with the fundamental goal of protecting financial accounts and confidential systems from unauthorized access. Research suggests that security evolution could be considered through three primary authentication classes. (A. Domingo et al 2025). The first one is Knowledge-Based models ("Something you know") that includes passwords, security codes and PINs. While these models have been the industry standard for a long time, they are becoming less effective due to user password memorability fatigue and high exposure to cyber-attacks like credential harvesting[1] and brute-force cracking[2]. Possession/Ownership models ("Something you have") including physical cards, smartphones, hardware tokens, although strengthen multi-factor authentication, their main disadvantage is vulnerability to loss, physical theft, and unauthorized duplication. And last one, Inherence-Based Models ("Something You Are") represent the authentication method that relies on unique human traits, such as physical or behavioral biometrics that cannot be lost, shared or misplaced.

A distinction should be made between physical and behavioral biometrics. Behavioral biometrics track learned habits such as typing patterns, voice traits, or signature styles in order to authenticate users via pattern recognition (Patil & Renke, 2016). In contrast, physiological biometrics rely on fixed physical characteristics, including facial structure, fingerprints, iris scans, and hand geometry (A. Domingo et al, 2025). While

[1] A phishing website set up to simply collect usernames and passwords from users by mimicking a legitimate site. **(**National Cyber Security Centre, 2018)**.**
[2] A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords. (National Institute of Standards and Technology)

these biological traits eliminate the risk of forgotten or misplaced credentials and are far harder to reissue than passwords, biometric systems remain vulnerable to security breaches across different areas.

From an economic standpoint, other than fraud prevention, another reason behind the adoption of biometrics by Fintech companies is the efficiency and the goal to improve the customer checkout experience. Traditional systems such as long passwords, waiting to receive verification codes, create unnecessary hurdles when a customer is trying to complete a payment. In digital commerce, any extra step or delay during checkout oftentimes lead the customers to totally abandon their purchase. By introducing inherence-based options and replacing manual passwords with physical traits such as fingerprint or facial recognition, drastically increases transaction speed and user convenience. (Prakasha and Sumalatha. 2025). Hence, FinTech platforms are able to minimize the payment friction and boost completion rates which makes biometrics an essential business tool in digital economics.

However, despite these economic incentives, implementing biometrics in financial transaction networks poses a critical security challenge known as the irreversibility problem (Prakasha & Sumalatha, 2025). While traditional credentials, such as passwords or payment card numbers are revocable and instantly replaceable if they're compromised. In contrast, biometric traits are immutable physical features that cannot be altered once it's compromised. If a provider's database is poorly protected and biometric information is leaked, the user's biological identity is at huge risk and permanently exposed.

Hence, this commercial push for friction-free checkout reveals a critical theoretical tension: are consumers genuinely willing to exchange permanent, unchangeable biological traits for faster checkout times?

I.2 CONSUMER TRUST, PRIVACY AND PERCEIVED CONTROL

To assess the way consumers decide to adopt innovative financial technologies, foundational information systems literature leans on the Technology Acceptance Model (TAM) established by Davis (1989). It argues that an individual's acceptance of an information technology is mainly determined by two cognitive frameworks: Perceived Usefulness (PU), according to which, people decide to use or not to use the application based on its capability of improving their daily tasks and when they believe it offers clear functional benefits. Secondly, Perceived Ease of Use (PEOU) theory suggests that even if users believe a system's functional utility, it could also require excessive physical or cognitive effort, therefore the perceived operational burden quickly outweighs the expected convenience (Davis, 1989).

Biometric payments naturally excel on both areas by replacing manual input with instant physical scans. However, it should be noted that the fundamental aim of TAM was to evaluate standard workplace software where privacy threats were minimal (Davis, 1989). Since biometric payments incorporate unchangeable biological traits into financial transactions, convenience on its own cannot fully explain why someone adopts the service. This forces us to move away from TAM and examine privacy risk, control, and trust.

I.2.1 Privacy Calculus and the Privacy Paradox

To address the limitations of traditional technology acceptance models, digital business literature also draws on Privacy Calculus Theory (Culnan & Bies, 2003). Based on the theory, the information disclosure by the consumers is conceptualized as a "second exchange", where consumers exchange their sensitive personal data in return for non-monetary value, such as greater operational convenience, personalized services and faster transactions. The reason why this calculus becomes particularly intense in biometric payments is the balance that users need to perform between immediate and friction-free checkout and their immutable biological traits (Dinev & Hart, 2006). Ultimately, this decision-making process oftentimes manifests as the Privacy Paradox (Norberg et al., 2007), in which the users voice severe concerns regarding the biological data security, yet willingly submit to physical scans when offered immediate operational speed that benefits them (Norberg et al., 2007; Dinev & Hart, 2006)

I.2.2 Perceived Risk and Non-Financial Vulnerabilities

Within the aforementioned privacy calculus framework, the perceived risk remains the primary cognitive barrier to customer acquisition and retention in digital applications. While the main risk concerns in traditional e-commerce was centered on basic financial loss or credit card security (Kim et al., 2008), modern biometric payments pose a whole different, non-financial risks. Today, consumer anxiety stems from the irreversibility of biological markers, more specifically the fear of secondary data misuse, unauthorised behavioral tracking, function creep[3] (Koops, B. J. (2021) and central database breaches.

[3] Function creep – the expansion of a system or technology beyond its original purposes (Koops, 2021)

If digital platforms neglect these modern security threats, they're at the risk of creating a checkout friction for users that counteracts the speed advantage that biometric payments offer.

I.2.3 Trust, Control, and Adoption Intention

Consumer trust remains the critical strategic mechanism in overcoming consumer anxieties and implementing secure adoption. The highly uncertain nature of the digital environment causes the lack of trust and explains why consumers refuse to adopt e-commerce (Pavlou, 2003). To build this trust, two dual targets need to be addressed: Party trust (the belief that the platform will move with integrity and honesty without exploiting consumer vulnerabilities) and control trust (belief in the technical integrity and infrastructure of the control mechanisms). Moreover, empirical evidence shows that in consumer decision-making the information privacy risks often outweigh traditional economic or financial risks (Mashatan et al., 2022). The perceived privacy threats can be greatly reduced when the digital platforms are equipped with transparent data governance structure and transparency and traceability features, which allows users to control their biological credentials (Mashatan et al., 2022; Xu et al., 2012). Consequently, this dynamic interaction drives the final consumer adoption intention, in which, if the firm's trust and the control over data effectively neutralize the perceived privacy risk, the operational convenience of the biometric payments can lead to successful digital commerce transactions (Pavlou, 2003; Mashatan et al., 2022).

I.3 BIOMETRIC DATA GOVERNANCE MODELS

I.3.1 Centralized Storage and Market Risk

Section I.2 highlighted the necessity for consumers to have control and trust in the party to reduce psychological risk. Corporate data governance is the responsible part for implementing trust. In digital commerce, the crucial architectural decision has to be made by the payment providers and e-commerce platforms about where and how biometric information is stored and used. Corporate data governance typically splits into two opposing paradigms: centralized cloud architectures, frequently realized as Biometrics-as-a-Service (BaaS), and decentralized local storage models Castiglione et al. (2017)

Centralized cloud storage of biometric data, often delivered commercially as Biometrics-as-a-Service (BaaS), is an attractive choice for merchants because it removes the need for in-house security and allows companies to expand their storage as consumer transactions grow without the need to constantly buy new hardware. A value proposition reflected in the market's rapid growth, projected to expand from USD 1.5 billion in 2020 to USD 3.7 billion by 2025 (MarketsandMarkets, 2020).

However, centralization implies the following target: if one central repository is compromised, then all the biometric data of all registered users are compromised all at once. On the other hand, this threat is minimized with the decentralized systems where the impact of a data breach is isolated. This is not just a theoretical risk. In August 2019, security researchers discovered an unsecured, unprotected database belonging to Suprema's BioStar 2 biometric access-control platform, used by UK police, banks, and defense firms, that exposed fingerprint and facial recognition data for more than one

million people (Gallagher, 2019). This incident perfectly demonstrates how a single source of system vulnerability that exposes biometric information of a large population at one time, which cannot be reissued like a password could, poses a huge irreversible risk to users (Prakasha & Sumalatha, 2025).

A commercial example of this same centralized model is Amazon's palm-payment system, Amazon One, which encrypted and transmitted enrolled palm and vein images to a designated secure zone within the AWS Cloud, as opposed to storing them on the scanning device itself (Dash, 2023). This security was advertised as enterprise-grade security by Amazon, however, underneath there existed the same centralized-storage model as demonstrated in the Suprema case: one cloud repository storing the biometric information of a significant number of users. Notably, in early 2026, Amazon officially announced the discontinuation of the retail version of Amazon One, referring to a limited customer adoption (Soper, 2026), a development that itself highlights the exploration area of this thesis: consumer-trust and adoption barriers. Nevertheless, the primary weakness of centralized biometric data stores continues to be a major security concern for digital banking systems.

I.3.2 The GDPR Constraint

Beyond the security risks associated with the aforementioned examples, such as the Suprema case, companies face strong legal constraints under European data protection law. According to the Article 9 of the General Data Protection Regulation (Regulation (EU) 2016/679) Biometric information used to uniquely identify an individual is

classified as a "special category" of personal data, which is subject to stricter processing than regular personal information.

This distinction was affirmed by the Court of Justice of the European Union in the case of Michael Schwarz v Stadt Bochum (Case C-291/12, 2013), which established that biometric data constitute personal data because they objectively contain unique information enabling the precise identification of individuals.

The strategic importance of this classification is increased by the risk that the biometric information may unintentionally disclose other sensitive information that belong to a different category beyond mere identity. While some research indicates that fingerprint characteristics can convey information about an individual's lineage (Fournier & Ross, 2015), other studies have demonstrated that fingerprint ridge patterns can signify greater health risks, such as diabetes (Kahn et al., 2009) (Jasserand, 2016). This implies that biometric information processed for payment authentication purposes could simultaneously expose a company to compliance risks concerning multiple categories of sensitive data, rather than solely within the scope of the biometric classification itself.

In practice, this means that processing biometric data without a legitimate legal basis, such as explicit consent, exposes a firm to a major regulatory liability, including fines that can reach up to €20 million or 4% of global annual turnover, whichever is high (Art. 83(5) GDPR). Hence, GDPR compliance functions as a first-order constraint on the storage-architecture decision itself. Ultimately, conforming to the GDPR forces businesses to include privacy regulations into their data storage design, which makes compliance an important architectural decision rather than a trivial legal detail.

I.3.3 Decentralized Storage as a Strategic Solution

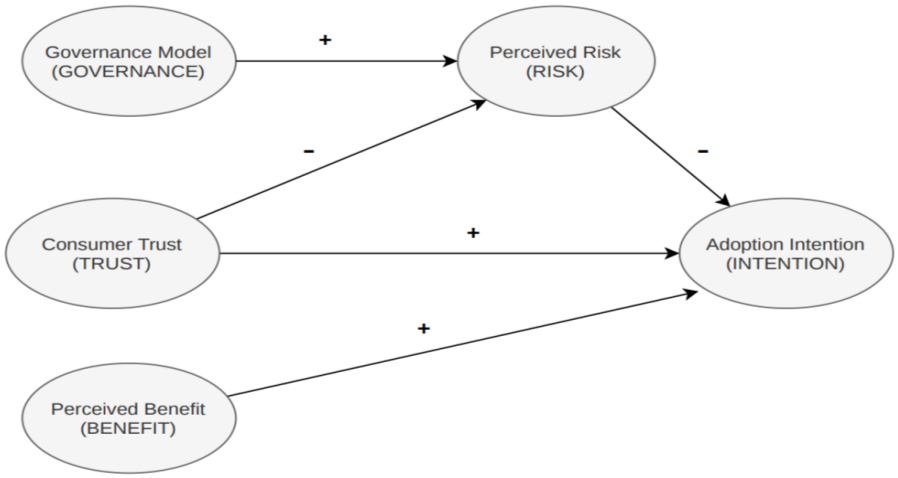
A structural solution to the concerns mentioned above is provided by decentralized, on-device storage. In this model, instead of the biometric data being sent to and retained by the merchant, the device validates the user and only transmits a match/no-match result. For instance, Apple's Face ID technology is made to ensure that the fundamental facial data never leaves the user's device or gets to Apple's servers (Apple Inc., 2026). From a managerial perspective, this architecture is far more important as a compliance strategy rather than as a technical safeguard because, according to regulatory guidance that treats such local processing as exempt (EDPB, Guidelines 1/2020, as discussed in Dahi & Corrales Compagnucci, 2022), firm usually avoids the GDPR controller responsibilities and obligations that normally apply to centralized processing because it never receives or holds the raw biometric data.

CHAPTER II: CONCEPTUAL FRAMEWORK AND METHODOLOGY

II.1 PROPOSED CONCEPTUAL FRAMEWORK

To examine how these three components: privacy risks, data storage architecture, and consumer trust influence the adoption and purchase of biometric payment system, my thesis offers an extension and adaption of the pre-existing model developed by Kim et al. (2008), in which perceived risk and consumer trust are shown to be influencing purchase intention, whereas perceived benefit has direct influence on intention in parallel. The model I developed for this thesis, adds one new piece to the aforementioned model: the governance model box and demonstrates how the architectural choice of how the data is stored (centralized or decentralized) by companies influence perceived risk and how it affects trust, purchase and risk on adoption intention. These relationships are presented in Figure 1 below:

Figure 1. *Extended conceptual framework of biometric payment adoption.*



II.2 MODEL PROPOSITIONS

To analyze the structural paths in the model, the following propositions describe the relationships between governance, risk perceptions, trust, and adoption intention.

P1: The data storage architecture about biometric data storage influences consumer perceived risk in two ways, depending whether it is centralized or decentralized:

- If the data is on the central cloud, this is considered to have a positive relationship with the consumer perceived risk as it indicates a higher risk of data leaks.
- If the data is stored on-device, it's an indicator of lower risk since the hardware is more secure

P2: Consumer trust reduces perceived risk and has a direct negative relationship (Kim et al., 2008).

- High trust implies less uncertainty about biometrics
- Trusting the company results in consumers feeling safe about transmitting sensitive data.

P3: Perceived risk acts as a barrier and has a direct negative relationship with adoption intention. (if consumers have privacy concerns, they're most likely to refuse submitting their biometric information.)

P4: Consumer trust has a direct positive effect on adoption intention. (Mashatan et al., 2022). (when consumers trust the service provider, they're most likely to be willing to adopt the biometric technology)

P5: Perceived benefit has direct positive effect on adoption intention (Mashatan et al., 2022). (When consumers believe the service, such as fast checkout and convenience, will benefit them, they're most likely to adopt the biometric technology)

II.3 RESEARCH APPROACH

This thesis uses a qualitative, secondary-data research method based on a systematic literature review. I collected literature from academic databases including Scopus, Google Scholar and JSTOR, in order to understand what effect corporate data governance has on consumer trust and biometric payment adoption. The selection strategy was based on peer-reviewed articles, legal statuses (GDPR Article 9), and applicable case law of the Court of Justice of the European Union (CJEU) as well as real world case studies (e.g. Suprema, Amazon One, Apple Face ID). In this thesis, I analyzed the chosen sources by grouping them into key themes and comparing the findings from the previous studies against five model propositions, evaluating the barriers that stand between consumers and adopting biometric technologies.

CHAPTER III: DISCUSSION AND MANAGERIAL IMPLICATIONS

III.1 SYNTHESIS OF FINDINGS

Taking the propositions developed in chapter 2, one can say that the way companies choose to govern biometric data serves as a hidden but significant factor in consumer purchase and adoption of biometric payment. As mentioned in Proposition 1, the centralized storage models increase perceived risk. This case was demonstrated in the 2019 Suprema BioStar2 breach case, which deals with exposed fingerprints and facial data of millions of users (Gallagher, 2019). This risk is aggravated by the irreversible nature of biometric traits, unlike forgotten password or card number, a compromised biometric information cannot be restored (Prakasha & Sumalatha, 2025). The consequence of this is the increased risk that conflicts with the user trust which is identified in P2 and P4 as a crucial component for user adoption intention. This is also in accordance with the trust-risk relationship described by Kim et al (2008) as well as the common finding that privacy risk perceptions outweigh the conventional financial risk concerns in the decision-making of digital commerce (Mashatan et al., 2022).

This also explains rather intriguing pattern, why Amazon One was not able to sustain the palm payment adoption in consumers despite being a highly convenient system and having a strong perceived benefit (P5) Soper (2026). If benefit, risk and trust were independent determinants of purchase in consumers, they would be able to compensate for weaker trust. However, the propositions offered in this thesis suggest that in cases of high governance-driven risk, no amount of perceived benefit could fully compensate for it. This again indicates the dominance effect of data governance that should be a

separate factor in adoption frameworks. Further implications are covered in the following section.

III.2 MANAGERIAL RECOMMENDATIONS

The results of this research emphasize the importance of the factors that managers of digital commerce should take into account when they implement biometric payment systems.

Firstly, a crucial priority should be given to the way businesses store consumer data. This should be viewed as a strategic risk management decision. The risk of data breaches affecting the entire user base is increased when information is centralized in cloud storage, which was evidenced by the Suprema security incident (Gallagher, 2019). This goes to show that instead of viewing data storage choices as a routine IT decision focused on budgeting preferance, a safer solution is to make the consumer data decentralized and local on the user's device, like Apple's Face ID (Apple Inc., 2026). This could be a better way to handle the adoption barriers that consumers face.

Secondly, compliance with GDPR needs to be embedded into the managerial decisions of storage architecture from the beginning and should not be treated as a secondary legal formality. As discussed in Section I.3.2, the way of storing consumer's information directly impacts the compliance exposure of a company and gives them a strong regulatory liability of biometric data processing. Decentralized method is an effective way to minimize the operational scope of a standard controller's data custody obligations. (EDPB, Guidelines 1/2020).

Thirdly, companies should strive to be transparent about the data governing processes to their consumers. As demonstrated by the Amazon One case in Section 3.1, it's not sufficient to only consider perceived benefit and convenience to drive adoption. It must be addressed to the consumer where exacly their biometric data is stored that makes their experiences convenient. This will help in building structural trust that is needed for long-term consumer adoption and will not result in adoption failure like it happend for Amazon One palm payment case mentioned in the article by Soper (2026).

III.3 LIMITATIONS AND FUTURE RESEARCH

While this thesis offers the way biometric governance shapes consumer trust and digital commerce, it's entirely based on existing literature, regulations and has a conceptual nature. Hence, the next step for future work would be to actually test these ideas through quantitative surveys or behavioural experiments. Variables such as the individual's age, digital literacy, and concerns about privacy and their preferences could offer a better understanding of how different individuals perceive the same data-storage design.

This would also be more concrete way to see the difference of the effects between centralized versus decentralized way of storing consumer biometric data and how it impacts their adoption choices in real time. Eventually, as the technological advancement is fast-paced and new security models and the way data is governed also evolves, consumer perceptions may also evolve. At the same time, biometric payments are thought to be widely implemented in the future. Future research could reevaluate the existing frameworks of data governance and review whether the relationships around trust, perceived benefit, risk and adoption remain consistent.

CONCLUSION

This thesis explored how biometric data governance choices, more specifically the choice between centralized cloud storage and decentralized on-device structure, influence consumer trust, risk perception, and adoption in biometric payment systems. My thesis was driven by the fundamental behavioural paradox that we can compare to two sides of the same biometric coin: the unique and irreversible nature of biometric data that strengthens the e-commerce security is also what makes it extremely risky for consumers if data breach occurs. A forgotten password or card can be reissued, however data breach that deals with the sensitive data such as person's face, iris and fingerprint shifts a heavy responsibility onto companies that handle this data.

To address this tension, this thesis expanded on the traditional trust-risk framework developed by Kim et al. (2008) by adding an important block, storage architecture. The findings in my thesis demonstrate that decentralized cloud storage significantly reduces privacy risks that is also in accordance with the requirements under GDPR Article 25 about data-minimization. On the other hand, centralized cloud storage poses heavy risks on the consumer's sensitive data that could lead to a large-scale incidents such as the Suprema breach in 2019.

Accordingly, architectural choice of data storage must remain a priority when handling sensitive, unchangeable biometric data of consumers. It should not be viewed as a secondary administrative task. As illustrated by the adoption failure of Amazon's palm payment system, firms can easily miscalculate what truly drives service adoption. Convenience only cannot overcompensate for a lack of privacy safeguard concerns when it comes to the firm's data governance model. This heavily undermines the genuine consumer trust and discourages them for long-term service adoption.

BIBLIOGRAPHY

CULNAN, M. J., & BIES, R. J. Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, Vol. 59, 2003, pp. 323-342. https://doi.org/10.1111/1540-4560.00067

PAVLOU, P. A. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, Vol. 7, No. 3, 2003, pp. 101-134.

XU, H., TEO, H. H., TAN, B. C., & AGARWAL, R. Research note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. Information Systems Research, Vol. 23, No. 4, 2012, pp. 1342-1363.

KOOPS, B. J. The concept of function creep. Law, Innovation and Technology, Vol. 13, No. 1, 2021, pp. 29–56. https://doi.org/10.1080/17579961.2021.1898299

MASHATAN, A., SANGARI, M. S., & DEHGHANI, M. How perceptions of information privacy and security impact consumer trust in crypto-payment: An empirical study. IEEE Access, Vol. 10, 2022, pp. 69441-69454.

PRAKASHA, C., & SUMALATHA, V. A Comprehensive Survey on Biometric Authentication Techniques: Performance Evaluation, Security Challenges, and Future Directions. IEEE Access, Vol. 13, 2025, pp. 15420-15445.

DOMINGO, M. C. An Overview of Biometric Security and Privacy in FinTech. IEEE Communications Surveys & Tutorials, New York, Vol. 22, 2020, pp. 1205-1228.

PATIL, R. A., & RENKE, A. L. Keystroke Dynamics for User Authentication and Identification by Using Typing Rhythm. International Journal of Computer Applications, Vol. 144, No. 9, 2016, pp. 18-21.

European Parliament and Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 9—

Processing of special categories of personal data. Official Journal of the European Union, L 119, 2016, pp. 1–88. EUR-Lex CELEX: 32016R0679

European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0). europa.eu, 2020.

APPLE INC. Apple Platform Security: Facial matching security. Apple Support, 2026. https://support.apple.com/it-it/guide/security-pdf/sece151358d1/web

GALLAGHER, R. Major breach found in biometrics system used by banks, UK police and defence firms. The Guardian, 2019, August 14. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

DASH, S. Amazon One checkout coming to all Whole Foods stores in the U.S. Amazon News, 2023, July 20. https://www.amazon.com/news/retail/amazon-one-whole-foods-market-palm-scanning[cite: 2]

SOPER, T. Amazon is ending its palm ID system for retail, Amazon One, as it closes physical stores. GeekWire, 2026, January 28. https://www.geekwire.com/2026/amazon-is-ending-its-palm-id-system-for-retail-amazon-one-as-it-closes-physical-stores/

National Cyber Security Centre. (2018, November 19). *Use of credential stuffing tools*. NCSC. https://www.ncsc.gov.uk/news/use-credential-stuffing-tools
National Institute of Standards and Technology. (n.d.). *Brute force password attack*. Computer Security Resource Center (CSRC) Glossary. https://csrc.nist.gov/glossary/term/brute_force_password_attack [1]

Dahi, A., & Corrales Compagnucci, M. (2022). Device manufacturers as controllers: Expanding the concept of 'controllership' in the GDPR. Computer Law & Security Review, 47, 105762. https://doi.org/10.1016/j.clsr.2022.105762