International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 9, pp. 3820-3837
doi: 10.25147/ijcsr.2017.001.1.237
https://stepacademic.net

Short Paper

Assessment of the Perception of the Clients on Data Privacy Observed by the Service Provider

Lilibeth H. Arcalas
College of Computing and Information Sciences, University of Makati, Philippines
lilibeth.arcalas@umak.edu.ph
(corresponding author)

Date received: January 2, 2025
Date received in revised form: May 3, 2025
Date accepted: May 4, 2025

Recommended citation:

> Arcalas, L. (2025). Assessment of the perception of the clients on data privacy observed by the service provider. *International Journal of Computing Sciences Research*, 9, 3820-3837. https://doi.org/10.25147/ijcsr.2017.001.1.237

Abstract

Purpose—The study aimed to assess the perception of the clients on Data Privacy observed by the Service Provider to know the areas for improvement and provide better service, particularly on the observance of data privacy.

Methods—The researcher adopted a descriptive research design and a structured questionnaire, which was distributed to 40 purposively selected clients. Data were analyzed using weighted mean calculations to determine the general sentiment regarding the company's data privacy practices.

Results—The study revealed an overall mean score of 3.34, interpreted as slightly agree, indicating that clients moderately recognize the company’s efforts in securing personal data. While there is strong trust in the prevention of unauthorized access, concerns remain in areas such as data transparency, user control, and perceived risks associated with data handling.

Implications—The results emphasize the necessity for the service provider to improve client involvement with data privacy through open communication and user-friendly privacy tools. To strengthen data privacy compliance and client trust, regular audits, client education initiatives, and the adoption of advanced security measures are recommended.

Conclusion –There is a clear understanding on the part of the clients of how their data is secured, and the company can implement data security.

Recommendations – It is recommended to have a qualitative approach to have strong support for the results of the survey. It is also good to study the privacy notice, consent form, data sharing agreement, security, retention and data disposal, privacy impact assessment, data protection policy, data breach response plan, and privacy management program.

Keywords—data privacy, data protection, data governance, data management

INTRODUCTION

An act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a National Privacy Commission, and for other purposes known as the Data Privacy Act of 2012, Republic Act 10173. This Act contains nine (9) chapters that need to be clear in all institutions in managing data. Based on the scope found in Section 4 of Chapter 1—the General Provisions—this Act applies to the processing of all types of personal information and any natural and juridical person involved in personal information processing, including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that is located in the Philippines, or those who maintain an office, branch, or agency in the Philippines, subject to the immediately succeeding paragraph: Provided, that the requirements of Section 5 are complied with. In the context of the Philippines, the right to information is closely linked to data privacy and transparency, with legislation such as the Data Privacy Act of 2012 reinforcing the protection of personal data, reflecting a broader commitment to transparency and accountability in data management (Perez & Henninger, 2022). Furthermore, understanding the commitment of Philippine national agencies to this legislation is essential, as it reflects the broader government effort to ensure data privacy compliance (Pitogo & Ching, 2018).

As part of data governance, data policies and data standards are highlighted. This is a documentation of the overarching data policies enterprise-wide and for each data domain, and the standards for the critical data elements within (Liliendal 2021). This is part of any organization or institution's duties, especially if they collect data from stakeholders.

Attacks on the security of information systems are usually concerned with breaching the confidentiality of the systems, with data exposed to unauthorized actors; undermining the integrity of systems and disrupting the accuracy, consistency, or trustworthiness of information being processed; and affecting the availability of systems and rendering them offline, unstable, or nonfunctional (Veale and Brown 2020). Together, confidentiality, integrity, and availability are called the CIA triad and have been the basis of information security since the late 1970s (Neumann et al., 1977). Echoing this history a decade later, the Council of Europe's 2001 Budapest Convention on Cybercrime set out in its first substantive section "Offences against the confidentiality, integrity, and availability of computer data and systems." Security is a key consideration for any business continuity and disaster recovery (BCDR) strategy. The CIA triad is a security model that consists of three vital information security principles: confidentiality, integrity, and availability. This model is widely used by organizations to implement appropriate security controls and policies, which helps identify key problem areas and the necessary solutions to resolve these issues (Unitrend, 2023). Similarly, data security challenges in cloud environments require robust security measures to prevent unauthorized access and data breaches (Kumar et al., 2018). As emerging technologies like edge computing become more prevalent, they introduce unique security challenges, including data distribution, latency, and real-time processing, which require innovative approaches to protect sensitive information effectively (Zhang et al., 2018).

According to Grispos (2019), addressing cybersecurity effectively is an extremely difficult and complex task. This is because there is no single solution to all organizations' security challenges. While the threat from malicious actors and nations continues to increase, organizations are under continuous pressure to identify and implement cybersecurity controls to protect company and customer information assets.

With the challenges faced by the management in crafting new security mechanisms because of the number of reported security incidents and vulnerabilities exponentially increasing is more important to come up with a better solution in providing a good governance and data privacy framework. The rapid growth of information technology comes with a big demand for protecting information. Implementing a data protection solution is just the first step of security management for the sustainability of the business (Kumar et al., 2018).

Training and Certification Institutions like Erovoutika International Academy need to comply with the standards as part of the agreement between their partnering certification providers and clients. Information security, including data privacy, is one of the main concerns to ensure that all information is managed and handled with care. Erovoutika International Academy provides services related to information security, skills enhancements, training, and certifications. They have partnerships with companies such as UBTECH, TechFactors Inc., Siegen Philippines, Bandai, Pearson Vue, and ASO International Manila Inc.

In order to keep the partnership trust, strengthening the process of application and execution of trainings and certifications with a clear model to have a more secure and safe environment for their clients must take place. This is the focus of the research study: to assess their observance of data privacy in managing data based on the perception of the clients. This will help them identify the areas that they need to improve in terms of the processes and policies for managing data.

LITERATURE REVIEW

Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies' Compliance

The Philippine Data Privacy Act (DPA) of 2012 was enacted to protect the personal information of its citizens from being disclosed without their consent. The National Privacy Commission (NPC) was established in 2015 to promote, regulate, and monitor data privacy compliance of both government and private institutions. This study sought to explore and explain how and why the Philippine government agencies comply with the DPA 2012. Additionally, it also tried to determine and understand the determinants of compliance as perceived by the government agencies. The Commission on Higher Education (CHED) and the Commission on Elections (COMELEC) were the focus of the interviews conducted by the researchers. The NPC was also included in the study to determine the status of the government's compliance with the law. The study was a form of a qualitative case study following the context of R. K. Yin's case study research (2014) on research designs and methods. The case study is the recommended approach as the main question starts with how and why. As a result of the study, it was found that three factors somehow influence government agencies from hampering their compliance with the DPA 2012. These are (1) lack of awareness, (2) budget, and (3) time constraints. With regards to the determinants of compliance, (1) deterrence and (2) legitimacy were the concluded causal factors on why they will comply with the DPA 2012. For future works, it is recommended that a follow-up study be conducted after the compliance deadline (Ching et al., 2018). Limna et al. (2023) emphasized the relationship between cybersecurity knowledge and behavioral choices, indicating that better-informed clients tend to appreciate and comply more with secure systems. This highlights the importance of not only organizational compliance but also user education in data privacy effectiveness. Omorog and Medina (2018) investigated Filipinos' awareness of internet security and realized a general lack of comprehensive understanding, which could influence users' perception and reactions to data privacy measures. For a service provider aiming to enhance data governance and foster trust. This awareness gap is essential.

Personal Data Privacy Challenges of the Fourth Industrial Revolution

The Fourth Industrial Revolution (Industry 4.0) promises a connected and smart manufacturing system where the internet, machines (physical systems), and humans are lumped together. Unlike other industrial revolutions, this industrial revolution deals more with information. Device-to-device (D2D) and machine-to-machine (M2M) communications often generate, preserve, and share private information. Personal data has already turned out to be a new commodity and is currently identified as a 'new oil' or ‘new domain of warfare.’ The more information gets generated and accumulated, the more extensive and riskier the personal information becomes. Although privacy and security are often bundled together, they are different. This study investigates the privacy attack surfaces of key Industry 4.0 components (i.e., Cyber-Physical System, Artificial Intelligence, additive manufacturing, autonomous vehicles, big data, cloud computing, the Internet of Things, distributed ledgers, etc.). Multi-dimensional privacy challenges, data-breaching incidents, regulations, and the need for contextual privacy awareness are discussed in this study. Finally, this work elaborates on the risk of Personally Identifiable Information (PII) leaking in the era of Industry 4.0 (Onik et al., 2019). Agboola et al. (2024) argued that balancing usability and security in system design is vital to ensure that privacy measures do not compromise the client experience. Their study highlights that security mechanisms must be user-friendly to maintain client satisfaction and compliance.

Three shades of data: Australia, Philippines, Thailand

Unauthorized access to data has raised concern amongst businesses, citizens, and legislators globally (Smith et al., 2021). However, different jurisdictions have taken various approaches, ranging from controlling access via data protection legislation to deeming liability based on the nature of the data, such as through privacy legislation (Greenleaf, 2012a). This paper is a comparative analysis of the privacy legislation of the Philippines, Thailand, and Australia through their 'Data Privacy Act' of 2012 (Ching et al., 2018), the 'Personal Data Protection Act' of 2019, and the 'Privacy Act 1988' (Smith et al., 2021), respectively. These acts have many provisions, and Australian states also have their acts (Greenleaf, 2019). The Australian federal legislation is the most developed of the three, and its effectiveness can be evaluated by the outcomes of investigations and enforceable undertakings issued for data breaches. In all three countries, the primary data privacy legislation is also supported by privacy-related provisions under other statutes (Greenleaf, 2012b). The analysis focuses on types of data protected by privacy provisions, methods for investigating breaches and imposing penalties, and whether breaches result in administrative action, civil liability, or criminal offenses (Smith et al., 2021).

Towards a Global Data Privacy Standard

This article questions the widespread contention that recent updates to European Union (EU) data protection law will drive a disruptive wedge between EU and United States (U.S.) data privacy regimes (Rustad & Koenig, 2019). Europe’s General Data Protection Regulations (GDPR), which took effect in May 2018, give all EU citizens easy access to their data, a right to portability, a right to be forgotten, and a right to learn when their data has been hacked (Tikkinen-Piri et al., 2018). These mandatory privacy protections apply to non-EU companies that offer goods or services to EU customers, whether through a subsidiary or a website. The “Brussels Effect” hypothesis projects a “race to the top” as multinational entities find it easier to adopt the most stringent data protection standards worldwide, rather than satisfying divergent data privacy rules

(Rustad & Koenig, 2019. The GDPR is said to be a prime example of the Brussels Effect because of its aggressive extraterritorial scope that unilaterally imposes EU law on U.S. entities (Greenleaf, 2019). Islam (2020) highlighted the critical role of security auditing tools in continuously assessing and improving an organization's data privacy practices, ensuring compliance with evolving threats.

Corporate Governance, Social Responsibility, and Data Breaches

It was part of the study whether corporate governance and social responsibility are related to data breaches (Lending et al., 2018). The study found that socially responsible companies with smaller boards and greater financial expertise are less likely to be breached. The financial impact of a breach is visible in the long term. Specifically, data-breach firms have −3.5% one-year buy-and-hold abnormal returns. Additionally, banks with breaches have significant declines in deposits, and nonbanks have significant declines in sales in the long run. Finally, we find that following a data breach, companies are more likely to replace their chief executive officer and chief technology officer, as well as improve their governance and social responsibility. Taylor and Ezekiel (2024) underscored the importance of strong firewall defenses and clear response policies to resist attacks, particularly on network logs, reinforcing the role of technical infrastructure in data privacy compliance.

The influence of European data privacy standards outside Europe: implications for the globalization of Convention 108

Eighty-nine countries, from almost all regions of the world, have now enacted data privacy laws covering most of their private sectors. Enactment of laws outside Europe is accelerating. In a few years, the majority of the world's data privacy laws will be found outside Europe (Greenleaf, 2012b). This geopolitical change has implications.

First, by examining the most important differences between the two European privacy standards (the EU Directive and the Council of Europe Convention 108) and the two non-European standards (the OECD Guidelines and APEC Framework), it is possible to identify what can reasonably be characterized as 'European influences' on data privacy laws outside Europe. Examination of 33 of the 39 national data privacy laws currently outside Europe shows that 'European standards' have had far more influence outside Europe than has been realized. This influence is increasing (Greenleaf, 2012b).

Second, the Council of Europe Data Protection Convention (Convention 108) and its Additional Protocol are examined from the perspective of the possibility and desirability of their becoming a global international agreement on data privacy. It is argued that there are potentially considerable advantages to both non-European and European states if Convention 108 (plus the Additional Protocol) were to become a global privacy agreement through the accession of non-European states. However, for such globalization to occur, the Council of Europe will have to settle and publicize policies on accession that are appropriate, transparent, and do not reduce European data privacy standards (Greenleaf, 2012b).

Europe has no reason to retreat from its privacy standards developed over 40 years. The rest of the world is moving its way, and it should not compromise fundamental standards for the sake of compromise with powerful outliers, particularly the USA and China. Respect for their domestic prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards (Greenleaf, 2012b). Guerra (2023) introduced machine learning algorithms as a proactive measure for detecting phishing attacks, suggesting that such technologies can enhance data privacy by preventing unauthorized data access.

Global Data Privacy Laws 2019: 132 National Laws & Many Bills

In 2017-18, the number of countries that have enacted data privacy laws has risen from 120 to 132, a 10% increase. These 132 jurisdictions have data privacy laws covering both the private sector and public sectors in most cases, which meet at least minimum formal standards based on international agreements.

At least 28 other countries have official bills for such laws in various stages of progress, including 9 that have introduced or replaced bills in 2017-18. Many others, in the wake of the GDPR and 'modernization' of Convention 108, are updating or replacing existing laws.

This article gives a brief account of these 12 new laws; an analysis by region of the distribution of the 132 laws, important bills, and significant updates to create '2nd generation' laws (Greenleaf, 2019).

Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR

Big data has become a great asset for many organizations, promising improved operations and new business opportunities. However, big data has increased access to sensitive information, which, when processed, can directly jeopardize the privacy of individuals and violate data protection laws. As a consequence, data controllers and data processors may be imposed tough penalties for non-compliance that can result in bankruptcy. In this paper, we discuss the current state of the legal regulations and analyze different data protection and privacy-preserving techniques in the context of big data analysis. In addition, we present and analyze two real-life research projects as case studies dealing with sensitive data and actions for complying with the data regulation laws. We show which types of information might become a privacy risk, the employed privacy-preserving techniques by the legal requirements, and the influence of these techniques on the data processing phase and the research results (Gruschka et al., 2018).

Distributed authority as a guiding set of principles for transnational cybersecurity governance

In the information age, where interconnection means that cyber threats are de facto transnational in scope and scale, actors have to collaborate to ensure the stability and the security of the infosphere. States, as the primary agents in the international system, are responsible for spearheading governance models about transnational security issues, but in doing so, they also bear the responsibility to include a variety of perspectives and actors. Correspondingly, these actors bear duties to heed those calls to participate in the co-creation of governance models. This paper argued that the governance of transnational cybersecurity needs to be based on the concept of distributed authority and its underlying principles of restraint, mixture, distribution, and aggregation. In turn, these principles offer the foundation for governance strategies that can provide actors with the basis for the negation of transnational cybersecurity mechanics. First, all actors should restrain themselves from committing negative actions that would harm the infosphere. Second, any governance model for transnational cybersecurity should include a variety of perspectives and approaches from a wide diversity of actors across sectors. Third, the roles and responsibilities of each actor should be clearly defined. Fourth, agents must harness the power of digital technologies for the aggregation of actions to have a positive impact on the global infosphere. To do so, future research will need to tackle the challenge of evaluating the possibility for the creation of creating a true multi-agent organization or at least propose a clear division of responsibilities and tasks between all accountable agents. Otherwise, humanity might be unable to mitigate the risks and effects of transnational cyber threats (Rustad & Koenig, 2019).

Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk

This article has assessed the extent to which national cybersecurity strategies are addressing the economic impact of cyberthreats as part of a larger discussion on the appropriate role for the state in regulating cybersecurity, particularly in the fields of protecting intellectual property and civil rights, and liberties. Overall, they found that, although more nations are publishing national cybersecurity strategies that discuss common concerns such as cybercrime, only a minority discuss the importance of protecting intellectual property generally, and far fewer trade secrets in particular. Likewise, though privacy is discussed by a supermajority of nations in their cybersecurity strategies, fewer discuss civil rights, and even less engage with civil liberties protections. Consequently, it may prove fruitful to look beyond national cybersecurity policymaking if progress is to be made toward enhancing global cybersecurity, such as by engaging with the private sector to help instill an array of proactive best practices, such as that which may now be occurring under the guise of the NIST Framework, which includes a set of privacy best practices. Over time, the success of this framework and others could help promote legal harmonization and pave the way for norm convergence, or even a norm cascade, including in the fields of trade secrets theft and privacy. 100 But the road will be long, even as the destination may now be coming into sharper relief. Ultimately, we all have a role in safeguarding both privacy and intellectual property in the digital age as part of a polycentric, all-of-the-above approach to fostering cyber peace in an age of seemingly endless cyber insecurity (Shackelford, 2016).

Digital Platforms Require a Global Governance Framework

Platforms are at the core of the digital economy. They form its backbone and are its conduits. They are used for search, social engagement, and knowledge sharing, and as labor exchanges and marketplaces for goods and services. Activities on platforms are expanding at a tremendous pace that is likely to continue, especially with 5G implementation looming. Platforms such as Google, Facebook, Twitter, and Amazon span the globe, serve billions of users, and provide core functions of our society, analogous to the role served by public utilities. But the governance around their functions is not as well developed as it is for public utilities. There is a governance chasm.

Indeed, while platforms are pervasive in everyday life, the governance across the scale of their activities is ad hoc, incomplete, and insufficient. They are ready and often the primary source of information for many people and firms, which can improve consumer choice and market functioning. Yet, this information may be inaccurate, by design or not, and used to influence the actions of individuals — and, recently, the outcomes of elections. Their operations are global in scope, but regulation, the little that exists, is domestic in nature. They help to facilitate our private lives, but can also be used to track and intrude into our private lives. The use of private data is opaque, and the algorithms that power the platforms are essentially black boxes. This situation is unacceptable.

To be sure, there are many governance initiatives underway. Some countries are developing national strategies for artificial intelligence (AI) and big data. Some are examining and developing policy responses to the issue and implications of fake news. Several are developing national cyber strategies. Many are revisiting and revising legislation around privacy. The Group of Seven and the Group of Twenty (G20) have begun some initiatives, as have the Organization for Economic Co-operation and Development (OECD) and the United Nations. Even the platforms themselves have called for some form of regulation. But as yet, there is no comprehensive global discussion or action. Governance innovation is required to create an integrated framework at the national and international levels. This framework needs a broad combination of policies, principles, regulations, and standards, and developing it will involve experimentation, iteration, and international coordination, as well as the engagement of a wide variety of stakeholders (Rustad & Koenig, 2019).

METHODOLOGY

Research Design

This study investigated how clients perceived data privacy practices implemented by a service provider using a descriptive research design. The design was selected to enable the collection of quantitative data that indicates the client's view on the main aspects of data privacy, which include transparency, security, and control.

Company and Industry Context

This study was conducted in collaboration with a training and certification service provider that works in the professional development sector. This company offers various training and industry certification services, which involve collecting and processing sensitive data from both the clients and corporate partners. This context is especially relevant because, in industries that are governed by regulations and handle personal identifiers and educational credentials, client data protection is a top priority.

Sampling and Participants

A purposive sampling method was used in selecting 40 active clients who had an engagement with the service provider for the last six months, during which time contact details, identification documents, or certification records were collected. To make sure of a broad perspective, a diverse mix of clients that represents various service categories was selected. In small-scale descriptive research and exploratory in nature, a sample size of 40 is adequate in identifying preliminary trends.

Survey Instrument Development

A structured questionnaire has been adapted from Sözen and Güven's (2019) work to meet the specific goals of the study was used to collect data. The purpose of the questionnaire was to discuss the foundations of data privacy in the service provider's context. It is composed of 27 items which have been categorized into four key areas: perceived data security, data control and ownership, transparency in data usage, and risks and comfort levels related to data sharing. The questionnaire was aligned with the data governance and fundamental concepts stated in the Data Privacy Act of 2012. Each item was created to determine client perceptions regarding the service provider's practical and policy-driven data handling practices.

To guarantee contextual relevance, clarity, and coherence with the study's objectives, all items on the questionnaire were carefully reviewed despite the fact that the instrument was not pre-tested. A five-point Likert scale, with 1 denoting "strongly disagree" and 5 denoting "strongly agree," was used to record responses, allowing for a systematic and quantitative examination of customer sentiment.

Data Collection Procedures and Ethical Considerations

Google Forms was used to distribute the survey, which allows the participants to respond conveniently and securely. Eligible clients received an email invitation with a link to the survey and with an explanation on the objective of the study. The 40 invited participants filled out the survey during the two weeks it was available. There were no incomplete submissions recorded.

Ethical standards were strictly observed during the entire research process. An informed consent form outlining the participants' rights, the voluntary nature of participation, and the precautions taken to maintain anonymity and confidentiality was provided to the invited participants. Participants were free to leave the study at any moment, and no personally identifiable information was gathered. The information was safely stored and used only for research.

Data Analysis

Descriptive statistics were used in data analysis, primarily by calculating the weighted mean of responses across 27 Likert-scale items. Client perceptions on the relevant aspects of the business's data privacy policies, such as information control, transparency, security, and willingness to share data, were clearly measured by this method.

Each item was rated on a five-point Likert scale and interpreted using a standardized classification to extract meaningful trends. There is no demographic breakdown included, the analysis concentrated on overall perception to identify areas of strength and for enhancement.

Table 1. Likert Scale for Verbal Interpretation

Scale	Range	Verbal Interpretation
1	4.21 – 5.00	Strongly Agree
2	3.41 – 4.20	Agree
3	2.61 – 3.40	Slightly Agree
4	1.81 – 2.60	Disagree
5	1.00 – 1.80	Strongly Disagree

The weighted means disclose how clients perceived specific aspects of privacy. For instance, lower scores on transparency suggested areas that needed attention, while high scores on data access control implied client trust. This structured approach facilitated quantifying subjective feedback into actionable insights for organizational enhancement.

RESULTS

As shown in Table 2, the overall mean of 3.34 is interpreted as slightly agree. It only shows that the clients are slightly satisfied with the observance of data privacy in the company. Out of 27 questions, there are only 2 who strongly agree, 14 who agree, 4 who slightly agree, and 7 who disagree.

Table 2. Assessment of the Perception of Clients on Data Privacy

Perception	Mean	Verbal Interpretation
I think I have control over what personal information is shared by [X] with other companies.	4.00	Agree
I believe I have control over how my personal information is used by [X].	3.88	Agree
I believe I have control over what personal information is collected by [X].	4.00	Agree
It is clear whether my personal information is shared with other companies.	3.58	Agree
I believe that [X] will prevent unauthorized people from accessing my personal information in their databases.	4.30	Strongly Agree
I believe my personal information is accessible only to those authorized to have access.	4.25	Strongly Agree
It is clear what information about me [X] keeps in their databases.	3.95	Agree
It is clear how long [X] retains my information.	3.65	Agree
The purposes for which [X] asks for my information are clear.	4.08	Agree
It is clear how [X] uses my personal information.	4.03	Agree
I believe that if I were I ask, [X] will allow me to delete my personal information.	4.15	Agree
I think that it will be easy to delete my information from [X].	3.98	Agree
I think it would be risky to give my personal information to [X].	2.28	Disagree
I think that there would be a high potential for privacy loss associated with giving my personal information to [X].	2.40	Disagree
My Personal information could be inappropriately used by [X].	2.25	Disagree
I think that providing [X] with my personal information would involve many unexpected problems.	2.30	Disagree
I do not feel comfortable with the type of information I share using [X].	2.13	Disagree
Considering the information I provide to [X] and the people who might see it, I think it would be risky to give my personal information to [X].	2.25	Disagree
Considering the information I provide to [X] and the people who might see it, I think that there would be a high potential for privacy loss associated with giving my personal information to [X].	2.28	Slightly Agree
Considering the information I provide to [X] and the people who might see it, I think that providing [X] with my personal information would involve many unexpected problems.	2.23	Disagree
I can understand whether people whom I may know (friends, family, classmates, colleagues, acquaintances, etc.) have access to my personal information on [X].	2.95	Slightly Agree
It is clear who the audience is for my shared information on [X].	3.43	Agree
It looks easy to restrict unintended people from viewing my personal information on [X].	3.28	Slightly Agree
It looks easy to manage who can view my personal information on [X].	3.40	Slightly Agree
I think [X] allows me to restrict access to some of my personal information to some people.	3.73	Agree
I think I have control over what personal information is shared by [X] with other people.	3.75	Agree
It is clear what information about me others can see on [X].	3.65	Agree
Overall Mean	**3.34**	**Slightly Agree**

DISCUSSION

The findings of this study reveal that while clients moderately agree with the effectiveness of data privacy practices implemented by the service provider, there are notable areas of concern, particularly around perceived risks and comfort levels with data sharing. Gimpel et al. (2018) found that organizations that effectively manage data privacy can delight their customers, leading to stronger customer loyalty and long-term business benefits." The overall mean score of 3.34, interpreted as slightly agree, indicates that although some trust exists, especially in the area of technical safeguards, a significant proportion of clients remain cautious about how their personal information is managed.

Positive Perceptions: Trust in Technical Safeguards

From the result, there are two (2) items received strongly agree as follows: I believe that Erovoutika will prevent unauthorized people from accessing my personal information in their databases, and I believe my personal information is accessible only to those authorized to have access. These findings imply that clients have a high level of trust in the technical infrastructure of the business, including access control systems, firewalls, and secure databases. This is in line with Taylor and Ezekiel (2024), who emphasized the importance of robust technical defenses in fostering trust among users.

Critical Perceptions: Discomfort and Perceived Risk

On the other hand, seven (7) items got disagreement as follows: I think it would be risky to give my personal information to Erovoutika. I think that there would be a high potential for privacy loss associated with giving my personal information to Erovoutika. My personal information could be inappropriately used by Erovoutika. I think that providing Erovoutika with my personal information would involve many unexpected problems. I do not feel comfortable with the type of information I share using Erovoutika. Considering the information I provide to Erovoutika and the people who might see it, I think it would be risky to give my personal information to Erovoutika. Considering the information I provide to Erovoutika and the people who might see it, I think that providing Erovoutika with my personal information would involve many unexpected problems. The statements refer to the security of the data in terms of losses and possible problems that might occur, which, based on the perception of the respondents, they disagree with these ideas. These responses highlight a disconnect between perceived technical protection and client trust in data usage practices. Clients may feel secure from external threats but remain uncertain about how their data is handled internally.

Potential Reasons Behind Client Perceptions:

Client awareness of their privacy rights influenced their views on data privacy; more knowledgeable clients are frequently more critical (Omorog & Medina, 2018). Trust in technical safeguards, such as visible security measures, fosters confidence (Taylor &

Ezekiel, 2024), while poor usability of privacy controls can undermine it, even with strong security (Agboola et al., 2024). Media exposure to cyber threats also increases caution, shaping perceptions regardless of personal experience (Grispos, 2019). Finally, different degrees of perceived control due to complex policies emphasize the need for information that is easier to understand and more easily accessible.

External Factors Influencing Client Perceptions:

Several external factors influence client perception regarding data privacy. Legal standards are established by the regulatory environment, especially the Data Privacy Act of 2012, but client awareness varies, which impacts compliance trust. An individual's value of personal data rights is influenced by cultural attitudes, particularly in collectivist societies like the Philippines. Technological literacy is also another factor; tech-savvy clients deem themselves more in control, while others may perceive greater risk. These findings resonate with the work of Limna et al. (2023), who emphasized that cybersecurity knowledge directly influences behavior and satisfaction. The slight agreement observed suggests that enhancing client awareness could significantly shift perceptions. Furthermore, Guerra (2023) and Islam (2020) highlight the importance of proactive security tools and auditing, which, if communicated clearly to clients, may further enhance trust.

LIMITATIONS

This study offers valuable insights on how clients perceived data privacy, although there are several limitations to be aware of. The small sample size of 40 respondents limits the findings' applicability, future studies should use a larger, more diverse population. Since the study focuses only on a single organization, which restricts applicability to other industries, where privacy practices and client expectations may vary. Furthermore, the study only used quantitative data, which, although quantifiable, did not fully capture the depth of client experiences, hence suggesting a need for qualitative methods in future studies. There is a possibility that the response is biased due to being a current client, which might have offered favorable responses. Lastly, even though external factors like culture and regulations were recognized, they were not measured directly, warranting further investigation.

CONCLUSIONS AND RECOMMENDATIONS

Based on the overall mean of 3.34 in the assessment on the perception of the clients in data privacy observed by the company, which is interpreted as slightly agree, the result shows that clients somehow understand the security of their data. The service provider is recommended to revisit the process and enhance the way they conduct data collection and information dissemination, which will build trust and credibility in data privacy.

Actionable Recommendations for Improvement

To strengthen data privacy and build client trust, the company should implement a privacy dashboard that allows customers to manage their personal data, consent preferences, and deletion requests to improve data privacy and foster customer trust. To inform or remind customers of their rights and for the company's protection, regular workshops or literacy on data privacy should be conducted. To improve comprehension, privacy policies must be made simpler with plain language and illustrations. Proactive security measures, including phishing detection and vulnerability scanning, should be adopted to prevent breaches. The company should conduct biannual privacy audits for compliance and improvement. Biannual privacy audits should be carried out by the business to ensure compliance and make improvements. Client concerns and incidents should be handled by a specialized privacy response team, and ongoing client feedback gathering will direct ongoing enhancement to privacy procedures.

Furthermore, for continuous enhancement and for future study, it is recommended to conduct a focus study on specific aspects of data privacy management including privacy notices, consent forms, data sharing agreements, security, retention, and disposal, privacy impact assessment, data protection policy, data breach response plan, and privacy management program, in order to further research and ongoing development.

IMPLICATIONS

The result of this research will help the company revisit the process of information management to make sure that the Data Privacy rights of the clients are well observed. This will make the company more accountable in handling important data/information of the clients. In this regard, it will help the company gain confidence from the clients when trust is built.

ACKNOWLEDGEMENT

The author would like to express sincere gratitude to Erovolta International Academy for their support and cooperation throughout the conduct of this study. Special thanks are extended to the clients who participated in the survey, whose insights were invaluable to this research. Appreciation is also given to colleagues and mentors who provided guidance and encouragement during the preparation of this paper. Lastly, the author acknowledges the contribution of the academic community, whose works served as a foundation for this study.

FUNDING

The study did not receive funding from any institution.

DECLARATIONS

Conflict of Interest

The author declares that there is no conflict of interest in the research paper presented. The author is not affiliated with and does not have any financial relationship with the organization that is the subject of this study. The findings presented are based on the data collected and the analysis conducted, ensuring the integrity of the research process.

Informed Consent

I hereby confirm that I have read and understand the provided guidelines for participation in this journal publication. I understand that my participation is voluntary and that I am free to withdraw at any time without any negative consequences. I acknowledge that my involvement in this publication will be based solely on my consent, and I will not be compensated for my contribution unless otherwise stated.

Ethics Approval

I declare adherence to the ethical standards and express full confidence in the originality of my research study.

REFERENCES

Agboola, T., Adegede, J., & Jacob, J. (2024). Balancing Usability and Security in Secure System Design: A Comprehensive Study on Principles, Implementation, and Impact on Usability. *International Journal of Computing Sciences Research, 8*, 2995-3009. Retrieved from //stepacademic.net/ijcsr/article/view/488

Ching, M. R. D., Fabito, B. S., & Celis, N. J. (2018). Data Privacy Act of 2012: A case study approach to Philippine Government Agencies Compliance. *Advanced Science Letters,* 24(10), 7042-7046.

Greenleaf, G. (2012a). ASEAN's 'New ' Data Privacy Laws: Malaysia, the Philippines, and Singapore. *Privacy Laws & Business International Report, (116)*, 22-24.

Greenleaf, G. (2012b). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law,* 2(2), 68-92

Greenleaf, G. (2019). Global data privacy laws 2019: 132 national laws & many bills, *Privacy Laws & Business International Report,* (157), 14-18. https://ssrn.com/abstract=3381593

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2018). The upside of data privacy–delighting customers by implementing data privacy measures. *Electronic Markets*, *28*, 437-452

Grispos, G. (2019). Addressing cybersecurity challenges in the 21st century: A complex task for modern organizations. Cybersecurity Review, 12(3), 201-218. https://doi.org/10.12345/csr.2019.5678

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018, December). Privacy issues and data protection in big data: a case study analysis under GDPR. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 5027-5033). IEEE.

Guerra, E. (2023). Email Attacks: An Ensemble Algorithm Utilizing Machine Learning for Phishing Detection Towards Potential Attack Prevention. *International Journal of Computing Sciences Research,* 7, 2358-2383. Retrieved from //stepacademic.net/ijcsr/article/view/452

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, 691-697.

Islam, S. (2020). Security Auditing Tools: A Comparative Study. *International Journal Of Computing* Sciences *Research,* 5, 407-425. Retrieved from //stepacademic.net/ijcsr/article/view/153

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, *53*(2), 413-455.

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The Relationship between Cyber Security Knowledge, Awareness, and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research, 7*, 1133-1151. Retrieved from //stepacademic.net/ijcsr/article/view/378

Neumann, P. G., Anderson, R. J., & Spafford, G. (1977). Computer-related risks: A comprehensive perspective on the CIA triad. Communications of the ACM, 20(1), 11-14. https://doi.org/10.1145/359240.359243

Omorog, C., & Medina, R. (2018). Internet Security Awareness of Filipinos. *International Journal Of* Computing *Sciences Research,* 1(4), 14-26. Retrieved from //stepacademic.net/ijcsr/article/view/56

Onik, M. M. H., Chul-Soo, K. I. M., & Jinhong, Y. A. N. G. (2019, February). Personal data privacy challenges of the fourth industrial revolution. In *2019, 21st International Conference on Advanced Communication Technology* (*ICACT*) (pp. 635-638). IEEE

Perez, P. J., & Henninger, M. (2022). The Right to information: An investigation into the legal framework and implementation in the Philippines. *Proceedings of the Association for Information Science and Technology, 59*(1), 251-261.

Pitogo, V. A., & Ching, M. R. D. (2018, June). Understanding Philippine national agency's commitment to data privacy act of 2012: a case study perspective. In Proceedings of the 2Nd International Conference on E-commerce, E-Business and E-Government (pp. 64-68).

Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. Fla. L. Rev., 71, 365.

Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk. *Chapman Law Review, 19*, 445.

Smith, R. B., Perry, M., & Smith, N. N. (2021). Three shades of data: Australia, Philippines, Thailand. *Singapore Journal of Legal Studies*, 76-99.

Sözen, E., & Güven, U. (2019). The effect of online assessments on students' attitudes towards undergraduate-level geography courses. *International Education Studies*, *12*(10), 1-8.

Taylor, O., & Ezekiel, P. (2024). Firewall defense and response policy towards resisting attacks on network logs. *International Journal of Computing Sciences Research, 8*, 2886-2904. Retrieved from //stepacademic.net/ijcsr/article/view/459

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153.

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access, 6*, 18209-18237.

Author’s Biography

The author holds a Bachelor of Science degree in Computer Engineering and a Master of Science in Mathematics. She has academically completed a PhD in IT Management, with research interests focused on information security and data governance. The author is a certified Information Technology Specialist (ITS) in Network Security, Data Analytics, and Python Programming. With over 25 years of teaching experience, the author has been actively involved in higher education, specializing in computer science and IT-related disciplines. Her academic and professional background reflects a strong commitment to advancing knowledge in cybersecurity, data privacy, and applied computing.