Privacy Impact Assessments of Technology AI Companies

Joshua Cepler
Cybersecurity and Threat Intelligence
University Of Guelph
Guelph, Ontario, Canada
jcepler@uoguelph.ca

Tarun Kalyani
Cybersecurity and Threat Intelligence
University Of Guelph
Guelph, Ontario, Canada
tkalyani@uoguelph.ca

***Abstract*—This research project conducts a comprehensive analysis of Privacy Impact Assessments (PIAs), GDPR, and NIST AI policies, from leading technology companies Microsoft, Google, and IBM, focusing on their data protection and privacy practices. The study aims to identify and address prevalent privacy issues within these organizations, examining how they store, share, and process data, including their approaches to data retention, transparency, and security in AI and machine learning contexts. Utilizing frameworks provided by the GDPR, NIST AI and PIA, the project compares public PIAs, and Policies under GDPR and NIST AI to assess compliance with data protection laws and the management of privacy risks. Preliminary findings reveal varied data retention policies and practices among these tech giants, with insights into their compliance strategies under GDPR and NIST guidelines. We offer a comprehensive report offering a comparative analysis of Microsoft Copilot, Google, and IBM's privacy practices and note improvements needed for enhanced privacy management in the technology and AI sectors.**

***Index Terms*—PIA, Data retention, GDPR, Data Storage policy, NIST AI, National Institute of Standards and Technology, Google, Microsoft, IBM**

I. Introduction

As soon as companies started trying to gather consumers' data, there surely were people who were concerned about how it could be used. The status quo of society giving information to companies spiralled to the point where companies are even collecting it without our permission. Big technology companies had grown complaisant in their roles as rulers of society's data, and consumers took notice. Privacy legislation and rules were put in place to protect consumers, and companies became more transparent about the information they collected. As the cycle continues, the policies are still updating and it's time to make sure the companies are still up to snuff.

A. Research Motivation

The issue stated in our topic "Privacy Impact Assessments of Technology AI Companies" focuses on the critical analysis of privacy issues within major technological companies such as Microsoft Copilot, Google, and IBM, in light of increasing reliance on digital services and data privacy concerns. The document underlines the necessity of understanding how these corporations manage personal data, particularly in light of the European Union's General Data Protection Regulation (GDPR). It also emphasizes the importance of following the National Institute of Standards and Technology's (NIST-AI) requirements, especially for AI-powered goods [1].

Our research intends to analyze the transparency and trustworthiness of these companies' data collecting, usage, retention, and protection procedures [2]. This evaluation is critical for understanding how these companies negotiate existing privacy requirements while preparing for future issues as AI and machine learning technologies improve. The global nature of data necessitates a global view on privacy, taking into account diverse legal and cultural standards [2].

In addition, the paper covers the significance of Privacy Impact Assessments (PIAs) in detecting and mitigating privacy risks in new initiatives, as well as providing insights into potential privacy issues and compliance gaps within major digital organizations. The research aims to provide best practices for other businesses to improve their privacy strategy and contribute to industry-wide privacy benchmarks.

Overall, the problem statement emphasizes the importance of analyzing these IT companies' privacy practices to understand their commitment to data protection, ethical AI use, and preparation for the shifting digital landscape.

II. Background

Consumers are becoming increasingly dependent on digital services and concerned about data privacy. Over time, it has become increasingly necessary to investigate the privacy practices of companies to determine if there is any wrongdoing. This paper overviews large technology companies such as Microsoft, Google, and IBM. These companies have a major impact on what consumers interact with on the web, so they must be scrutinized to determine if they are acting safely [3].

The General Data Protection Regulation (GDPR) of the European Union impacts how organizations manage personal data. This increasing need implores public awareness of their compliance, and legal proceedings if non-compliance is found. The National Institute of Standards and Technology (NIST) issues AI guidelines based on ethics and reliability, making it necessary to assess these companies' adherence to these standards, especially for AI-powered items [4]. Because they provide insight into how digital companies deal with possible privacy issues, Privacy Impact Assessments (PIAs) are crucial

for identifying and mitigating privacy risks in new initiatives [5].

The growing public desire for transparency in data collection, use, and protection emphasizes the significance of this research in determining these companies' transparency and trustworthiness. Understanding how businesses navigate current privacy limits allows them to assess their readiness for future challenges as AI and machine learning develop. Because data is globally available, a global perspective on privacy is essential, taking into consideration differing legal and cultural standards. Examining these internet behemoths' privacy practices can provide best practices for other businesses, helping them improve their privacy strategy. This analysis is essential for understanding these firms' commitment to data protection, ethical AI use, and readiness for the evolving digital landscape, as well as contributing to industry-wide privacy benchmarks and best practices [6].

A. *GDPR (General Data Protection Regulation):*

The EU's General Data Protection Regulation (GDPR) establishes severe regulations on personal data processing, stressing Data Minimization and Purpose Limitation, which require data to be collected only when necessary and for stated purposes. It requires explicit agreement for data processing as well as transparency in data use, storage, and sharing. Individuals are given rights such as data access, rectification, erasure, and portability under GDPR. To mitigate hazards quickly, high-risk operations require Data Protection Impact Assessments (DPIA) and a rapid breach reporting system [7].

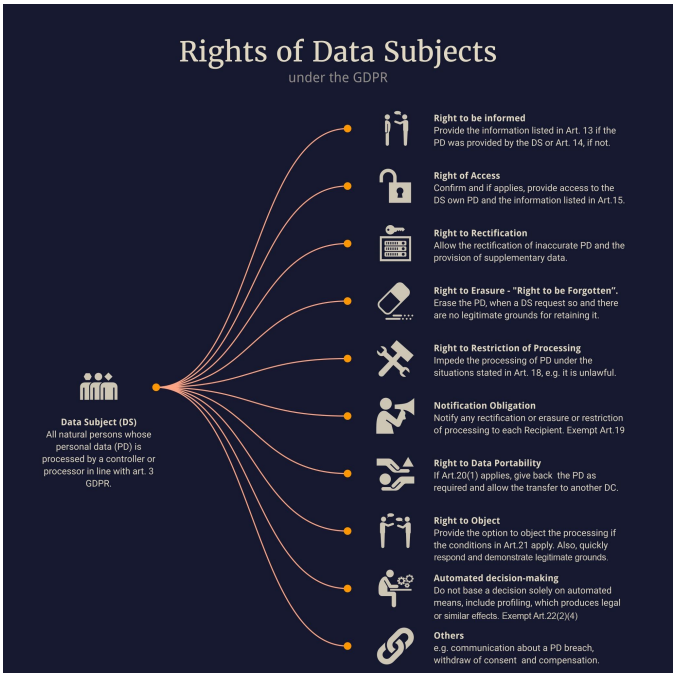

Fig. 1. Data Subject Rights Under GDPR

B. *NIST AI (National Institute of Standards and Technology - Artificial Intelligence):*

The National Institute of Standards and Technology (NIST) supports responsible AI development, with its AI Risk Management Framework focusing on reducing privacy concerns. This paradigm provides a structured strategy for detecting and mitigating risks in AI systems, including privacy problems. NIST promotes ethical AI development by incorporating privacy considerations from the start and offering guidelines and best practices. These initiatives ensure that artificial intelligence technologies are developed and implemented with a significant emphasis on privacy and ethical norms [8].

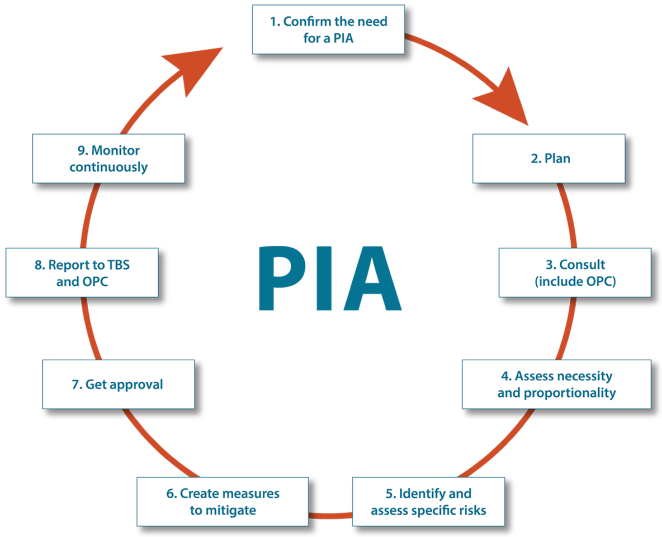

Fig. 2. PIA

C. *Privacy Impact Assessment (PIA):*

A Privacy Impact Assessment (PIA) is an important technique for organizations to use in identifying and mitigating privacy concerns in their initiatives. It entails a thorough examination of how personal information is acquired, used, kept, and shared. This approach aids in identifying potential privacy issues and compliance gaps, allowing for the establishment of risk management measures. PIAs stress privacy impacts and feature stakeholder participation, frequently through public consultations, making them vital instruments in privacy risk management [9].

D. *Tools:*

*1) **Microsoft copilot**:* Microsoft Copilot, which might be used using huge language models such as OpenAI's GPT, aids in coding and document creation by simulating human-like text. It has been trained using data from books, webpages, and coding repositories such as GitHub. To handle personal data, Microsoft enforces privacy policies, with data protection varying depending on the tool's application and user engagement. Measures may include data anonymization and security,

but the extent to which personal data is used is determined by user interaction [10].

*2) **Google**:* Google uses artificial intelligence and machine learning technologies in a variety of services, including its well-known search engine, voice assistants, and other goods. These technologies are backed by algorithms intended to handle and understand massive databases, allowing Google to efficiently deliver relevant results and services. The collection of vast data, which includes search queries, website visits (tracked through Google Analytics), and location information (when location services are enabled), is an important component of Google's operation. While Google claims to make different efforts to protect user privacy, such as anonymizing and encrypting data, the firm has come under fire for its massive data-gathering tactics and the possible hazards they pose to user privacy [10].

*3) **IBM**:* IBM's artificial intelligence (AI) technologies, such as Watson, are used in a variety of industries for data analysis, natural language processing, and pattern identification. To train AI models, data is collected from a range of sources, including business-specific and public data. IBM stresses data security and user privacy, particularly for enterprise clients, and adheres to stringent data protection rules, however, specifics differ by service [11].

III. Methodology

In our testing, we decided to gather our analysis in a tabular format to keep our results formatted in an easily digestible format. We took each of our three key models (GDPR, PIA, and NIST AI), and added their features to a separate page of our workbook. Then, we added a separate column for each of our three companies (Microsoft Copilot, Google, and IBM) and looked through the appropriate policies to find the areas that each company followed within the frameworks. The results of this table were then analyzed below in the discussion section. The final table can be accessed online [12].

IV. Discussion

A. Data Life cycle for Microsoft copilot, Google, IBM:

1) Data life cycle under GDPR:: AI systems such as Microsoft's Copilot, Google's AI, and IBM's AI solutions must follow strict data management rules under the GDPR framework. Data collection is controlled by legal, fair, and transparent norms, which necessitate explicit communication and agreement from data subjects. Data must be processed only for particular, valid objectives, ensuring accuracy and limiting the scope of processing [13]. Data storage entails secure processing and stringent retention limitations, with mechanisms for data subjects to request deletion under the 'right to be forgotten'. Data sharing, particularly across borders, necessitates proper safeguards, whereas data security necessitates powerful risk-aversion techniques. Finally, secure destruction or anonymization of end-of-life data is required, and organizations must undertake regular audits and report any data breaches to authorities [13].

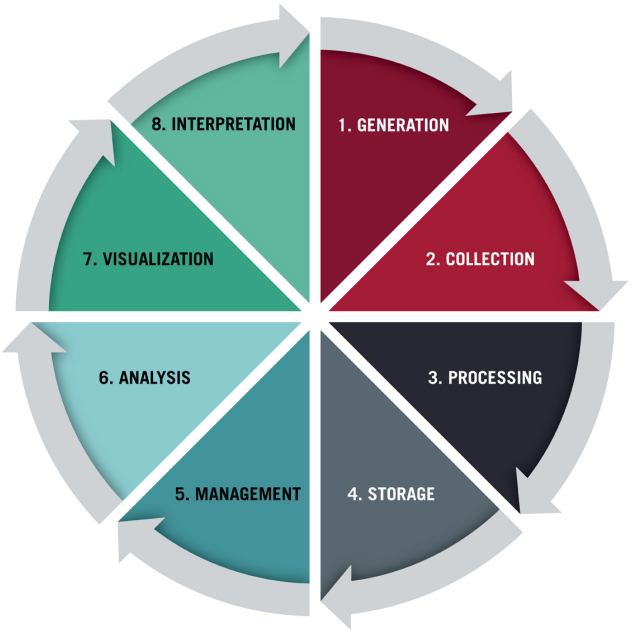

Fig. 3. Data Life Cycle [14]

*2) **Data life cycle under PIA**:* The PIA framework, on the other hand, focuses on examining the impact of data practices on privacy. It starts with assessing how personal data is acquired and verifying that it is required for the intended purpose. To minimize privacy threats, the framework examines the implications of data processing, storage procedures, retention policies, and management [15]. It also examines data sharing procedures to ensure they are following privacy rules and legal obligations. Security audits are essential for protecting data from unauthorized access and other dangers. To identify new threats and assure continued compliance with privacy rules, the PIA framework emphasizes constant monitoring and periodic reassessment [15].

*3) **Data life cycle under NIST AI**:* Under the NIST AI Framework, the data life cycle for AI systems such as Microsoft Copilot, Google AI, and IBM AI includes numerous critical stages. It begins with data collected from various sources, which is then processed and prepared for AI application[16]. This data is then efficiently saved and maintained. The following stage comprises data analysis and models utilizing AI algorithms to ensure that insights are derived accurately. Following that, these models are rigorously tested and validated to ensure performance and reliability. Once validated, these models are deployed and incorporated into a variety of systems, necessitating constant monitoring and maintenance to ensure their continued usefulness. Furthermore, a heavy emphasis is maintained throughout the cycle on data governance and compliance to conform to legal and ethical norms, a vital part of the NIST AI Framework in managing AI technology ethically and efficiently [16].

B. *AI Governances strategies:*

AI governance policies for technology companies such as Microsoft copilot, Google, and IBM are focused on ensuring that their AI systems are developed and deployed responsibly and ethically. Here's a rundown of some of the primary tactics they employ:

*1) **AI governances for Microsoft (Copilot)**::* For the developments of all AI technology, including the Copilot program, Microsoft has built a comprehensive ethical AI framework. Fairness, dependability, safety, privacy, security, inclusion, openness, and responsibility are among the concepts behind this paradigm. Microsoft has established a special AI Ethics Committee to oversee AI advances to assure adherence to these standards. Furthermore, the company highlights the significance of user input and control, allowing users to influence how AI systems such as Copilot interact with their data and tasks. Microsoft is committed to ensuring that people have clear information about how these systems make judgments and process data in its AI activities. Furthermore, Microsoft actively promotes and advances ethical AI practices through partnerships and collaborations with academic and industrial partners [17].

*2) **AI governances for Google:** :* Google has outlined a set of AI principles aimed at ensuring that their technology provides social benefit, safety, privacy, scientific difficulty, and responsibility. To fulfill these criteria, they created an independent AI Ethics Board that is in charge of analyzing AI initiatives and assessing their ethical implications and societal impact. Google also promotes open-source initiatives as a means of increasing openness and involving the broader community in AI development. Recognizing the need for ongoing learning and progress in the field, Google is actively involved in developing and financing research in crucial areas of AI ethics such as machine learning fairness, interpretability, and privacy. Furthermore, the company focuses a heavy emphasis on staff training and raising awareness about ethical AI development and usage, ensuring that their workforce is well-equipped to handle the complexity of AI responsibly [18].

*3) **AI governances for IBM:** :* IBM emphasizes trust and transparency in AI, emphasizing the necessity of explainability in AI decision-making processes. This focus is highlighted further by their creation of the AI Justice 360 Toolkit, a complete resource designed to detect and eliminate bias in AI models, emphasizing their commitment to AI Justice. IBM has built a systematic governance framework that guides its operations in this field to ensure ethical AI development and implementation [20]. Furthermore, IBM understands the need for collaboration with external organizations in creating responsible AI governance and is actively involved in this endeavour with policymakers and regulatory agencies. IBM has established an AI Ethics Board to reinforce its commitment to ethical AI. This internal organization is responsible for examining AI initiatives to ensure they adhere to IBM's ethical rules and procedures [20]. IBM has a clear AI Governance policy ensuring your AI is transparent, compliant, and trustworthy and all AI governance strategies are found on IBM's website.

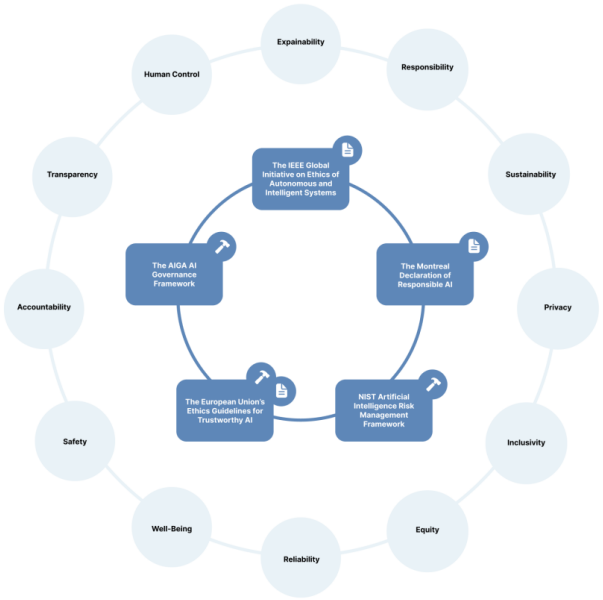

Fig. 4. AI Governances strategies [19]

*4) **Test Methodology**:* The initial stage of our process is to collect the frameworks that will be used. We discovered a PIA framework, a GDPR template, and NIST's AI framework to help us with our investigation. We shall use our frameworks to gain insight into the policies of this organization. We have entered the information of the three frameworks into a spreadsheet to compare them across our three firms. Following that, we will scan all three sources and enter any relevant information into the spreadsheet. This summary will be used to identify common and/or contrasting tendencies across the organizations, which we will highlight in our final report. With our summarized observations, we will recommend activities for any organization in this field to do to comply with privacy guidelines.

*5) **Privacy Risk**:* The General Data Protection Regulation (GDPR) and the National Institute of Standards and Technology (NIST) provide frameworks for addressing personal data privacy and security concerns. GDPR, which is applicable in the European Union, establishes criteria for lawful and transparent personal data processing, highlighting the risk of improper handling. Organizations must put in place strong security measures to protect personal data from breaches while also maintaining its availability, confidentiality, and integrity. GDPR also mandates Data Protection Impact Assessments (DPIA) for high-risk operations and requires specific informed consent for data processing[21].

NIST, a United States-based agency, focuses on cybersecurity and promotes stringent security safeguards. It advises against lax access controls and encryption, both of which can allow illegal data access. NIST highlights the necessity of incident response plans in addressing security vulnerabilities quickly[22]. Continuous monitoring of security measures is

also critical for detecting and resolving security issues as well as lowering the chance of undiscovered privacy breaches. Both the GDPR and the NIST aim to protect personal data through standards, consent, and strong security measures, but their techniques and scopes differ according to their various jurisdictions and focuses[22].

C. Applying the NIST AI Framework

The NIST AI framework specifically applies to AI policies, so separate AI policies were gathered for each of the three target companies. These policies are specifically used in only this section and are applicable throughout the section. The policies for Microsoft [23], Google [24], and IBM [25] can be found online in PDF form. All these policies are referenced constantly throughout the following paragraph (for brevity, citations were omitted). A summary of findings can also be found in a table created to summarize the findings of this model [12].

1) Govern: Govern principles surround the method of controlling the AI models. These surround internal criteria that only affect employees, and external criteria visible to everyone.

Under Govern 1 (Policy), many overseeing categories are covered from legal aspects to internal controls. From the Legal Perspective, Google has been forced into providing proof of understanding legal requirements by increased scrutiny by governments [26]. It's no surprise that this pressure means they are covering much of the Policy Section. IBM also covers most of the requirements in Policy through the consulting part of their business. Microsoft also covers many of the risk-management requirements of the Policy Section but does not properly account for the legal and regulatory aspects of AI. The companies are concerned about external compliance and systems for supporting external review requests. Only IBM covers risk tolerance, and it appears that Google and Microsoft are more concerned about offerings than risk.

Under Govern 2 (Accountability), it is required for companies to have people responsible for maintaining a chain that can be followed to ensure someone can prove a decision or fix a problem. Microsoft covers every section within this category, whereas IBM covers less and Google does not cover anything. Google's concerns do not lie with accountability of individuals or roles, they lie with the resulting product being useful. IBM's model covers accountability but does not cover accountability throughout the leadership chain. From IBM's consulting perspective, this makes sense since models need to be adaptable to meet customer specifications.

Due to rights movements around the world for Equity, Diversity, and Inclusion, all three companies cover the goals for Govern 3 (EDI) within their AI policies. This is likely due to public perception goals. On the other hand, all three companies are generally less concerned about principle Govern 4 (Organizational Culture); that their organizational culture is set up to properly safeguard AI, monitor risk, and test models. Only Microsoft Is concerned about internal safeguards and risk monitoring, and only Google is concerned about AI testing.

All three companies are concerned about principle Govern 5 (robustness). They all cover the requirements of the NIST model, gathering feedback from teams to better develop models. The Coverage of Govern 6 (Third Parties) is a bit more hit or miss because these companies may not collaborate with third parties in the same ways as smaller corporations. In the case of Google, it is less common to see them collaborating with others as they often build their systems. Google has partnerships to build their datasets [24]. Microsoft collaborates more often and IBM is a consultant, but none of the tools from all three companies account for high-risk data or AI systems.

2) Map: Map principles cover the application of Govern functions directly to the AI System. The process of mapping this should be covered within the methods being analyzed.

Map 1's (Context) principles cover the application of principles into a specific AI model. All three companies show concern about AI Adversaries but do not disclose their risk tolerance. It's also interesting that Google and IBM both identify concern for the business value of their AI, but Microsoft does not. This is potentially due to Microsoft's key business interests being within other corporate products.

Map 2 and 3 (categorization, targets) all have limited information available. This is likely due to keeping information internal and preventing competitors from getting an edge. This can be in the form of trade secret categorization methods, private business strategies, or others. Map 4 (Third Party Mapping) is not accounted for properly by most reports. This is a lack of oversight that needs to be resolved. The potential impacts of the AI model are seen under Map 5 (Impacts). Microsoft fully accounts for Impacts under the model, while Google falls short, and IBM does not analyze model impacts.

3) Measure: Measure principles involve the metrics that companies use to monitor the progress of their system. Within this section, the key criteria to evaluate from a privacy perspective is how data is being used to keep the model working.

Gathering performance data is covered within Measure 1 (Methods and Metrics). IBM does not have data in this section due to the generalization of their model. Microsoft's tools often have many ways to get metrics out of them, and this model is no different from that for them. Google has limited public knowledge of metrics, specifically targeting vulnerable communities.

Metrics gathered from Measure 1 can be used in Measure 2 (Trustworthiness) to evaluate how much trust we can put in the model. This, being the largest category in the entire model, makes it very difficult to cover all categories. All companies have coverage of different items here, but it's scattered over different criteria. Many of the models have not been out long enough to evaluate criteria Measure 3 and 4 (risk over time, feedback assessment), so there is limited content in most company's coverage. Microsoft does have this covered within their model though. Their standard has details to make it relevant and useful for longer.

4) Manage: Manage Principles handle the external effects of the model on society, of society on the model, and the risks exposed by allowing it to be used. Manage 1 deals with

responding to incidents as they arise. Google and IBM more publicly give response options in the case of something going wrong. Manage 2 (Maximize Benefits and Minimize Costs) is not a topic that is discussed by most companies as these are either trade secrets or not determined until applied to a specific project. Google is the only company of our three to cover it. Risk Treatments and Monitoring are also covered by all three companies so they have risk response capabilities.

The key uncovered category from this group is Manage 3 (Third Parties). Although all the companies have at least partial policies on the management of third parties, no companies surveyed had any policies on managing them once they are put into production. This is a critical management failure that must be accounted for.

V. Results

The output of the Results was taken from the Spreadsheet where we compared the policies for three different tools based on AI.

A. Result for NIST-AI:

In the Govern Function, companies are very concerned about the appearance of their compliance with legal requirements, and public opinion. Categories that are very public-facing are more covered (Govern 1, 3, 5), while those that concern internal practices are less covered (Govern 2, 4, 6). It can be argued that internal practices are more important because those principles drive the work companies are producing, but companies also operate in the court of public opinion. If you stay out of the court of public opinion, you stay away from government scrutiny, meaning internal principles are less critical when keeping the ship afloat. While all these companies covered much within the govern section, the application of that in Mapping fails to publicly cover the key interests of this model. Although it is likely intentional that much of this data is kept private, it is also possible that it does not even exist. In measure, Microsoft clearly showed that they have put work into their system that other companies have not covered surrounding performance metrics. Their system covers more details than IBM's and Google's policy but still needs work to be all-encompassing to monitor everything the model requests In Manage, it was shown that companies do not have sufficient protocols in place to manage their solution after the solution gets put into production. Sure, there are methods for feedback to the systems, but there is no method for risk response within most solutions.

B. Result for GDPR:

The GDPR sheet compares how Microsoft Copilot, Google, and IBM adhere to the General Data Protection Regulation (GDPR) rules, with a focus on data privacy procedures. While the sorts of data obtained differ and are not uniformly disclosed for each organization, the sheet exposes diverse data collection methodologies. Microsoft Copilot collects a wide range of information, including personal information, use information, and payment information. Google, on the other hand, is concerned with personal, demographic, and device data. Similarly, IBM collects personal information, service interaction data, and device information. Data collecting methods also differ: Microsoft Copilot captures data during account creation or service use, Google during service registration or interaction, and IBM during service use or event registration.

All three organizations collect data from client interactions via surveys, feedback forms, and other means. This report provides insights into their GDPR compliance, emphasizing their distinctive data handling techniques and displaying their dedication to privacy and data protection in a fast-changing digital context.

C. Result for PIA:

The spreadsheet "Privacy Comparisons" provides an analytical summary of privacy practices in Personal Information Assessment (PIA) across Microsoft Copilot, Google, and IBM. It demonstrates that IBM does not handle personal data, whereas Microsoft Copilot and Google do. While Microsoft Copilot admits to collecting personal information, Google does not, and IBM's position is unclear. Microsoft Copilot and IBM are participating in the types of personal data, but Google's stance is unknown.

In terms of third-party involvement, Microsoft Copilot and IBM, unlike Google, operate independently of third parties. All three companies agree on the collection of non-personal data, demonstrating a shared methodology for collecting non-identifiable information. This comparison demonstrates the major tech giants' various privacy policies and procedures. We mentioned the comparison of the privacy policies was done through the spreadsheets.

VI. Conclusion

Our analysis has gone to prove that although companies say they care about your privacy, they still fall short of living up to public reputable standards. In the digital era we live in now, companies are still more concerned about their economic bottom line than the triple bottom line. Society is at a disadvantage as long as solutions do not have the proper safeguards in place. As we continue forward, we hope that companies can see where their weaknesses are using these findings to improve their methodologies and make systems that are more beneficial to society as a whole.

References

[1] Y. Huang, Y. Li, W. Wu, J. Zhang, and M. R. Lyu, "Do not give away my secrets: Uncovering the privacy issue of neural code completion tools," *arXiv preprint arXiv:2309.07639*, 2023.

[2] I. S. Rubinstein and N. Good, "Privacy by design: A counterfactual analysis of google and facebook privacy incidents," *Berkeley Tech. LJ*, vol. 28, p. 1333, 2013.

[3] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[4] N. AI, "Artificial intelligence risk management framework (ai rmf 1.0)," 2023.

[5] D. Wright, "The state of the art in privacy impact assessment," *Computer law & security review*, vol. 28, no. 1, pp. 54–61, 2012.

[6] S. Wang, Z. Chen, Y. Xiao, and C. Lin, "Consumer privacy protection with the growth of ai-empowered online shopping based on the evolutionary game model," *Frontiers in public health*, vol. 9, p. 705 777, 2021.

[7] S. Sirur, J. R. Nurse, and H. Webb, "Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr)," in *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, 2018, pp. 88–95.

[8] A. M. Barrett, D. Hendrycks, J. Newman, and B. Nonnecke, "Actionable guidance for high-consequence ai risk management: Towards standards addressing ai catastrophic risks," *arXiv preprint arXiv:2206.08966*, 2022.

[9] R. Clarke, "Privacy impact assessment: Its origins and development," *Computer law & security review*, vol. 25, no. 2, pp. 123–135, 2009.

[10] F. Morandín-Ahuerma, "Ethics of ai from global companies: Microsoft, google, meta, and apple1,"

[11] E. Bertino, C. Brodie, S. B. Calo, *et al.*, "Analysis of privacy and security policies," *IBM Journal of Research and Development*, vol. 53, no. 2, pp. 3–1, 2009.

[12] J. Cepler and T. Kalyani, "Privacy comparisons." [Online]. Available: https://docs.google.com/spreadsheets/d/19rT3T1KEdhP1NdZrpKuvGUW8XGh9x1Vy4-Eio_UpR9I/edit?usp=sharing, see attached excel spreadsheet.

[13] K.-B. Ooi, G. W.-H. Tan, M. Al-Emran, *et al.*, "The potential of generative artificial intelligence across disciplines: Perspectives and future directions," *Journal of Computer Information Systems*, pp. 1–32, 2023.

[14] [Online]. Available: https://segment.com/blog/data-lifecycle/.

[15] K. Vemou and M. Karyda, "An evaluation framework for privacy impact assessment methods," 2018.

[16] M. P. Heim, N. Starckjohann, and M. Torgersen, "The convergence of ai and cybersecurity: An examination of chatgpt's role in penetration testing and its ethical and legal implications," B.S. thesis, NTNU, 2023.

[17] [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.

[18] Google, *Google ai principles*. [Online]. Available: https://ai.google/responsibility/principles/.

[19] N. Malter, *European ai alliance - implementing ai governance: From framework to practice*. [Online]. Available: https://futurium.ec.europa.eu/en/european-ai-alliance/best-practices/implementing-ai-governance-framework-practice.

[20] IBM, *Ai governance: Ensuring your ai is transparent, compliant, and trustworthy*, Oct. 2015. [Online]. Available: https://www.ibm.com/analytics/common/smartpapers/ai-governance-smartpaper/.

[21] K. Manheim and L. Kaplan, "Artificial intelligence: Risks to privacy and democracy," *Yale JL & Tech.*, vol. 21, p. 106, 2019.

[22] N. AI, "Artificial intelligence risk management framework (ai rmf 1.0)," 2023.

[23] *Microsoft responsible ai standard, general requirements*, 2nd ed., Microsoft, Jun. 2022. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5cmFl.

[24] *2022 ai principles progress update*, Google, 2022. [Online]. Available: https://ai.google/static/documents/ai-principles-2022-progress-update.pdf.

[25] *Foundation models: Opportunities, risks and mitigations*, IBM Corporation, Jul. 2023. [Online]. Available: https://www.ibm.com/downloads/cas/E5KE5KRZ.

[26] M. McHardy, "Governments accused of using apple and google push notifications to spy on users," *The Independent*, Dec. 2023. [Online]. Available: https://ca.news.yahoo.com/governments-accused-using-apple-google-185211811.html.