


Usability Study on Data Protection Automated Policy Reviewer Tool for the Jamaica Data Privacy and Protection Environments

Mijan Morgan, BSc¹ 

¹University of Technology, Jamaica, mijanlmorgan@students.utech.edu.jm

Abstract– This paper provides a summary analysis specific to the conceptual requirements elicitation process towards the provision of a Human-Computer Interactive environment that tracks how we can evaluate the relevance of the various information technology security policies by way of search, updates, and mapping services for said documents. The Human-Computer Interaction tool is called our Data Protection Automated Policy Reviewer. This usability study supports a basic thematic analysis using a qualitative method. We chose to engage a convenient sample as our approach is to glean feedback with respect to a target audience familiar with the HCI concepts impacting the user experience which are then applied front-end design of our automated policy reviewer tool. In essence because of the high-level experimental user interface prototype along with the thematic reviews on the usability of our user interface for the policy reviewer, our work borders on a mixed methodology. This usability study builds on the contributions of authors of [8], [11], [12] and [13] through their related work on data privacy compliance within their respective scopes explained from the national, international, virtual, and physical perspectives.

Keywords- data protection; automation; policy implementation

I. INTRODUCTION

With the advent of the Jamaica Data Protection Act (JDPA) (2020) and its recent regulations that took effect on December 1, 2023, it has been noted that several organisations have been grappling with reconciling their data protection policies and all other associated policies that treat with personally identifiable and sensitive information within the organisation setting [1]. Implementing a data privacy programme that complies with the JDPA involves the careful consideration of the legal requirements of the data processing standards, which include [2]:

1. Fair and lawful processing,
2. Processing for one or more specified lawful purposes
3. Personal data is adequate, relevant and limited to what is necessary,
4. Personal data is accurate and kept up to date,
5. Proper retention and disposition is observed,
6. Processing is executed in accordance with data subject rights,
7. Technical and organisational measures are in place to protect against unlawful loss or damage, and,
8. Cross-border transfers are prohibited unless the state or territory outside of Jamaica ensures an adequate

level of protection in accordance with the rights of data subjects.

The JDPA boasts similar legal requirements to Europe's General Data Protection Regulations (GDPR), separated by slight nuances contributed by not only the physical geographic region but also differences in the approach to direct marketing, the right to erasure or to be forgotten, and penalties, among others. Due to the global effect of the GDPR, many countries have implemented or updated their privacy law(s) to include a direct or partial alignment with the European counterpart. This has further contributed to the issue of compliance for companies trading across borders and in different regional markets. The proffered solution to regional or global compliance, as the case may be, is posited in the implementation of an automated data protection policy review tool. Our work borrows from the authors in [3] the basic human-computer interaction framework for how we develop these types of data protection automated policy tools. HCI, over the years, has always been studied as an important sub-discipline of the Information Systems Management (ISM) field that considers the user's perception, attitudes and acceptance towards new technologies based on the developer's cognition of how the task is executed [4]. The basic framework assumes the following:

Definition of the system characteristics – this includes the basic functional requirements of the system that seeks to host our data protection automated policy reviewer service, seen in Fig. 1. We deploy our prototype design using the popular SITE 123 platform which runs on a public data cloud and loads as a website to the end user of our software as a service (SaaS) application.

Definition of Task characteristics – this automated policy reviewer tool has the basic requirements to carry out a policy search that will read the inventory database of policy text documents (e.g. .doc, .pdf) and load these policies to the end user, which in the context of this study, is our policy reviewer, data protection officer, or members of the data protection and privacy governance committees within the organisation(s).

The next task requirement is to perform a data classification and mapping function, consistent with what data is collected and stored within the different organisational database tables. Tables can be both of a structured and/or unstructured format, and a parsing routine is applied to this task to map the basic GDPR, by looking at the data type, purpose for the data collection, data retention period, data

Digital Object Identifier:
ISSN, ISBN:
DO NOT REMOVE

accuracy say using encryption or hashing techniques, and the verifiable logging mechanisms that support the data collected from these millions of records situated within these tables. This is a fine-grained analysis of the data sets because any anomaly based on the predefined GDPR rules runs the risk of a potential breach of the data sitting in these tables. This task captures the basic technical measures consistent with the data protection policy implementation within the organisation.

The fourth task is that of a Policy Mapping function. This Policy Mapping function is consistent with the need to drive an organisational measure. More specifically, the policy mapper generates an organisational table which shows the named policies, the policy owners, and the context in which the policy is applied or used for each department within the organisation. For example, in a hotel scenario, guest data applies an acceptable use encryption policy and a data disposal policy, with the measure that says all credit card data within the organisation is to be encrypted, and all credit card data older than seven (7) years need to be disposed of. Both Guest Services Supervisors and the Technical Services Manager would have remit for this function, in relation to the encryption and data disposal requirement. The Policy Analysis task looks at doing basic pattern analysis as a form of statistical inferencing as the underlined intended requirement. In short, when a policy is being read, a check across all policies within the policy inventory database is done to determine what are the common observations. Ideally, each policy should contain a policy revision table, and a section within the text document referring to “employee training and awareness”, a lack of one or more of these observed features based on the analysis may warrant a policy update as the requirement. Additionally, features of the task related to policy analysis would also look at the last modified dates when the policies were reviewed and provide a report on such policies by way of an update.

This now takes us to the final task which is our Policy Updates. The threshold for a policy update is set to be every three (3) years, anything exceeding this date warrants such an update. This feature can search for all recently updated policies, read for such a requirement, and where applicable, run the update against the said document(s). While this study does not assume that there could be errors within these documents that are updated and likely run the risk of policies being a source of dirty data, our assumptions at this time with all things being equal, assume a clean data set of information uploaded from policy files based on the prescribed formats. The policy update feature assumes that we can parse a document using basic read/write rules to make the changes to a prescribed policy setting. This feature under the task characteristics, can seek to assume that we should check for task error rates by way of outcomes like redundant processes, or repeated data not related to a task. Task completion and task responsiveness also come with a need for that type of observation under this requirement that can be tested. Fig. 1 below, helps to define the task characteristic requirement for the automated policy reviewer tool.

Definition of User characteristics – this feature speaks to the end user expectations and outcomes. A clear outline between what is perceived and what actually obtains/exists represents two different things. In our current design, we are still conceptual in our approach to suggest what is to come or what is expected by way of the design in a live production environment. We use basic Java to simulate the back-end functionality which is still a work in progress.

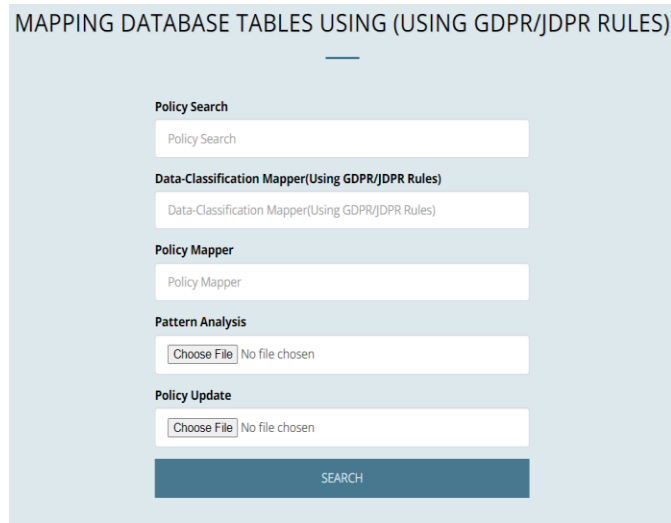


Fig. 1 User interface design for the Data Protection Automated Policy Reviewer tool.

Having introduced, at length, the vision for this conceptual policy reviewer, the remainder of this paper includes the methodology and analysis of the study discussed in section 2 which highlights the main takeaways of the experiment that would contribute to the tool’s development. Section 3 looks at the contributions and research into related works, and their contribution to the tool’s design and/or functionality. Section 4 presents our conclusions and summarises our key findings, while Section 5 outlines the paths for future work and development of the prototype tool.

II. Analysis

In this section of the paper, we provide a preliminary analysis of the results from our usability study, using a convenient sampling method. We created a Google Form survey to share our screen design and schematics with 93 persons to date, to evaluate the intuitiveness of the design. The schematics included a strawman model of the software’s Policy Parser Engine, Data Classification & Mapping Engine, and Mapping Database tables using GDPR/JDPR rules. To qualify as a participant in this study, respondents would have had intimate knowledge of the data privacy and protection rules, application design/development, principles required to satisfy compliance with the JDPR, or have been operating in the policy development and administration space. The sample

size is challenged by the lack of available experts practising within the field.

Of the ninety-three (93) prospective participants, twenty-nine (29) responses were received. Though it reflected a less-than-significant sample size, the quality feedback was analysed to gauge the features, usefulness, and applicability of the tool. Fig. 2 depicts the functional areas of the participants.

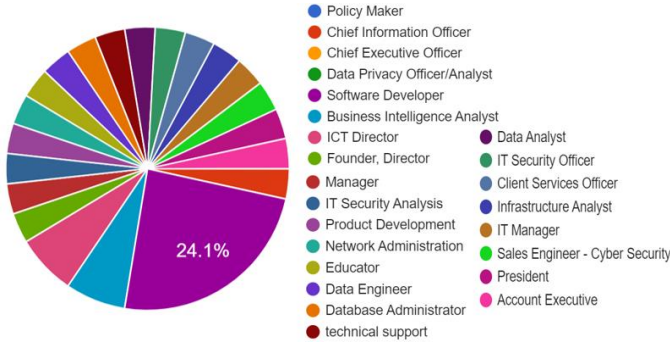


Fig. 2 Google survey responses on participant’s functional areas.

From Fig. 2 above, the observation indicates, that of the twenty-nine (29) participants, the demographics of the persons with whom the survey was shared were IT Managers, CEOs/founders of companies, software developers, Chief Information Officers, and Policymakers within academic as well as private sector companies.

The responses in Fig. 3 observed 6/29 respondents (20.7%) have the least interaction with software tools related to data protection and privacy policy and captured a score of 1 out of 5 on the Likert scale. More impressively, 8/29 respondents (27.6%) have some limited level interaction with a score of 2 out of 5. 4 respondents, representing (13.8%) have somewhat frequently interacted with software tools of this nature and the remaining 11 respondents (totalling 37.9%) represent users with frequent interaction with data protection and privacy HCI-focused tools, indicating levels of interaction at 4 and 5 on the Likert scale. The responses indicate that this study would benefit from the users’ expert advice as to what would make the tool an improvement on existing offerings, or at the very least, critique as to overlooked functionality in comparison to the participant’s exposure.

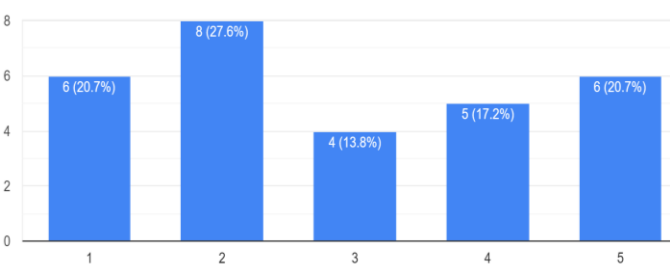


Fig. 3 Interaction level with HCI-focused policy management tools among participants on a scale of 1 (least frequent) to 5 (very frequent).

In terms of the ease of understanding the automated policy reviewer tool, participants rated the tool’s operation, excluding the need for extensive code development. Fig. 4 represents the charted responses to indicate where 3/29 respondents (10.3%) deem the tool very easy to understand as indicated by selecting 1 on the Likert scale. 7/29 respondents (24.1%) indicated the tool was fairly well understood and straightforward in the conceptual design. 12/29 respondents (41.4%) conveyed that the tool was neither straightforward nor complex in design and therefore communicates a fair/average enough ease of understanding of our policy reviewer tool. This is evidenced by a 3 out of 5 on the Likert scale. 6 respondents, representing 20.7%, then indicated there was a reduction in the ease of understanding as they deemed the tool slightly more complex. 1 respondent (3.4%) found the found the conceptual design very complex.

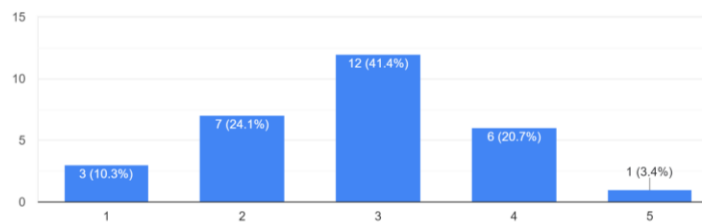


Fig. 4 Feedback analysis on user understanding of the prototype policy tool in the absence of extensive coding.

To gauge Interaction or increased engagement with the policy reviewer tool, participants were asked to indicate what HCI feature was the most important to incorporate. Preferences overwhelming 51.7% indicated the user design interface was essential or preferred for continued engagement. Fig. 5 illustrates this feedback.

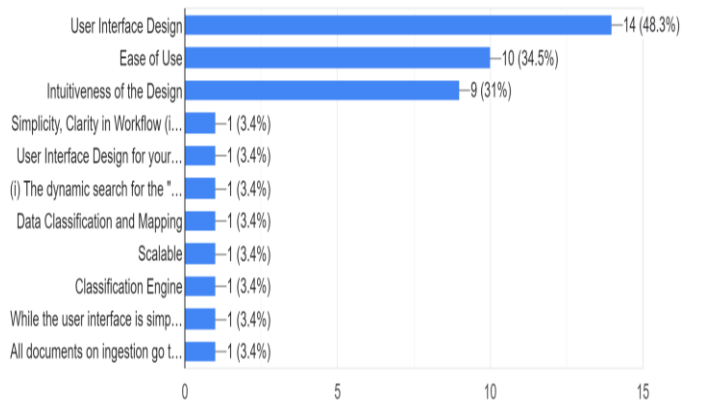


Fig. 5 Preference in HCI features for Automated Policy Reviewer Tool.

As researchers who are invested in the performance of the policy review tool in not only having an interactive UI, it should also be fit for purpose. Respondents were able to freely express their thoughts on the ability of the tool to handle data

protection and privacy-related tasks of policy reviewing and updating. The majority of the participants are truly of the opinion that the tool could manage the tasks highlighted with ease based on its modular design and its consistent and repetitive approach to streamlining a traditionally manual procedure. Many could appreciate the straightforward design and logical approach to policy management but are understandably concerned about just how easily the analysis could be executed if the tool is not connected to an external policy infrastructure. We can then infer that as-is the policy reviewer tool may be effective at assisting policy handlers but only in a context where it either considers integration with privacy leaders at the industry level or possible Artificial Intelligence (AI-enabled) resource that facilitates machine learning and pre-emptive updates.

Additional enquiry into the completeness and usability of the conceptual tool elicited consensus to indicate that additional features are not required in order to increase the usability of the tool. This suggested to the researchers that the majority of the convenience sample is comfortable accepting and using the policy reviewer tool as-is. Acknowledging that, as with any prototype, there will be iterations and improvements, the majority had not suggested updates at the time of participation. However, opposing views shared the inclusion of privacy controls, tooltips/How-to's/interactive onboarding, date, geolocation field, and even the use of AI engines to integrate with the parser engine would be great additions to enhance the facility. Upon aggregating these suggestions, we understand that the tool's simple design may be easy to interact with based on its current HCI features but may not be as easily understood and operable. We also see this sentiment expressed in the statistical analysis captured on the perceived ease-of-use scale. Therefore, to really be effective, the tool needs the support of additional features to incite use.

Though a favourable and simplistic design was presented and appreciated by the sample, significant and noteworthy concerns were raised as possible prohibitors to the tool's success. These are particularly concerning contextual ambiguity as the lexical and syntax analysis may have difficulty decoding jargon, slang, and idiomatic expressions, thus raising the error rate of the tool's accuracy. This coincides with other concerns about the robustness of the tool's mapping and parser engines' ability to handle complex updates and how those considerations are incorporated in the planning and development phases of the software development life cycle (SDLC). As an extension of this challenge, the question of, how soon after legislative change will the tool receive and suggest/commit the update(s)? Additionally, we can draw inspiration from [5] and [6] in prioritising the security concerns regarding the safety, integrity, strategy, management and quality of the monitoring services or other resource(s) that could feed the policy reviewer.

Of all the suggested challenges that could face the development and implementation of the Policy Reviewer Tool, there remains a very real possibility of low technological acceptance, trust or overall buy-in in regards to the tool's

usefulness. Nonetheless, almost all respondents responded favourably to recommending the tool for further design and practical application development. The envisaged benefits are derived mainly from the ardent need to stay compliant with constantly evolving yet punitive privacy legislation(s).

The independent feedback from the sample was interpreted and incorporated into version 2 of the Policy Reviewer Tool, as seen below in Fig.

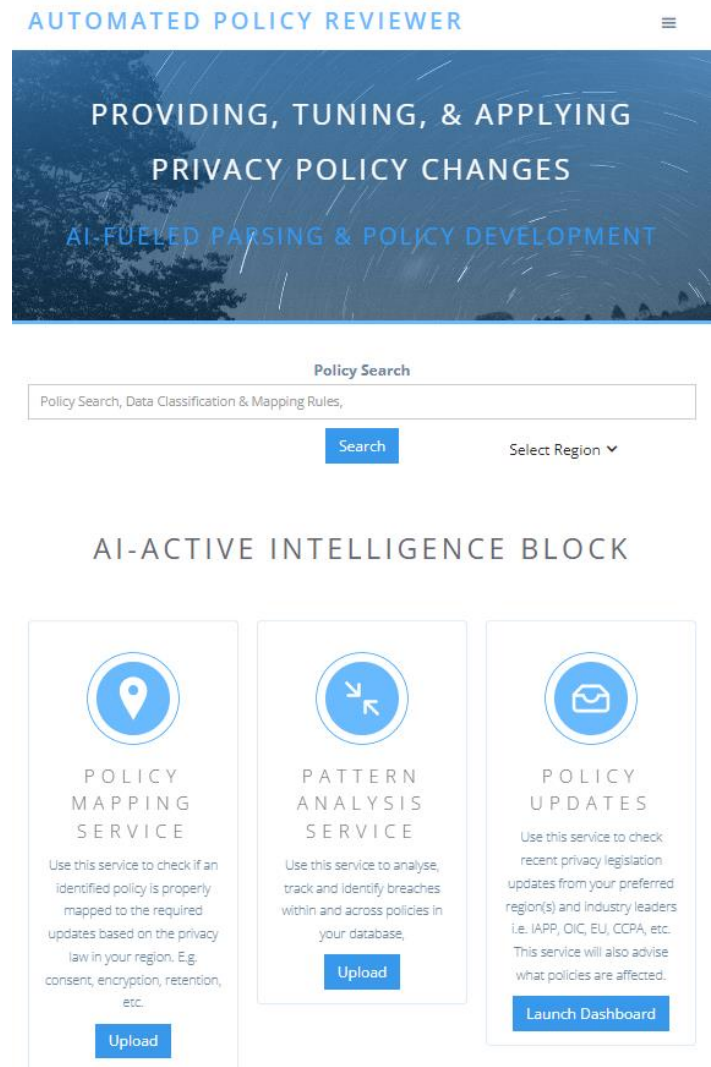


Fig. 6 Redesign of the Automated Policy Reviewer Tool with user feedback to enhance HCI features using Webflow.

III. RELATED WORK

During our research, we investigated the current status of GDPR, HIPPA, or even CCPA compliance among software applications and their ability to maintain that compliance among a diverse user base, and particularly the challenges they faced in doing so. The study by [7] on the Privacy Policies of Free Medical, Health, and Fitness Mobile

Applications and the GDPR, focuses on the data handling practices of fifty (50) apps across their scope: 31 medical and 19 health affiliated. The study posited concerns of potentially compromised user privacy via the over-collection of user data beyond what's necessary for functionality, issues contributing to informed consent as privacy policies were vague and lacked granularity for consent to be provided on different purposes for data usage and under what legal reason the processing was being executed. This further underscored the clear need for policy requirements that guide data collection, classification and mapping as a primary requirement not only under the EU's GDPR but also signals similar considerations for the JDPR, specific to policy implementation and compliance. We find where our work compliments and expands on the boundary of this body of work by [7], considering the policy challenges with international data protection regulations other than just the GDPR and how emerging technologies like AI can be used to assist entities in adapting appropriate and relevant data protection strategies.

In a study by [8] the authors significantly contribute to this concept by implementing a system designed to automatically detect violations between mHealth (mobile health) applications and the GDPR. The user software, called HPDROID, uses various machine learning algorithms that scan and analyse applications data practices against GDPR compliance requirements and takes it a step further to include an experimental prototype that supports systematic investigation into the mHealth-GDPR compliance. [8]'s study revealed that a substantial portion of these apps were not compliant and raised the need for awareness among users and developers. The main aim of this study was to raise awareness and educate stakeholders on privacy and empower users to make informed decisions about applications they chose to use while offering developers a tool to identify and rectify compliance issues during the software development lifecycle (SDLC), but definitely before app or software release. The mission of [8]'s study shares the same as our own as we seek to develop an internationally applicable version of our automated policy reviewer under the JDPR, to support the improvement of user awareness as well as support the front-end stack development of these applications to be most intuitive for such end users and guide developers in rectifying privacy gaps before apps reach the public domain, potentially reducing privacy breaches and legal liabilities.

The authors in [9] contribute to the above discourse by imparting an understanding of the impact of GDPR on the readability and content characteristics of privacy policies in mobile apps. The methodology involved the use of a web crawler to collect privacy policies, pre-GDPR and post-GDPR implementation, from the Google Play App Store for twenty-four thousand one hundred and ten (24,110) apps in both English and German and then performed an analysis using quantitative textual metrics (e.g., number of sentences, words) and popular readability metrics (FKGL, SMOG, FRE, etc.) for English and German texts.

The study revealed that the introduction of the GDPR did not positively impact the readability of privacy policies for most categories of mobile apps, as between the initial and new versions of the policies, there was an increase in the number of sentences per policy. However, categories such as Music & Audio, News & Magazines, and Medical, among others, show improved readability post-GDPR. Categories like Productivity, Shopping, Communication, etc., exhibit a decline in policy readability despite the privacy policy's emphasis on clearer policies. The authors' work contributes to the need for understanding the nuanced impact of GDPR on privacy policy characteristics and even though it is focused on mobile apps for the end users, it sheds light on readability changes and content alterations post-GDPR implementation as just one of the issues affecting compliance for organisations. This informs our own study to ensure updates ingested from legislative developments, industry best practices, or any other source, should leverage the lexicon of both the issuer and receiver to increase not only the readability of the policy update(s) but also the understandability and applicability of the policy statements.

The authors of [10] further progress the work of [7],[8] and [9] by introducing a model to facilitate fine-grained, policy-driven controls for information sharing within healthcare settings using a publish/subscribe framework. The model posited in the paper advocates and introduces a policy-based approach to govern the dissemination of medical information. These policies are designed to define the conditions under which data access is permitted and enable customization of information based on specific contexts or requirements. This publish/subscribe model advocates for a dynamic policy template approach to the policy implementation process and the build-out of a Middleware integration model on top of the publish /subscribe middleware, enhancing its capabilities to enforce information-sharing policies. This integration allows for the seamless implementation of policy-driven control within an active notification environment, allowing for attribute-level sharing of medical information. In essence, the model achieves this by allowing policies to dictate conditions for data access and ensuring that sensitive data is only released under specified circumstances. A further finding of this work is the tailoring of information based on particular contexts or requirements specified in policies. The model ensures that shared data is relevant and appropriate for the intended recipients or situations. Hence, within the context of an augmented publish/subscribe framework, the integration of policy-driven controls within the publish/subscribe middleware enhances its functionality. It transforms the traditional publish/subscribe system into a more robust and adaptable platform, suitable for sensitive healthcare environments. This work captures well, the desired approach of our own work in applying relevant and appropriate policies within the context of the user's region and business interests practices and adhering to privacy regulations.

The authors of [11] outline a model framework that emphasizes the initiation of a user dashboard, serving as a communication medium between the News Media industry and its users. This dashboard facilitates user consent management and provides transparency in data usage policies. This lends well to our own work in terms of the creation of a front-end end user interface dashboard to interact with the functional policy documents that serve as an enforcement point within the data protection-regulated environments. By implementing various use cases of their industry, this work demonstrated significant transformations necessary in user data management processes to align with GDPR regulations. The work by [11] also advocates a system design and development requirement with a detailed discussion on system design elements, such as the user dashboard requirements and functionalities, highlighting the necessary features for ensuring compliance, including user consent options, policy management, and data collection processes. The authors also delineate very well, an active data flow management provision where the data flow within a news media corporation, illustrates how data is collected, stored, and utilized in compliance with GDPR guidelines. We contend that this type of data flow and its associated mapping needs to also occur within our JDPR environments. The work by these authors demonstrates a useful discussion around the GDPR impact in terms of the specific implications of GDPR compliance, penalties for non-compliance liabilities for service providers and consumers, potential issues, and related works in the field. The proposed graphical representations, Fig. 7, and streamlined approaches for presenting privacy policies could contribute to improved transparency and user comprehension in various industries beyond news media and draw parallel to our own efforts with respect to the modelling for our own JDPR designs.

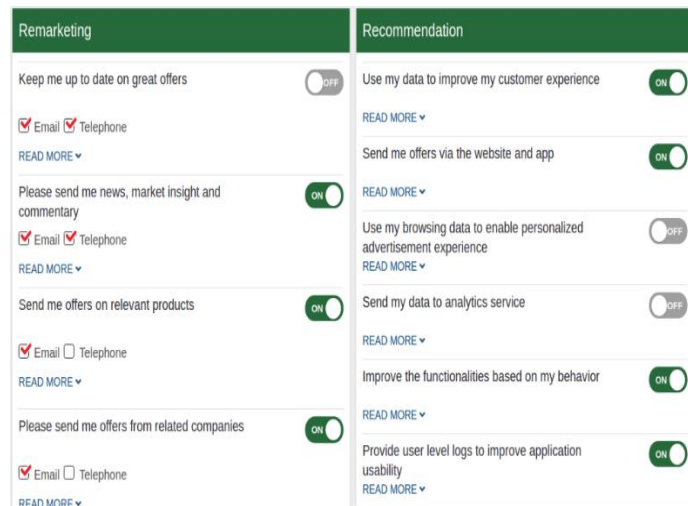


Fig. 7 Sample User Dashboard design by authors of [11].

IV. CONCLUSION

The challenges of data privacy compliance are not unique to any one region. The authors of [8], [11], [12] and [13] significantly contributed to this point and ultimately our research through their related work on data privacy compliance within their respective scopes. Their perspective further explained the national, international, virtual, and physical challenges or breadth of issues being experienced by all industries and countries, exacerbated by the fact that there were cultural and administrative hurdles with respect to the transition required to support the type of policy adherence. While some industries may receive more pointed attention, like Media and Medical, for their sensitive personal data, the overarching risk and liability to this data increases if policies are misapplied. The convincingly positive feedback and interpretations, from both the related work and our respondents, indicate that there exists a gap in the data privacy discipline as far as it concerns the need for policy management, maintenance, and data classification and mapping, validating the contribution of our work.

The overwhelming impression is that privacy professionals and policy managers have always been relentlessly trailing a moving goal post as their responses suggest the creation of the policy reviewer tool that leverages HCI and artificial intelligence, would finally allow many businesses, particularly in the private sector, to attain and retain compliance, especially in Jamaica where the introduction of the privacy is still novel. One participant would highly recommend this tool due to its particular benefit to the supervisory authority in Jamaica in promoting automation as a part of regulatory compliance, and by doing so, illuminating the wider picture as we leverage the advancements in technology, and particularly the ability to apply the use of that technology within data processing practices of international data processors using complex privacy policies to chase compliance across multiple regions.

V. FUTURE WORK

This study is poised to emerge from a conceptual design and enter the prototyping development stages of the SDLC. With the steady progression of the tool's development, the researchers acknowledge the need for sensitisation and training of policymakers and enforcers regarding the Data Protection Act (2020) within Jamaica. The limited exposure to the targeted legislation directly impacts the participation of the convenience sample for policymakers/enforcers who are not data privacy professionals. Therefore, incorporating focus groups and interviews could help uncover valuable perspectives towards the tool's development by removing the uncertainty of a self-paced questionnaire and the insertion of an interactive human component.

Outside the current research, additional investigation into the influencing factors of legislative or policy enforcement could contribute valuable insights or trend analysis as to how

privacy policy statements, guidelines, or frameworks are created and differ across regional and international boundaries.

REFERENCES

- [1] ISSA International. (2023, October 3). Challenges and opportunities in implementing privacy by design in the Caribbean - The Jamaica Data Protection Act 2020 as a case study - ISSA International. <https://www.issa.org/event/challenges-and-opportunities-in-implementing-privacy-by-design-in-the-caribbean-the-jamaica-data-protection-act-2020-as-a-case-study/>
- [2] Government of Jamaica, Jamaica Data Protection Act (2020) , <https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf>, retrieved December 2, 2023
- [3] Rzepka, C., & Berger, B. (2018). User Interaction with AI-enabled Systems: A Systematic Review of IS Research. *ResearchGate*. https://www.researchgate.net/publication/329269262_User_Interaction_with_AI-enabled_Systems_A_Systematic_Review_of_IS_Research
- [4] (PDF) The Intellectual Development of Human-Computer Interaction Research: A Critical Assessment of the MIS Literature (1990-2002). (2003, September 1). ResearchGate. https://www.researchgate.net/publication/220580561_The_Intellectual_Development_of_Human-Computer_Interaction_Research_A_Critical_Assessment_of_the_MIS_Literature_1990-2002
- [5] Carl A Gunter , Security Policy implementation strategies for Common Carrier Monitoring Service Providers, Proceedings of the IEEE Symposium on Policies for Distributed Systems and Networks , 2009.
- [6] Cheng, G., Li, Y., & Liu, X. (2017). Cloud Data Governance Maturity Model. China Electronic Product Reliability and Environment Testing Research Institute.
- [7] Muhammad Yaqub; Feng Jinchao, Imran Shabir, Chuhan Kaleem, Privacy Policies of free Medical, Health,Fitness Mobile Applications and the GDPR , Proceedings of the 5th International Conference on Intelligent medicine and image processing , 2023
- [8] Ming Fan, Le Yu , Sen Chen, Hao Zhou , Xiapu Luo, Shuyu Li,Yang Liu , Jun Liu,Ting Liu An Empirical evaluation of GDPR Compliance Violations in Android Health Apps, Proceedings of the 31st IEEE International Symposium on Software Reliability, 2020.
- [9] Maxim Anikeev, Haya Shulam, Hervais Simo Privacy Policies of Mobile Apps – A usability study , IEEE conference on Computer Communications workshops , 2021
- [10]Jatinder Singh, Luis Vargas , Jean Bacon , Ken Moody, Policy Based Information Sharing in Publish/Subscribe Middleware, Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks, 2008
- [11]Ahmedur Rahman Shovon, Shanto Roy, Arnab Kumar Shil,Tanjila Atik, GDPR compliance - : Implementation use cases for user data privacy in News Media industry, Proceedings of the 1st International Conference on Advances in Science, Engineering, and Robotics, 2019
- [12]Nina Gumzej, Law and Technology in data processing – A risk based approach in EU data protection law and implementation challenges in Croatia , Proceedings of the 40th international convention on Information and Communication Technology, Electronics and Microelectronics, 2017.
- [13]Muhamad Abubakhar , Armaya`u , Umar , Abubakhar, Personal Data and Privacy protection regulations : State of Compliance with Nigerian Data Protection Regulations (NDPR) in Ministries , Departments , and Agencies , 5th Information Technology for Education and Development, 2022.