



The Data Protection Act in Jamaica: Implications for Research Practice and the Legal Status of Demographic Data

Paul Andrew Bourne¹, PhD, DrPH & Feliciano Thorpe², MSc

¹Adjunct Professor, Northern Caribbean University [NCU], Manchester, Jamaica, WI.

²Student Success Coach, Excelsior Community College, Kingston, Jamaica, WI.

Abstract

The enactment of the Data Protection Act (Jamaica, 2020) represents a transformative shift in the governance of personal information in Jamaica, aligning national legal frameworks with global data protection standards such as the GDPR. This study examines the structure, principles, and operational implications of the Act, with a particular focus on its impact on academic and policy-oriented research. A central gap in the literature is identified in the limited scholarly interrogation of how routine demographic variables, such as age, gender, marital status, religious affiliation, and number of children, interact with statutory definitions of personal and sensitive personal data within the Jamaican legal context. Using doctrinal legal analysis and a synthesis of scholarly privacy literature, the study evaluates whether such variables constitute breaches under the Act and under what conditions. Findings indicate that while most demographic variables are classified as personal data, only specific categories, particularly religious affiliation, fall under sensitive personal data requiring heightened protection. The legality of processing these variables depends not on their mere collection but on adherence to core principles such as lawful processing, data minimisation, and informed consent. For researchers, the Act introduces significant ethical and procedural obligations, including anonymisation, purpose limitation, and institutional accountability. The study contributes to Caribbean data governance scholarship by clarifying ambiguities surrounding demographic data usage and proposing a framework for compliant research practice. It concludes that responsible data handling, rather than categorical exclusion of variables, is essential for lawful and ethical research under the Act.

Keywords: Data Protection Act, Jamaica, research ethics, personal data, sensitive data, privacy law.

Introduction

The Data Protection Act (Data Protection Act; Jamaica House of Parliament, 2020) establishes a comprehensive legal framework governing the collection, processing, and storage of personal

data in Jamaica, reflecting a global shift toward privacy protection and digital accountability (Organisation for Economic Co-operation and Development, 2013; United Nations, 2018; Greenleaf, 2023). The Act is modelled significantly on international standards, particularly the General Data Protection Regulation, thereby embedding principles such as fairness, transparency, and accountability into Jamaican law (Bennett, 2018; Voigt & Von dem Bussche, 2017; Myers & Fletcher, 2026; DunnCox, n.d.-a, n.d.-b, n.d.-c). Despite its importance, there remains a paucity of empirical and theoretical scholarship examining how the Act affects academic research, particularly within Caribbean contexts. Existing discussions focus largely on business compliance and regulatory obligations rather than research methodologies or ethical implications (Altman et al., 2018; Carey, 2018; Custers et al., 2018). This creates a critical gap in understanding how researchers can lawfully use individual-level data in social science and public health studies (Israel, 2015; Altman et al., 2018). The absence of such analysis is particularly concerning given the increasing reliance on microdata in Jamaican research (Boyd & Crawford, 2012; Lane et al., 2014). Consequently, this study seeks to bridge that gap by providing a structured academic assessment of the Act's implications for research. It also clarifies ambiguities surrounding common demographic variables frequently used in scholarly inquiry.

A particularly underexplored issue is whether standard demographic variables, such as age, gender, marital status, religious affiliation, and number of children, constitute breaches of the Act when collected or analysed. Many researchers operate under implicit assumptions that such variables are harmless or exempt from strict regulation, yet the Act defines personal data broadly as any information capable of identifying an individual (Myers & Fletcher, 2026; Purtova, 2018). This expansive definition raises critical questions about the legality of even routine survey instruments (Ohm, 2010; Rocher et al., 2019). Furthermore, the distinction between personal data and sensitive personal data introduces varying thresholds of protection that are not always well understood in academic practice (Bygrave, 2014; González Fuster, 2014). Religious affiliation, for instance, is explicitly categorised as sensitive personal data, while other variables are not. However, when combined, seemingly innocuous variables may enable identification, thereby increasing legal risk (Samarati & Sweeney, 1998; El Emam & Arbuckle, 2013). The literature has not adequately addressed these nuances in the Jamaican setting. This study, therefore, interrogates these classifications systematically.

The relevance of this inquiry is heightened by the growing digitisation of research data and the increasing use of administrative and longitudinal datasets in Jamaica (Marelli et al., 2020; Metcalf & Crawford, 2016). Researchers frequently collect large volumes of personal data, often without fully appreciating the legal obligations imposed by data protection laws (Solove, 2013; Nissenbaum, 2010). The Act mandates lawful and fair processing, purpose limitation, and data minimisation, all of which directly affect research design (Office of the Information Commissioner, 2024; Cavoukian, 2012). These requirements necessitate a re-evaluation of traditional data collection practices. Moreover, non-compliance may expose researchers and institutions to legal penalties and reputational harm (Rubinstein, 2013; Zarsky, 2016). This underscores the need for a clear and context-specific interpretation of the Act for research purposes. The study responds to this need by offering doctrinal clarity and applied guidance.

Ultimately, this research contributes to both legal scholarship and methodological discourse by integrating statutory analysis with research ethics (Warren & Brandeis, 1890; World Medical Association, 2013). It advances the argument that compliance with the Act is not merely a legal obligation but also an ethical imperative aligned with respect for persons and confidentiality. By addressing the gap in the literature, the study provides a foundation for future empirical research on data governance in Jamaica. It also supports institutional review boards and policymakers in developing clearer guidelines for researchers. The findings have implications beyond Jamaica, particularly for other Caribbean jurisdictions adopting similar legislation (Taylor et al., 2017). The study, therefore, represents a timely and necessary intervention in the evolving field of data protection and research ethics.

Methods: PRISMA Approach to Reviewing Data Protection and Research Implications

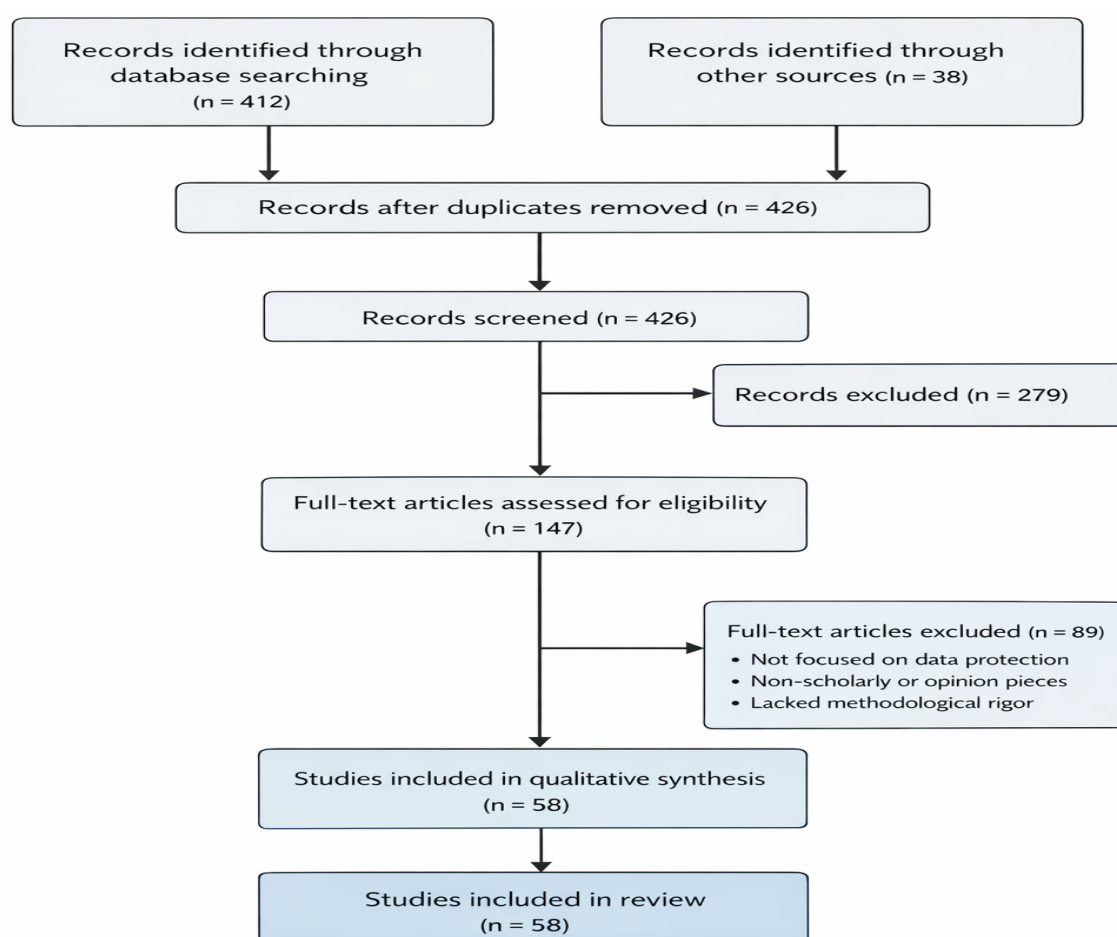
This study employed the PRISMA Statement as a structured methodological framework to systematically identify, screen, and synthesise relevant literature on data protection laws and their implications for research. PRISMA is widely recognised as a gold standard for enhancing transparency and reproducibility in systematic reviews (Page et al., 2021; Yin, 2018). The adoption of this framework ensures that the selection of studies is both comprehensive and methodologically sound. Given the interdisciplinary nature of data protection, the review incorporated legal, ethical, and empirical research sources (Dove et al., 2014; Hansen & Kindt, 2013). The approach was particularly suitable for identifying how demographic variables are treated under privacy legislation. It also allowed for the integration of statutory analysis with peer-reviewed scholarship. The use of PRISMA therefore strengthens the credibility and replicability of the study.

The literature search was conducted across multiple academic databases, including PubMed, Scopus, Web of Science, JSTOR, and Google Scholar, to ensure broad coverage of relevant studies. Search terms included combinations of keywords such as “data protection,” “privacy law,” “research ethics,” “personal data,” “sensitive data,” and “Jamaica Data Protection Act.” Boolean operators were used to refine search results and improve precision. Inclusion criteria were limited to peer-reviewed journal articles, legal analyses, and official policy documents published between 2000 and 2025. Studies were required to address data protection, privacy law, or research ethics in a manner applicable to the Jamaican or comparable international context. Exclusion criteria included non-scholarly sources, opinion pieces, and studies lacking methodological transparency. The search process yielded an initial pool of studies that were subsequently screened for relevance. This systematic approach ensured that only high-quality and pertinent sources were included.

The screening process followed the PRISMA flow model, beginning with the removal of duplicate records and proceeding to title and abstract screening. Studies that met the initial criteria were subjected to full-text review to assess their relevance and methodological quality. A standardised data extraction form was used to collect key information, including study objectives, methodology, legal context, and findings related to data protection and research practices. Particular attention was given to how demographic variables were classified and

regulated within each study. The quality of included studies was assessed using established appraisal tools appropriate for legal and social science research (Page et al., 2021). Discrepancies in study selection were resolved through critical evaluation and consensus. This rigorous screening process ensured the reliability of the evidence base. It also minimised bias in the selection of studies.

The final synthesis involved a narrative and thematic analysis of the selected studies, focusing on key themes such as definitions of personal and sensitive data, legal obligations for researchers, and ethical considerations in data handling. The Data Protection Act (Jamaica, 2020) was analysed doctrinally and integrated with the findings from the systematic review. This dual approach allowed for a comprehensive understanding of both the legal framework and its practical implications. Thematic categories were developed inductively and refined iteratively to ensure analytical coherence. The findings were then synthesised to address the research questions and identified gap in the literature. Limitations of the review process, including potential publication bias and jurisdictional differences, were acknowledged. The PRISMA framework thus facilitated a transparent and robust methodological approach. It ensured that the study's conclusions are grounded in a systematic and reproducible evidence base.



PRISMA Flow Diagram of Study Selection

Figure 1: PRISMA Flow Diagram of Study Selection

Conceptual and Legal Framework of the Act

The Data Protection Act defines personal data as any information relating to an identifiable individual, whether directly or indirectly identifiable. This broad definition includes demographic variables such as age, gender, and marital status, particularly when combined with other identifiers (Myers & Fletcher, 2026; Purtova, 2018). The Act also distinguishes sensitive personal data, which includes religious beliefs, political opinions, health status, and biometric data, requiring enhanced safeguards (Bygrave, 2014; González Fuster, 2014). This distinction is critical for researchers, as it determines the level of legal protection required. Sensitive data processing typically necessitates explicit consent or a strong legal basis (Voigt & Von dem Bussche, 2017; Carey, 2018). The Act therefore introduces a tiered system of data governance. Understanding this distinction is essential for lawful research practice. It also aligns Jamaica with international privacy standards (Organisation for Economic Co-operation and Development, 2013; United Nations, 2018; Greenleaf, 2023).

The Act is underpinned by core data protection principles, including lawful processing, purpose limitation, data minimisation, accuracy, storage limitation, and security safeguards (DataPro Consulting, 2025; Information Commissioner's Office, 2018). These principles collectively ensure that personal data is handled responsibly and ethically (Cavoukian, 2012; Kuner, 2007). For researchers, the principle of data minimisation is particularly significant, as it requires collecting only data that is necessary for the research objective (Altman et al., 2018; Israel, 2015). This challenges traditional practices of extensive data collection for exploratory purposes (Boyd & Crawford, 2012). Additionally, the principle of purpose limitation restricts the use of data to the specific purpose for which it was collected, meaning that secondary analysis without consent may constitute a breach (Marelli et al., 2020; Rubinstein, 2013). These principles impose a disciplined approach to research design. They also reinforce accountability in data handling (Solove, 2013).

The Act also establishes rights for data subjects, including the right to access, rectify, and erase their data (Office of the Information Commissioner, 2024). These rights empower individuals and introduce new obligations for researchers as data controllers (Nissenbaum, 2010; Regan, 2013). Researchers must be prepared to respond to data access requests and ensure data accuracy. The right to erasure poses challenges for longitudinal studies where data retention is essential (Kaye et al., 2015). However, exemptions may apply where data is used for statistical or research purposes under strict safeguards (Dove et al., 2014; Hansen & Kindt, 2013). This creates a balance between individual rights and scientific advancement. Researchers must navigate these rights carefully. Institutional policies play a critical role in ensuring compliance (University of Oxford, n.d.; University of the West Indies, 2021).

Furthermore, the Act applies extraterritorially in certain cases, meaning that researchers outside Jamaica processing data of Jamaican residents may also be subject to its provisions (Voigt & Von dem Bussche, 2017; Greenleaf, 2023). This has implications for international collaborations and data sharing agreements (Lane et al., 2014). Institutions must ensure that partners adhere to equivalent data protection standards. The requirement for data protection officers and registration of data controllers further institutionalises compliance (Myers & Fletcher, 2026; Carey, 2018).

These provisions highlight the systemic nature of data protection obligations. For researchers, compliance is no longer optional but embedded in the legal framework. This reinforces the importance of integrating legal knowledge into research training and practice (Israel, 2015).

Implications for Researchers

The Data Protection Act (Jamaica, 2020) fundamentally reshapes research practice by imposing legal obligations on the collection and processing of personal data. Researchers are classified as data controllers when they determine the purpose and means of processing data (Voigt & Von dem Bussche, 2017). This classification carries responsibilities such as ensuring lawful processing and implementing appropriate safeguards (Carey, 2018; Kuner, 2007). Ethical approval alone is no longer sufficient; legal compliance is also required (Israel, 2015). Researchers must therefore integrate data protection considerations into study design from the outset. This includes developing data management plans and obtaining informed consent (World Medical Association, 2013; University of Oxford, n.d.). Failure to do so may result in legal liability (Rubinstein, 2013).

One of the most significant implications is the requirement for informed and explicit consent, particularly when processing sensitive personal data. Consent must be freely given, specific, informed, and unambiguous (Office of the Information Commissioner, 2024; Solove, 2013). This raises challenges in large-scale surveys and secondary data analysis where obtaining consent may be difficult (Metcalf & Crawford, 2016). Researchers must also clearly communicate the purpose of data collection and any potential data sharing (Nissenbaum, 2010). Transparency is therefore a central requirement. Additionally, consent can be withdrawn, requiring researchers to cease processing unless another legal basis exists (Voigt & Von dem Bussche, 2017). This introduces complexities in ongoing studies. Robust consent mechanisms are therefore essential (Kaye et al., 2015).

Another key implication is the requirement for anonymisation or pseudonymisation of data wherever possible. Fully anonymised data falls outside the scope of the Act, making it a preferred approach for researchers (El Emam & Arbuckle, 2013; Ohm, 2010). However, achieving true anonymisation can be challenging, particularly with detailed datasets (Rocher et al., 2019). The risk of re-identification increases when multiple variables are combined (Samarati & Sweeney, 1998). Researchers must therefore implement technical safeguards such as encryption and restricted access (Heurix et al., 2015). Data security becomes a critical component of research methodology. Institutions must provide the necessary infrastructure. This represents a shift toward more technologically informed research practices (Custers et al., 2018).

Finally, the Act emphasises accountability and documentation, requiring researchers to demonstrate compliance with data protection principles (Accountability principle: Cavoukian, 2012; Gellert, 2016). This includes maintaining records of processing activities and conducting data protection impact assessments where necessary (Voigt & Von dem Bussche, 2017). These requirements increase the administrative burden on researchers. However, they also enhance transparency and trust in research processes (Richards & King, 2014). Compliance may also improve the quality and credibility of research findings. Funding agencies and journals are

increasingly prioritising ethical and legal compliance (Taylor et al., 2017). The Act, therefore, aligns Jamaican research with global best practices. It represents both a challenge and an opportunity for the research community.

Do Demographic Variables Breach the Act?

The collection of age, gender, marital status, and number of children does not inherently breach the Data Protection Act (Jamaica, 2020), as these variables are classified as personal data rather than sensitive personal data. Personal data is broadly defined as any information that can identify an individual, either directly or indirectly (Myers & Fletcher, 2026; Purtova, 2018). Therefore, these variables are lawful to collect provided that the principles of lawful processing, necessity, and proportionality are satisfied (Kuner, 2007; Carey, 2018). However, the combination of these variables may increase the risk of identification (Ohm, 2010; Rocher et al., 2019). This is particularly relevant in small samples or geographically specific studies (El Emam & Arbuckle, 2013). Researchers must therefore assess the identifiability of their datasets. Compliance depends on context rather than the variables themselves.

Religious affiliation, however, is explicitly classified as sensitive personal data under the Act and requires heightened protection (Myers & Fletcher, 2026; Bygrave, 2014). The processing of such data typically requires explicit consent and a clear legal basis (Voigt & Von dem Bussche, 2017). Collecting religious information without adequate justification or safeguards may constitute a breach. Researchers must therefore carefully justify the inclusion of such variables in their studies (Israel, 2015). Ethical approval alone is insufficient without legal compliance. Additional safeguards such as anonymisation and restricted access are necessary (Heurix et al., 2015). This highlights the importance of distinguishing between types of personal data. It also underscores the need for careful research design.

Marital status and number of children, while not sensitive, may still pose risks when combined with other identifiers. For example, a dataset containing age, location, and family structure may enable re-identification of individuals (Samarati & Sweeney, 1998; Rocher et al., 2019). This would constitute a breach if appropriate safeguards are not in place. The principle of data minimisation requires that only necessary variables be collected (DunnCox, n.d.-a, n.d.-b, n.d.-c; Cavoukian, 2012). Researchers must therefore justify each variable in relation to their research objectives (Altman et al., 2018). Unnecessary data collection increases legal risk. This principle encourages more focused and efficient research designs. It also aligns with ethical standards of confidentiality.

Ultimately, a breach of the Act occurs not from the mere collection of demographic data but from unlawful processing, lack of consent, excessive data collection, or inadequate security measures (Solove, 2013; Rubinstein, 2013). Researchers must therefore adopt a holistic approach to compliance. This includes obtaining consent, minimising data, anonymising datasets, and ensuring security (Heurix et al., 2015; Custers et al., 2018). The Act does not prohibit the use of demographic variables but regulates how they are used. This distinction is critical for researchers. Proper compliance enables the continued use of valuable data in research while protecting individual privacy (Nissenbaum, 2010; Taylor et al., 2017).

Limitations of the Study

This study is not without limitations. First, the research relied primarily on a doctrinal legal analysis and a systematic review of existing literature rather than empirical data collected from researchers or institutions in Jamaica. As a result, the study does not provide direct evidence on how researchers are currently interpreting or implementing the Data Protection Act in practice. The reliance on secondary sources means that the findings are largely interpretive and theoretical rather than behavioural or institutional. While the PRISMA approach ensured a systematic and transparent review of the literature, the study may still be subject to publication bias, as it included primarily peer-reviewed articles, legal analyses, and official policy documents. Some relevant institutional reports, unpublished studies, or internal university guidelines may not have been captured in the review process (Page et al., 2021). Additionally, much of the data protection literature is based on European and North American contexts, which may not fully reflect the legal, institutional, and research environment in Jamaica (Marelli et al., 2020; Zarsky, 2016).

Second, the interpretation of the Data Protection Act was conducted from a research and academic perspective rather than through judicial interpretation or case law analysis, as there is currently limited case law in Jamaica interpreting the Act in relation to academic research. This means that some legal interpretations presented in this study may evolve as courts, regulators, and policymakers provide further guidance on the application of the law. Furthermore, the study focused primarily on demographic variables such as age, gender, marital status, religion, and number of children, and did not examine other types of personal data, such as genetic data, digital behavioural data, or geolocation data, which may present different legal and ethical challenges (Dove et al., 2014; Ohm, 2010). Future research should therefore include empirical studies involving researchers, ethics committees, and data protection officers in Jamaica to better understand how the Act is being implemented in practice and to identify the practical challenges faced by researchers in complying with data protection legislation.

Discussion

This study examined the implications of the Data Protection Act (Jamaica, 2020) for academic research, with particular emphasis on the classification and use of demographic variables. The findings indicate that the Act does not prohibit the use of demographic data in research; rather, it regulates the way such data are collected, processed, stored, and shared. This interpretation aligns with international data protection frameworks, which emphasise lawful processing, transparency, and accountability rather than outright restrictions on data use (Organisation for Economic Co-operation and Development, 2013; United Nations, 2018; Voigt & Von dem Bussche, 2017). The Jamaican legislation, therefore, reflects global norms in privacy governance and reinforces the principle that research and privacy protection are not mutually exclusive but must be balanced through appropriate safeguards (Greenleaf, 2023; Bennett, 2018; Medine & Murthy, 2020).

One of the key findings of this study is that demographic variables such as age, gender, marital status, and number of children are classified as personal data rather than sensitive personal data. However, the study also demonstrates that the combination of multiple demographic variables may increase the risk of re-identification, particularly in small samples or geographically specific

datasets. This finding is strongly supported in the data privacy literature, which shows that individuals can often be re-identified using only a few demographic variables (Samarati & Sweeney, 1998; Ohm, 2010; Rocher et al., 2019). The implication is that researchers must move beyond the assumption that demographic data are inherently anonymous. Instead, identifiability must be assessed within the context of each dataset and research design (El Emam & Arbuckle, 2013).

The study also found that religious affiliation constitutes sensitive personal data under the Act and therefore requires explicit consent and stronger safeguards. This classification is consistent with international privacy law, which treats information relating to religion, health, political opinions, and biometric data as sensitive due to the potential for discrimination or harm if disclosed (Bygrave, 2014; González Fuster, 2014). For researchers, this means that the inclusion of such variables must be clearly justified and supported by a lawful basis for processing. This finding reinforces the argument made in research ethics literature that the collection of sensitive data must be guided by necessity, proportionality, and respect for persons (Israel, 2015; World Medical Association, 2013).

Another important finding is that anonymisation and data minimisation are central to lawful research under the Act. The literature consistently shows that anonymisation is one of the most effective ways to protect privacy while enabling research (El Emam & Arbuckle, 2013). However, studies also demonstrate that complete anonymisation is difficult to achieve in the era of big data, where datasets can be linked and cross-referenced (Boyd & Crawford, 2012; Marelli et al., 2020). This creates what some scholars describe as the “re-identification risk,” where anonymised data can be traced back to individuals using auxiliary information (Ohm, 2010; Rocher et al., 2019). The implication for Jamaican researchers is that anonymisation must be combined with technical and organisational safeguards such as encryption, access controls, and data governance policies (Heurix et al., 2015; Custers et al., 2018).

The study further found that the Data Protection Act introduces significant administrative and legal responsibilities for researchers, including documentation, consent management, and data protection impact assessments. While these requirements may increase the administrative burden on researchers, they also improve transparency, accountability, and public trust in research processes (Solove, 2013; Richards & King, 2014; Altman et al., 2024). This is particularly important in public health and social science research, where studies often rely on sensitive personal data. Strong data governance frameworks can therefore enhance the credibility and ethical integrity of research (Nissenbaum, 2010; Taylor et al., 2017).

More broadly, this study highlights the need for greater institutional support and training in data protection for researchers in Jamaica. Many researchers are trained in research ethics but not in data protection law, yet the two are now closely interconnected. Modern research governance requires an integrated approach that combines legal compliance, ethical principles, and data security practices (University of Oxford, n.d.). Universities and research institutions, therefore, have a responsibility to develop clear data protection policies, provide training, and establish data governance frameworks to support researchers, and this is the rationale for their involvement in

writings on the matter (European University Institute, 2019; University College London, n.d). Without such institutional support, compliance may be inconsistent and legal risks may increase.

This study also contributes to the literature by addressing a gap in Caribbean research on data protection and research methodology. Much of the existing literature on GDPR and data protection focuses on Europe and North America, with limited discussion of Caribbean legal frameworks (Marelli et al., 2020; Zarsky, 2016). By providing a systematic analysis of the Jamaican context, this study contributes to the growing body of literature on global data protection and research ethics. The findings may also be relevant to other Caribbean countries that are developing or implementing similar data protection legislation.

Conclusion

This study examined the implications of the Data Protection Act (Jamaica, 2020) for academic research, with particular focus on whether the use of demographic variables constitutes a breach of the Act. The findings indicate that demographic variables such as age, gender, marital status, and number of children do not inherently breach the Act, as they are classified as personal data rather than sensitive personal data. However, the study also found that the combination of demographic variables may increase the risk of re-identification, particularly in small or specialised datasets. Compliance with the Act, therefore, depends not only on the type of data collected but also on how the data are processed, stored, and protected.

The study further concludes that religious affiliation is classified as sensitive personal data and therefore requires explicit consent and stronger safeguards. Researchers must therefore carefully justify the collection of such data and ensure that appropriate legal and ethical safeguards are in place. More broadly, the Act requires researchers to adopt new research practices, including data minimisation, anonymisation, informed consent, and data security measures. These requirements represent a shift from traditional research practices toward more structured data governance frameworks.

Importantly, the study concludes that the Data Protection Act does not prevent academic research but instead promotes responsible and ethical research practices. The Act reinforces principles that are already central to research ethics, including confidentiality, respect for persons, and responsible data management (World Medical Association, 2013; Israel, 2015; Solove, 2013). Compliance with the Act should therefore be viewed not as a barrier to research but as a framework for improving research quality, transparency, and public trust.

The study also highlights the need for clearer institutional guidelines and researcher training on data protection in Jamaica. Universities, ethics committees, and policymakers must play a more active role in guiding how the Act applies to research. This includes developing data management policies, consent templates, anonymisation guidelines, and data protection training programmes. Such measures would help researchers comply with the law while continuing to produce high-quality research.

Finally, this study contributes to the limited academic literature on data protection and research in the Caribbean. Future research should examine how researchers in Jamaica are adapting to the

Data Protection Act, the challenges they face in compliance, and the impact of the Act on research productivity and data access. Empirical studies in this area would provide valuable evidence for policymakers and academic institutions. As data-driven research continues to expand, understanding the relationship between data protection law and research methodology will become increasingly important.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *Science (New York, N.Y.)*, 347(6221), 509-514. <https://doi.org/10.1126/science.aaa1465>
- Altman, M., Cohen, A., & Nissim, K. (2024, July). *Data privacy protection* (TechBrief). Association for Computing Machinery. <https://micahaltman.com/publication/techbrief/2024/>
- Altman, M., Wood, A., O'Brien, D.R., & Gasser, U. (2018). Practical approaches to big data privacy over time, *International Data Privacy Law*, Volume 8, Issue 1, February 2018, Pages 29-51, <https://doi.org/10.1093/idpl/ix027>
- Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, Big Data, and the Public Good*, 44-75.
- Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalisation of privacy standards. *Information Polity*, 23(2), 239-246.
- Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, 15(5), 662-679.
- Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.
- Carey, P. (2018). *Data protection: A practical guide to UK and EU law*. Oxford University Press.
- Cavoukian, A. (2012). Privacy by design: Origins, meaning, and prospects. *Privacy Protection Measures and Technologies in Business Organizations*, 170-208.
- Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S. (2018). EU personal data protection in policy and practice. *Computer Law & Security Review*, 34(2), 226-235.
- DataPro Consulting. (2025). *Know your rights under Jamaica's Data Protection Act*. <https://dataprocaribbean.com/resources/know-your-rights/>
- Dove, E. S., Joly, Y., Tasse, A.-M., Committee, P. P. P. I. G. A. S. PG. I. S., Committee, I. C. G. C. E. A. P., & Knoppers, B. M. (2014). Genomic cloud computing: Legal and ethical points to consider. *European Journal of Human Genetics*, 23(10), 1271-1278. <https://doi.org/10.1038/ejhg.2014.196>
- DunnCox. (n.d.-a). *Understanding data protection standards: Part I*. <https://dunncox.com/articles/understanding-data-protection-standards-part-1/>
- DunnCox. (n.d.-b). *Understanding data protection standards: Part II*. <https://dunncox.com/articles/understanding-data-protection-standards-part-2/>
- DunnCox. (n.d.-c). *Understanding data protection standards: Part III*. <https://dunncox.com/articles/understanding-data-protection-standards-part-3/>

- El Emam, K., & Arbuckle, L. (2013). *Anonymizing health data: Case studies and methods to get you started*. O'Reilly Media.
- European University Institute. (2019). *Guide on good data protection practice in research* (3rd ed.). <https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf>
- Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, 27(1), 1-3. <https://doi.org/10.1007/s13347-014-0157-8>
- Gellert, R. (2016). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 32(5), 641-653.
- González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer.
- Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”. *AI Magazine*, 38(3), 50-57. DOI: <https://doi.org/10.1609/aimag.v38i3.2741>
- Greenleaf, G. (2023). Global Data Privacy Laws 2023: 162 National Laws and 20 Bills. *Privacy Laws and Business International Report*, 181, 2-4. <https://doi.org/10.2139/ssrn.4426146>
- Hansen, M., & Kindt, E. (2013). Privacy and data protection in biomedical research. *European Data Protection Law Review*, 2(1), 1-15.
- Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53, 1-17.
- Information Commissioner's Office. (2018). *Guide to the General Data Protection Regulation (GDPR)*.
- Israel, M. (2015). *Research ethics and integrity for social scientists*. Sage Publications.
- Jamaica House of Parliament. (2020). Data Protection Act, 2020 (Jamaica). <https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf>
- Kaye, J., et al. (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics*, 23(2), 141-146.
- Kuner, C. (2007). *European data protection law*. Oxford University Press.
- Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (2014). *Privacy, big data, and the public good*. Cambridge University Press.
- Marelli, L., Testa, G., & Van Hoyweghen, I. (2020). Big data research and GDPR. *BMJ*, 370, m2210.
- Medine, D., & Murthy, G. (2020). *Making data work for the poor: New approaches to data protection and privacy* (Focus Note). Consultative Group to Assist the Poor. https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf
- Metcalf, J., & Crawford, K. (2016). Where are human subjects in big data research? *Big Data & Society*, 3(1). <https://journals.sagepub.com/doi/10.1177/2053951716650211>

- Mittelstadt, B. D., & Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and engineering ethics*, 22(2), 303-341. <https://doi.org/10.1007/s11948-015-9652-2>
- Myers, Fletcher & Gordon. (2026). *Data protection FAQs and legal interpretations in Jamaica*.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Office of the Information Commissioner, Jamaica. (2023). *Guidance on the Data Protection Act*.
- Office of the Information Commissioner. (2024). *Data protection standards*. <https://oic.gov.jm/page/data-protection-standards>
- Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57, 1701-1777.
- Organisation for Economic Co-operation and Development (OECD). (2013). *OECD privacy framework*. https://www.afapdp.org/wp-content/uploads/2018/06/oecd_privacy_framework.pdf
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Purtova, N. (2018). The law of everything: Broad concept of personal data. *Law, Innovation and Technology*, 10(1), 40-81.
- Regan, P. M. (2013). *Legislating privacy: Technology, social values, and public policy*. University of North Carolina Press.
- Richards, N. M., & King, J. H. (2014). Big data ethics. *Wake Forest Law Review*, 49, 393-432.
- Rocher, L., Hendrickx, J. M., & De Montjoye, Y. A. (2019). Estimating the success of re-identifications. *Nature Communications*, 10, 3069.
- Rubinstein, I. S. (2013). Big data: The end of privacy? *International Data Privacy Law*, 3(2), 74-87.
- Samarati, P., & Sweeney, L. (1998). Protecting privacy when disclosing information. *Journal of Computer Security*, 1(1), 1-20.
- Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880-1903.
- Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
- Taylor, L., Floridi, L., & Van der Sloot, B. (2017). *Group privacy: New challenges of data technologies*. Springer.
- Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data. *Stanford Law Review Online*, 64, 63-69.
- Terry, N. P., & Francis, L. P. (2007). Ensuring the privacy and confidentiality of electronic health records. *University of Illinois Law Review*.
- United Nations. (2018). *Guidelines for the regulation of computerized personal data files*. <https://digitallibrary.un.org/record/43365?ln=en&v=pdf>

- University College London. (n.d.). *UCL GDPR data protection for researchers handbook* (PDF). UCL. https://www.ucl.ac.uk/data-protection/sites/data-protection/files/ucl_gdpr_data_protection_for_researchers_handbook.pdf
- University of Oxford. (n.d.). *Data Protection Policy*. <https://compliance.admin.ox.ac.uk/data-protection-policy>
- University of the West Indies. (2021). Resource: The UWI Data Protection Policy. <https://uwi.edu/data-protection/?q=policy>
- Van der Sloot, B. (2014). Privacy as personality right. *European Data Protection Law Review*.
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Volume 7, Issue 2, May 2017, Pages 76-99, <https://doi.org/10.1093/idpl/ix005>
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.
- World Medical Association. (2013). Declaration of Helsinki. *JAMA*, 310(20), 2191-2194.
- Yin, R. K. (2018). *Case study research and applications*. Sage Publications.
- Zarsky, T. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, 47, 995-1020.