

To the CEO,
Company X,
A Multi-national Corporation.

The Legal and Ethical Compliance for Data Division's Mandate in EU and Americas

Executive Summary

The most essential, yet contentious issue of the modern day is the legal and ethical practices around data. Following the rise of big tech and the emergence of big data tools such as analytical and behavior-altering algorithms, governments and organizations across the globe have become sensitive to both commercial and private use of data. This has led to the enactment of data protection laws, which are now in earnest in Europe in the US, and lately in South America. These laws define compliance and can be used either as a strength or a roadblock to an organization's operations in a given jurisdiction. In lieu of this, there is need for the organization's division on these matters to be conversant with all legal and ethical issues around data. This report captures the core elements of ethical data approaches, and underpins their significance, especially in compliance, and also as a mitigation against legal and ethical liabilities such as moral failures in perpetuating inequality or biases. This report shows that the division has to create measures consistent with The Purpose Paradigm, The Personal Protection of the Consumers as Human Subjects; Modes and Rules of Application of Data, and Concerns on the Use of Data with Other Parties, and the limits of application of data science and sustainable practices in preparing the organization in meeting its ethical and legal obligations.

Introduction

In the European Union, the regulation of personal data is protected by the General Data Protection Regulation (GDPR), which sets severe requirements for companies in terms of data gathering, processing, and storage (Kuner et al., 2020). It has provided businesses with new concepts such as the right to consent, the right to be forgotten, and the right to data portability. In the United States, the laws regulating modern data processing are fragmented, and the main legal act is the CCPA accompanied by numerous state laws. In addition to these general privacy regulations, business organizations face the question of the ethicality of their data usage. The issue of fairness is also a concern and increasingly attention is being paid to how the AI system may be biased against protected categories. This concern links up with legal instruments like the Fair Credit Reporting Act in the United States and the proposed AI Act in European Union that seeks to uphold both fairness and explainability in the process of decision-making by artificial intelligence. Further, data localization requirements add another level of constraint to the analysis as companies must think not only about what information they store, but how and where it is stored as well. The processes of cross-border data transfers are rather complex especially the one occurring between the EU and the US where certain legal frameworks have to be followed (Kuner et al., 2020).

Owing to the rise in international laws and regulations on data practices, and the new models of operations, this report seeks to establish the rules and guidelines for the data division in compliance with the current legal and ethical concerns. As the area of jurisdiction is the Americas and in the short term the European Union, due diligence is put to establish guidelines that fit the two regions. The report considers the following issues to be the most essential in data laws and ethics: The Purpose Paradigm, The Personal Protection of the Consumers as Human Subjects; Modes and Rules of Application of Data, and Concerns on

the Use of Data with Other Parties, and the limits of application of data science and sustainable practices.

On the Purpose Paradigm

To attune the division to the purpose paradigm, the division stands advised that there should be rules on the range of data use, and the technical applications of data. Some of the core uses of data are for market operations such as e-commerce, and electronic money transfers and for market identification as applies in the case of social media services. Thus, as per the purpose paradigm, the data provided by the users should not exceed the purpose for which the necessity to yield the data is required. Therefore, any details that are unnecessary for the data usage – as those that mayacerbate inequality or targeting of the people based on sensitive issues such as race, and religion should not be collected. For every good usage of the data points, there is potential questionable usage of the data (Martin 2015; Martin, 2019). Therefore the division must care to minimize the possibility for questionable data usage by collecting only the needed data. This is done by creating a justification or matching table clause for data collection methods, and a necessity in a given target market population.

The Personal Protection of Humans and Users as Human Subjects

The concept of human subjects is guided by ethical guidelines that regard that all persons should be informed of the uses of their data, and the business bears the responsibility to inform the people. The division has the task of enacting laws that protect user safety by protecting their identity, as well as ensuring that all laws and procedures in data acquisition are followed. The essence of this model is to ensure that there are no violations made against the individual or any acquisition of data illegally (Martin, 2015). The European and the US data laws put liability on the companies and organizations acquiring data from the users to ensure that there is compliance with data protection laws. The division as such has the task of enacting the user laws, and data disclosure laws that the users are to surrender their data voluntarily and the purpose for which their data will be used. In addition, as the company has the liability of ensuring that the consumers or users understand the data laws, they are tasked with simplification of the data laws/ compliance to a language that the ordinary citizen can relate and understand (Martin, 2020). This is essential in ensuring that there are no violations of the users, or taking advantage of the users as established across the EU data regulation laws, and the US data compliance laws on social media usage.

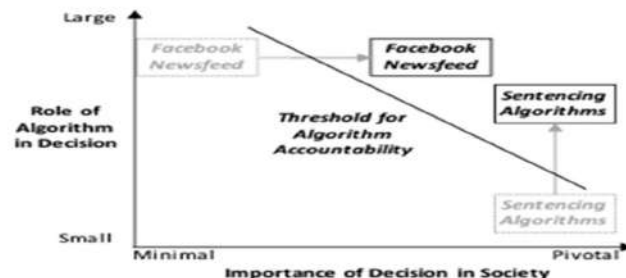
The division shall hence be expected to enact the methods and procedures of ethical and legal adherence to data-gathering methods. The core models task the organization to first inform the individuals that their data will be used, and also the extent to which their data will be used. There are also protected groups whose data cannot be gathered online, without the guardians or parental approval. This is useful in creating legal identities and protecting human subjects. There are also laws concerning the limitations of the questions that the individual can disclose – for example, the information on the person's private data or sensitive information once disclosed is at the liability of the organization. Thus, division has the task of creating means of protecting the human subject by protecting their data against leakage, or third-party access. This necessity is put in place to secure the individual against damages such as theft or fraud that may occur if the individual due to the data handed to the organization. In order to protect the human subject the division has to create cyber security measures aimed at mitigating incidences of data theft either by hacking, sharing or physical intrusion to the company computers. Further, as regards to the protection of the human subject, the division has to comply with surveillance laws and thereby set laws that guide against phishing or any other acts that target the user data.

The Modes and Rules of Application of Data

There are ethical aspects of the range of applications surrounding the use of algorithmic designs, and consequently the uses of data. With the rise in concerns about the ethical usage of algorithms to protect users from manipulation, the division is advised that it must set internal rules on its operations and practices. The usage and application of its platforms or any products must set certain limitations to ensure that there is no indirect manipulation of the people. The use of algorithms and data in the 2016 US elections serves as a warning sign that unless the organization takes proactive measures to build the guardrails against external party manipulation or intrusive practices such as data mining, there will be a violation of big data usage.

The division should be aware of concerns about the use of algorithms as established by Kirsten Martin, a professor at the George Washington University School of Business, who noted that indolence does not account for excludability in the design of algorithms (Martin, 2019). Thus, the primary issue in the development and design of algorithms in this division must pay attention to ensuring that the possibility of mistakes is diminished. This is done through internal controls and reviews of the implications of the algorithms from multiple points. As such, the division has the responsibility of reviewing the algorithms based on analysis of multiple results and behavioral patterns that are emergent, if it cannot be solved at the very beginning during the design process. The significance of this approach is to eliminate the possibility of indolence or negligence, as there is notable results that as algorithms are non-thinking things based on reinforcing patterns, there is a likelihood of inequalities being reinforced unless an intervention is made.

Threshold Model for Algorithm Accountability



The graph shows the levels of liability that the division should bear toward fulfilling the algorithmic accountability.

Otherwise, the likely consequence of negligence in checking and correcting the moral foundations of the data and its patterns is the unintended yet woeful consequence of increasing inequalities and perpetuating biases. For example, when biased data is used based on racial profiling, it may lead to discriminatory outcomes where negative beliefs about a given racial group are advanced. This has a core repercussion as it affects entire social economic models as machine learning and AI are now part of the hiring, lending, and law enforcement process. Therefore, if they get it wrong, it is unimaginable the extent and scope of the wrong done to the people. In so doing lives and destinies of people are affected – this shows the necessity for the data division to consider the use of data and to establish internal systems of reviewing data mining models and their external outcomes, and clean any of the weaknesses that may be within it, if weaknesses be found (Martin, 2015; Martin, 2019). Therefore, as the custodians of a bold new feature, the organization through this division has to take the moral responsibility of establishing critical pathways of detecting biases, and eliminating them.

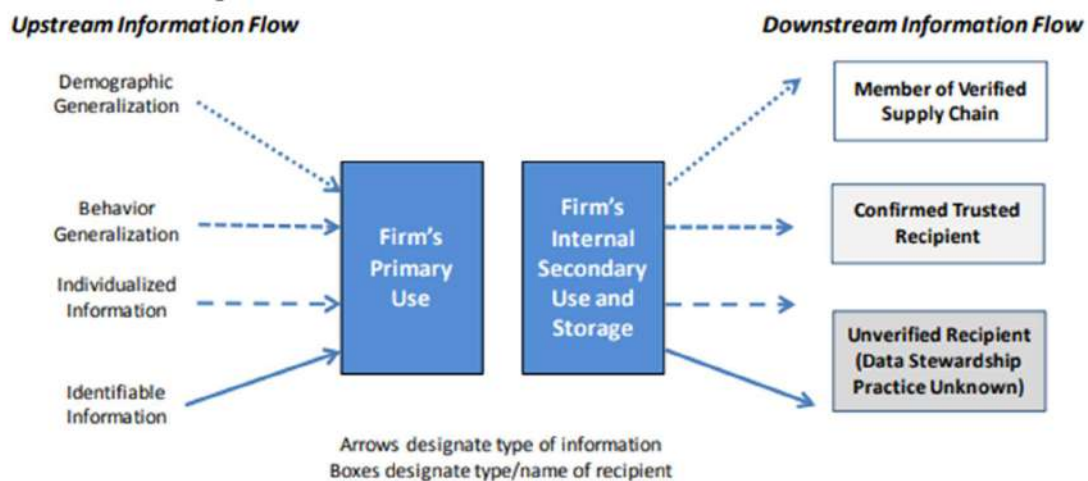
Mistake\ Context	False positive: Incorrectly include in a category	False negative: Incorrectly exclude from a category	Process Mistake: What factors drive the algorithmic decision? How is data gathered and used?
Manufacturing	Shipping a product as finished when it is actually defective	Rejecting a perfectly good product as defective	Deciding to ship a product only because it will help hit sales targets
Contacts and Friends	Identifying someone as a friend who is not	Not listing a friend (who may be a great fit)	Identifying friends based on individuals attending AA meetings
Political/ Advertising	Placing the wrong ad	Not placing the right ad	Targeting ads based on a medical condition; Google following users to see if advertising works
Social Services/ Public Goods	Family is given access to food stamps or Medicaid when they do not qualify	Family services program failing to flag toddlers who are in danger	Considering race when determining how to allocate police in a city
Judicial	Incorrectly labeling someone as a future criminal	Labeling someone as not a future criminal when they are	Considering a defendant's father's criminal history in categorizing risk of re-offending
Housing	Approving housing application for someone who doesn't qualify	Denying someone housing who does qualify	Placing a housing-related Facebook ad that excludes blacks, Asians, and Hispanics
Employment	Promoting the wrong person	Rejecting a good candidate	Considering a candidate's marital status
Location	Categorizing someone as at home when they are not	Deciding someone is not at a store when they are	Strava's heatmap software identifying U.S. military bases overseas

Types of Mistakes in Algorithmic Decisions

The table illustrates the impact of algorithmic decisions, and how they can perpetuate biases.

Concerns on the Use of Data with Other Parties

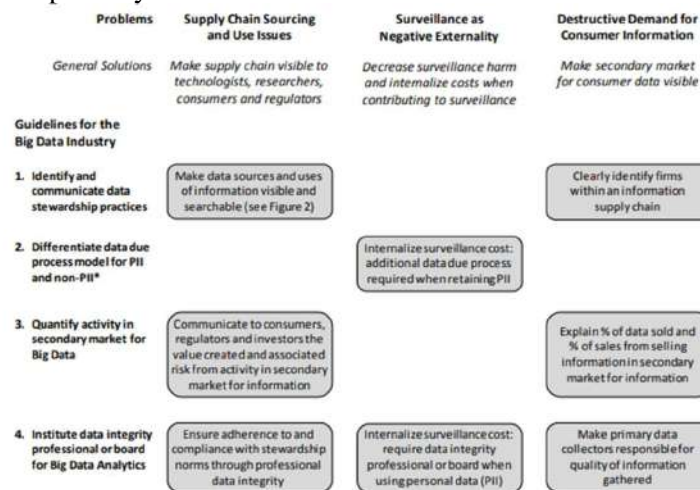
It is established that the company bears the liability of protecting the user data, and establishing protection on the user data across the data supply chain. The data supply chain cascades between the internal specific usage of data and the internal general use of the data. The division as such as the legal liability of establishing protocols on the nature of filing and data storage techniques, and data sharing protocols within the organization. For example, there are categories of various data, and there is also the data sensitivity index based on the personal identity details of the data (Martin, 2015). In view of this the division has to ensure that the data shared across the departments is only to the relevance of the divisions, and issues around user private data are secured.



Firm's Information Supply Chain Diagrams

Limits of application of data science and Sustainability Practices

There are limits to the extent of legal or ethical guards that can be allayed, but if per adventure there are new changes in the laws and standards, the core moral and ethical foundations of practice are instilled among the employees of the division, it can be anticipated that no matter what the future holds, the organization will remain adaptable to the US, European and global standards. These include the adoption of ‘Guidelines for Sustainable Big Data Industry’; which establishes a sustainable framework for a good operational model in big data (Martin, 2015). Among the core concerns that the division must put in place is data stewardship practices vis-a-vis clear communication of the use of the data to the people. The second principle to adapt a system that advances the distinction of personal identifiable data (PII), and non-personal identifiable data (none—PII). The third principle is to quantify identity in the secondary market for the big data (Martin, 2015). This is done by disclosing the percentage of information or data shared with third parties. The fourth principle that the division should adapt is to institute data integrity professional board dedicated to practices of Big Data analytics which oversees compliance as well as sets new rules for internal adaption by the division.



Guidelines for Big Data Industry Sustainability

This table shows the summative practices that the division should adapt in line with mitigating against unknown factors.

Summative Views on Legal Compliance Measures

In adherence with these views; the division should, therefore, act in compliance with the following legal issues:

- (i) Act in full compliance with the EU data doctrine, especially regarding all operations that are in the European countries, as the EU data laws are significantly different from the US and American laws.
- (ii) When operating in the Americas, there should be clear legal compliance with the existing data laws of each jurisdiction – noting that South America and North America are distinct data jurisdictions. For good standing on the laws, the US senate and congressional reports, especially on emergent issues, as regards the Tech space should be adhered to.
- (iii) For operations in Latin/South America, there should be adherence to universal laws of data operations, and also the existing country specific laws. For instance in Jamaica, due diligence has to be put to follow laws formulated under “the AN ACT to Protect the privacy of certain data and for connected matters.” Of specific

attention is the protection of minorities, including children, on data decisions, and seeking to act in lieu of prior protection of their privacy, and interests as they are a vulnerable group and are classified as a special group (The Data Protection Act, 2020, 2020). Also, special probity should be given to anti-fraud and anti-misuse of data acquisition to ensure that there is no excesses that contravenes the data laws. Given that this is an international organization, and the peoples of these nations are wary of any theft of data, as anticipated in Article 31 of the same bill, against the use of data from Jamaica with foreign governments unless there exists assurance, the division has to seek the assurance of the government of Jamaica on this matter.

As a matter of urgency, and show of confidence, and adherence to all core issues of data standards and compliance, the division should establish the following practices:

- (i) To teach the locals and engage them on the various uses of their data, during the onboarding process.
- (ii) Inform the people of any controversial issues, and consistently advise the users on their rights and options.
- (iii) Assure the clients of the sensitive issues that they can waive their identity on, or can, in the event of being uncertain or uncomfortable with sharing personal data to skip or write NA.
- (iv) To inform the users of their right to anonymity in the event they seek to use the service and feel it is best they remain anonymous, if that option applies.
- (v) To advise the organization of the various practices that infer to products development models that create equality, and restrain against any practices that contravene basic human standards and rights.

References

- Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). *The EU general data protection regulation: a commentary*. Oxford University Press. Available at: <https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826491>.
- Martin, K. (2015). Ethical Issues in the Big Data Industry. (2015). *MIS Quarterly Executive*, 14(2), 67-85.
- Martin, K. (2019). Designing Ethical Algorithms. *MIS Quarterly Executive*, 18(2), 129-141. <https://doi.org/10.17705/2msqe.00012>
- Martin, Kirsten E. "Ethical issues in the big data industry." In *Strategic Information Management*, pp. 450-471. Routledge, 2020.
- The Data Protection Act, 2020. (2020). Government Publication.