KB LAW SCHOLARS JOURNAL

https://orcid.org/0009-0004-7341-0868

No. 2 The Laurels Dun An Oir Kanturk Co. Cork Republic of Ireland
Greenbelt Rd Lanham Md. 20706, Maryland, US

www.growkudos.com

KBLSP Journal

ISSN 3027-2440 (online/Print) (2024) Volume 1 Issue Number 4 (June)

Google Analytics Google Scholar ResearchGate.net

EXAMINING THE EFFECTIVENESS AND APPLICATION OF DATA PROTECTION MODELS IN CONTEMPORARY CONTEXT

***Aghogho Kwame-Okpu** [PhD, B.L] <**akwameokpu@gmail.com**> <https://orcid.org/0009-0000-1028-6688>

Abstract

The choice of data protection model is important for policymakers, regulators, and organizations seeking to strike a balance between innovation, consumer trust, and data protection, especially in an era characterized by rapid technological advancements and growing concerns over privacy infringement. The paper considered the four primary models of data protection: the comprehensive model, sectorial model, self-regulatory model, and co-regulatory model. This paper therefore, is a comparative analysis of the different models of data protection. The paper considered the strengths, weaknesses, and suitability of the different models in addressing the threats posed to personal data. This was achieved by evaluating the effectiveness of these models in safeguarding personal data, promoting transparency, and fostering accountability among data controllers and processors. Against this background, the author highlighted the factors influencing the choice and implementation of data protection models, considering variables such as history, technological infrastructure, and economic considerations. By explaining the interplay between regulatory frameworks and real-world applications, the paper offers valuable insights into the adaptability and scalability of different data protection models across various sectors and regions. Based on comparative approach, it is maintained the need to inform policymakers, regulators, and stakeholders about the strength and weaknesses of different data protection models as well as the introduction of hybrid model acting as a platform in making informed decisions in designing and implementing data protection frameworks.

Keywords: data protection, privacy, personal data, data privacy, primary models

1. Introduction

In the latter part of the twentieth century, advancements in information and communication technology resulted in the invention of systems that could collect, store, and process personal data, which is essentially any information that can be used to identify an individual.[1]

[1] Mark Burdon, *Digital Data Collection and Information Privacy Law* (Cambridge University Press 2020) 161

Concerns that these technologies would lead to privacy violations led to the emergence of data protection. Data protection regulates the collection, control, processing and storing of personal data. It also provides penalties and remedies if personal data is collected or processed in a way that is contrary to regulations.[2]

Although an offshoot of the right to privacy with considerable overlaps, data protection diverges from the right to privacy which in a strict sense is oriented towards protecting the home, family life, and correspondence from intrusion.[3] For example, recording personal information without doing anything further cannot be considered an intrusion into personal space. However, this activity involves collecting personal data and is within the ambit of data protection.[4] It should be noted that data protection address the intricacies of privacy issues raised by ttechnological developments, which were beyond the contemplation of early privacy protection laws as contained in pre-existing rules and provisions on privacy.[5] Data protection also regulates the legal ability of an individual to determine what personal data in an ICT system can be shared with third parties.[6] Furthermore, data protection is used as a phrase to designate the laws which protect personal data.[7]

As the concept of data protection began to spread and as people began to demand protection for their personal data, countries and sometimes data controllers and processors across the world began taking steps to protect the personal data of individuals referred to as data subjects. This has resulted in the adoption of different models of data protection.[8] These

[2] J. Van den Hoven and others, 'Privacy and Information Technology' in Edward N. Zalta (ed.), *The Stanford Encyclopaedia of Philosophy* (Stanford University 2020) 5; S Sharma, *Data privacy and GDPR handbook* (John Wiley & Sons 2019) 29-31

[3] Gloria González Fuster, *The Emergence Of Personal Data Protection As A Fundamental Right Of The EU* (Vol. 16 Springer Science & Business 2014) 22; Raphael Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection', *Computer Law and Security Review*, (2013) (29) (5) 522 <https://works.bepress.com/serge_gutwirth/107/> accessed 1 June 2024; Jan Holvast, 'History of Privacy' in V. Matyáš, *et al* (ed.), *The Future of Identity* (Springer 2009)

[4] Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (PhD Thesis, Faculty of Law University of Pretoria 2016) <https://repository.up.ac.za/bitstream/handle/2263/53129/Abdulrauf_Legal_2016.pdf?sequence=1> accessed 31 May 2024

[5] Orla Lynskey., *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 90; Adrienn Lukacs.' What Is Privacy? The History and Definition of Privacy' (2016) <https://core.ac.uk/reader/80769180> accessed 17 May 2024

[6] Privacy International, 'A Guide for Policy Engagement on Data Protection Part 1: Data Protection, Explained' <https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf> accessed 31 May 2024

[7] Ibid. However, it is important to note that while the phrase 'data protection' is popular due to European influence, personal data protection has also developed in the United States of America under the nomenclature of information privacy.

[8] Ibid. But see Patricia Boshe, *Data Protection Legal Reforms in Africa* (Doctoral dissertation, Universität Passau 2017) <https://opus4.kobv.de/opus4-uni-passau/files/514/Data+Protection+Legal+Reforms+in+Africa.pdf> accessed 23 May 2024

models which differ in application and scope provide varying degrees of protection ranging from comprehensive to sectoral.[9]

This paper is divided into four sections; the first houses the introduction and provides a general overview of the concept of data protection and the emergence of data protection methods. The second gives a brief overview of the different models of data protection and highlights the use of privacy enhancing technologies. The third, discusses these models of data protection alongside their strengths and weaknesses while citing examples of jurisdictions where they are utilized. The paper concludes by reiterating the differences between these different models while recommending a hybrid model that allows for flexibility and adaptability to different sectors and regulatory needs.

2. Overview of the Different Models and Types of Data Protection

Across the world, different models are utilised to regulate the collection, control, processing and protection of personal data. The use of comprehensive laws is the popular model for data protection, though some jurisdictions however prefer to utilize sectoral laws. Data controllers and processors have also established codes of practice to provide for data protection.[10] In light of this, there are four major models for data protection, namely:

a. The Comprehensive Model
b. The Sectoral Model
c. The Self-Regulatory Model; and
d. The Co-Regulatory Model

Data subjects,[11] data controllers and processors with the use of Privacy-Enhancing Technologies[12] also resort to technological options to protect personal data.[13] The use of PETs often with a focus on encryption and/or anonymity allows the deployment of a range of programs and systems that ensure varying degrees of privacy and personal data protection in

[9] Michelle Frasher 'Adequacy versus equivalency: Financial data protection and the U.S.–EU divide' (2013) (56) (6) Business Horizons 787; Russell L Weaver, 'Privacy: The Trans-Atlantic Divide' (2019) (89) (4) Mississippi Law Journal 593, 618

[10] Shawn Marie Boyne, 'Data Protection in the United States' (2018) (66) (1) The American Journal of Comparative Law 299

[11] [Hereafter, DS]

[12] [Hereinafter PETs]

[13] Giuseppe D'Acquisto and others, *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics* (ENISA 2015) 5; David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) (18) (1) Journal of Information and Computer Law 1

a data-driven world where such data is of immense value.[14] The continued development and utilization of PETs has led Asrow and Samonas to group them into three broad categories, namely; PETs that alter data, PETs that hide/shield data and PETs for processing, managing, and storing data.[15]

PETs include anonymous browsers, remailers, virtual private network (VPN) providers, proxy servers, digital cash, password managers and smart cards. Software and technology manufacturers may also provide data protection safeguards for their customers through tools built into their applications that allow anonymous web browsing and content sharing.[16] These tools employ several cryptographic techniques and security protocols to ensure their goal of anonymity.[17] Examples of such include anonymous web browsers such as The Onion Router and *Duck Duck Go* as well as the cloud-based instant messaging service known as Telegram which markets itself as applying end-to-end encryption for messages.[18]

PETs are fundamental in industries like finance, electronic commerce and healthcare that depend on the massive gathering and utilisation of sensitive data.[19] Organisations in the said industries design their databases with privacy management tools such as a firewall[20] that focus on confidentiality and access controls. Mechanisms are also designed to encrypt confidential data stored in databases, while decryption keys are granted to data receivers.[21] Cloud storage has also been developed to serve as backups against erasure, assist data recovery as well as provide homomorphic protection.[22] Additionally, these cloud storages

[14] Electronic Privacy Information Centre and Privacy International, 'Privacy and Human Rights Report' (EPIC 2006) 12; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for The Future at The New Frontier of Power* (Profile Books 2019) 75

[15] Kaitlin Asrow and Spirow Samonas, 'Privacy Enhancing Technologies: Categories, Uses Causes and Considerations' (*Federal Reserve Bank of San Francisco*, June 1 2021) <https://bit.ly/3SdbLC5> accessed 28 February 2024

[16] Merry Marwing, 'The Evolution of Privacy Enhancing Technologies (PETs) Trends in 2022' (*G2*, January 18 2022) <*https://www.g2.com/articles/privacy-enhancing-technologies-pets-trends-2022*> accessed 28 February 2024; Banisar and Simon Davies, supra.

[17] Van den Hoven and others, supra

[18] Telegram, 'Frequently Asked Questions' <https://telegram.org/faq> accessed 28 February 2024; Lance Henderson, *Tor and the Dark Art of Anonymity* (Vol. 1, Lance Henderson 2022) 211

[19] Asrow and Samonas, supra

[20] A firewall is a network security device that monitors and restricts network traffic based on predefined security rules; K Neupane and R Haddad and L Chen, 'Next Generation Firewall for Network Security: A Survey' (Institute of Electrical and Electronics Engineers Southeast Conference, St. Petersburg, Florida April 2018) 1-6 <https://ieeexplore.ieee.org/document/8478973/> accessed 28 February 2024

[21] Giuseppe D'Acquisto and others, supra

[22] Homomorphic encryption is a type of encryption that allows users to conduct operations on encrypted data without having to first decode it. Michael Cobb, 'Privacy-enhancing technology types and use cases' (*TechTarget*, 25 February 2022*)* <https://www.techtarget.com/searchsecurity/tip/Privacy-enhancing-technology-types-and-use-cases> accessed 28 February 2024

facilitate data replication, which is the process of storing data in more than one location to support data availability, backup, and/or disaster recovery.[23]

Furthermore, there are cryptographic algorithms known as Zero-knowledge proof,[24] which permits the validation of information without disclosing the supporting data. For instance, ZKP can be used for age verification without revealing a person's date of birth.[25]

These technology-based safeguards come in different forms and can be hardcoded into devices. A good example of a hardcoded safeguard is the encryption on an iPhone, which Apple has repeatedly refused to bypass despite law enforcement requests and a court order to unlock iPhones central to law enforcement investigations.[26] In an open letter, the company CEO Tim Cook explained that it cannot unlock iPhones for police without compromising customer privacy. Apple has however admitted to having under a lawful court order, extracted data from an iPhone running the operating systems before iOS 8.[27]

In addition to PETs, data collectors and processors in a bid to ensure data protection and data availability utilize a method known as data lifecycle management to manage data throughout its lifecycle.[28] The generally accepted life cycle for data is acquisition/entry, storage, sharing and usage, archival and data destruction.[29] While PETs cannot replace the other substantive models of data protection, doubts remain about their effectiveness and safety due to reasons such as the presence of a backdoor for developers to access personal data or the possibility of developers overriding the protection at any time.[30] It must be said that they at least provide DS with some level of protection and control over their data.[31]

[23] SIOS Technology Corporation, 'Data Replication' <https://us.sios.com/resource/data-replication/> accessed 28 February 2024

[24] [Hereafter, The ZKP]

[25] Ibid. But see also Cem Dilmegani, 'Zero-Knowledge Proof: How it Works, Use Cases & Applications' <https://research.aimultiple.com/zero-knowledge-proofs/> accessed 28 February 2024

[26] Jack Nicas and Katie Benner, 'F.B.I Asks Apple to Help Unlock Two iPhones' *The New York Times* (New York, January 7 2020) <*https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html*> accessed 28 February 2024; Eric Licthbau, 'Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman' *The New York Times* (New York, February 16 2016) <*https://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html*> accessed 28 February 2024

[27]Tim Cook, 'A Message to Our Customers' (*Apple.Com,* 16 February 2016) <*https://www.apple.com/customer-letter/*> accessed 28 February 2024

[28] M El Arass and N Souissi, 'Data Lifecycle: From Big Data to Smart Data' (Institute of Electrical and Electronics Engineers 5th International Congress on Information Science and Technology, Marrakech, October 2018) 80-87 <*https://ieeexplore.ieee.org/abstract/document/8596547*> accessed 28 February 2024

[29] Ibid

[30] Ibid. Rama Bansode and Anup Girdhar, 'Common Vulnerabilities Exposed in VPN–A Survey' (2021) (1714) Journal of Physics: Conference Series 1 <*doi:10.1088/1742-6596/1714/1/012045*> accessed 28 February 2024

[31] Van den Hoven and others, supra.; Moses Namara and others, 'Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology' (2020) (1) 83

Furthermore, modern data protection legislations and guides place obligations on controllers and processors to put technical measures in place to protect data and promote, and encourage the use of PETs in tandem with observing the law.[32]

3. The Comprehensive Model

Also referred to as the omnibus model, it involves the passing of a law that governs the collection, use, and dissemination of personal information by both the public and private sectors.[33] A comprehensive law can adequately define concepts, and terms, embed stringent controls, provide fines in addition to any other criminal liability as punishment for violations of its provisions, as well as provide for several issues in data and privacy while also balancing them against its primary purpose of data protection.[34] The use of comprehensive laws can also help harmonize different data protection rules applicable to different sectors into one binding document and it is the favoured model for most nations that are enacting data protection legislation.

The comprehensive model can also be used to standardize data protection rules across borders and as such it is the model that the European Union[35] prefers for ensuring compliance with its data protection regime.[36] The EU General Data Protection Regulation[37] is the best example of a comprehensive law, outside Europe, the Protection of Personal Information Act[38] enacted by the Republic of South Africa in 2013 is one of the foremost comprehensive laws on data protection on the African continent. Nigeria which had erstwhile favoured a sectoral model finally joined the ranks of countries with a comprehensive law with the entry into force of the Nigerian Data Protection Act[39] in June 2023.[40] Also, the African Union[41] and

Proceedings on Privacy Enhancing Technologies 1 <*https://nru.uncst.go.ug/handle/123456789/3218*> accessed 28 February 2024

[32] Information Commissioner's Office, 'Data protection by design and default' <*https://bit.ly/3r3lgYz*> accessed 28 February 2024

[33] Van den Hoven, et al, supra. See also Orla Lynskey, supra Pp. 15,45

[34] Orla Lynskey, supra at P. 43; ThalesGroup.Com, 'Beyond GDPR: Data Protection Around the World' (*ThalesGroup.Com,* May 2021) <*https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data*-protection-around-world> accessed 28 February 2024

[35][Hereafter, EU]

[36] Orla Lynskey, supra at p. 23; see also Banisar and Davies, supra at p. 13

[37] [Hereafter GDP] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (GDPR)

[38] Protection of Personal Information Act 4, 2013 [(Hereafter, POPIA] Though enacted in 2013, implementation of the Act took place in in four stages beginning in 2014 with full implementation achieved in July 2021

[39] [Hereafter, The NDPA]

[40] Nigeria Data Protection Act 2023 [Hereafter, The NDPA] <https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf> accessed 2 March 2024

[41] [Hereafter, The AU]

the Economic Community of West African States[42] have attempted to standardise data protection safeguards at the continental and sub-regional levels respectively with the use of comprehensive laws,[43] in the form of conventions.[44]

European influence on data protection is most visible in countries adopting the comprehensive model in-order to regulate data protection.[45] This influence can be traced to the 1995 EU Directive which required member states to guarantee that personal information on European residents is protected by law when it is transmitted to and processed in countries outside of Europe.[46] This adequacy requirement resulted in increased demand for the implementation of data protection regulations outside of Europe and the major way this demand was met was through the passing of comprehensive laws.

While this model provides countries outside Europe with a chance to bring their laws into consonance with Pan-European laws to increase the chances of an adequacy decision and to allow for trans-border data flows, it also provides them with an opportunity to react to past injustice perpetuated through access to personal information.[47] As was the case in Germany, the horrors of Nazi rule led to the adoption of comprehensive laws to regulate the use of personal information to prevent a repeat of violations that occurred under previous authoritarian regimes.[48]

In most of the countries that adopt this model, the comprehensive law established a supervisory or data protection agency/authority[49] headed by an independent official to oversee the enforcement and monitor compliance.[50] This official is known diversely as a

[42] [Hereafter ECOWAS]

[43] Graham Greenleaf and Bertil Cottier 'International and regional commitments in African data privacy laws: A comparative analysis,' *Computer Law & Security Review* (2022) (44) (7) 1

[44] African Union Convention on Cyber Security and Personal Data Protection Adopted by the 23rd Assembly of Heads of States and Governments held in Malabo, Equatorial Guinea, June 27, 2014 (Malabo Convention); ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010) (ECOWAS Data Protection Act)

[45] Orla Lynskey, supra at Pp. 41-45; Graham Greenleaf and Bertil Cottier, 'Data Privacy Laws and Bills: Growth in Africa, GDPR Influence' (2018) (152) *University of New South Wales Law Research Series* 11-13; Yinka Okeowo 'How European Union's GDPR Influenced Data Privacy Law in Africa' (*Techeconomy*, 2 June 2022) <https://techeconomy.ng/how-european-unions-gdpr-influenced-data-privacy-law-in-africa/> accessed 2 March 2024

[46] EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

[47] Banisar and Davies, supra at p. 11

[48] Douwe Korff and Marie Georges, 'The Origins and Meaning of Data Protection' (2020) <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3518386_code1098072.pdf?abstractid=3518386&mirid=1&type=2> accessed 2 March 2024

[49] [Hereafter DPA]

[50] Orla Lynskey, supra at p. 27

Commissioner, Chairman, Ombudsman, or Registrar. In South Africa, section 39 of the POPIA established the office of the Information Regulator which is headed by a Chairperson. In Nigeria, section 4 of the NDPA establishes the Nigerian Data Protection Commission. Article 68 of the GDPR established the European Data Protection Board (hereinafter EDPB) headed by a chairman to perform this function at the regional level, while states are directed under Article 52 to establish supervisory authorities to perform the same functions at the municipal level. In addition to the aforementioned functions, these agencies are empowered by the comprehensive law to conduct investigations into alleged breaches. In some cases, the agency can find against controllers and processors who breach the law. Also, the responsibility for educating the public on issues of data protection falls on this agency and it acts as an international liaison in data protection and data transfer.

4. Challenges and Prospects of the comprehensive model

The major appeal of this model is that it allows the government to pass a single legislation that will provide for a lot of issues on the subject of data protection. Such a law can act as a reference point for stakeholders, harmonize data protection principles, establish well-understood regulatory mechanisms, and also improve general awareness of privacy issues. While this *ex-ante* approach which is essential to the omnibus structure of the law means that the lawmakers try to anticipate all conceivable data activities and infractions and construct the law accordingly, it has the disadvantage of being prescriptive, which can make compliance difficult while also constraining both the direction of innovation and the options accessible to consumers. The GDPR has been cited as an example of a highly prescriptive *ex-ante* regulation, [51] which in operation and implementation affects innovation and the availability of numerous products, ranging from email management applications to online games and even websites due to cost or difficulty of compliance by businesses.[52] In their data-driven analysis of the effects of the GDPR, Ran Zhuo *et al* found that service providers across the world take advantage of numerous not-so-stringent existing bi-lateral independent

[51] Ibid, at p. 84; Jenifer Huddleston, 'A Primer on Data Privacy Enforcement Options' (*American Action Forum,* 4 May 2020) <https://www.americanactionforum.org/insight/a-primer-on-data-privacy-enforcement-options/> accessed 2 March 2024; Ran Zhuo and others, 'The Impact of the General Data Protection Regulation on Internet Interconnection' (2021) 45 Telecommunications Policy <https://doi.org/10.1016/j.telpol.2020.102083> accessed 2 March 2024; Launa P Nogueira, 'How the GDPR on Data Transfer Affects Cross-Border Payment Institutions' (*Internet Policy Review,* 22 June 2020) <https://policyreview.info/articles/news/how-gdpr-data-transfer-affects-cross-border-payment-institutions/1485> accessed 2 March 2024; Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies' (2016) 12 (1) Washington Journal of Law on Journal of Law, Technology & Arts 11 <http://digital.law.washington.edu/dspace-law/handle/1773.1/1654> accessed 2 March 2024

[52] Ibid

network agreements which comprise the internet, to deliver goods and services.[53] They posit that the GDPR may affect this interconnectedness by raising the operational cost of online businesses, as firms that collect personal data within the jurisdictional scope of the GDPR need to comply with a set of stringent obligations.[54]

While most commentators in the field of data protection agree on the strengths of a GDPR-type law that is comprehensive, they continually express concerns about how difficult it may be to implement such a law, particularly for governments facing significant resource constraints.[55] The DPA established by the comprehensive law can also be hampered by a lack of autonomy from other government agencies. On that note, it has been said that Countries in Africa may struggle to enforce GDPR-type laws as the current DPAs in Africa face severe resource constraints and question marks about their independence which makes it difficult to carry out their duties.[56] Also, comprehensive laws require expertise to implement and most DPAs in low- and middle-income countries already face funding constraints and may in addition to lacking autonomy from other government agencies, struggle to attract employees with the necessary expertise.[57]

I. The Sectoral Model

This model involves the use of different sectoral laws to provide for and regulate data protection in different industries operating in different economic sectors within a single country. With this model, rather than a comprehensive or omnibus law, data protection relies on a combination of industry-specific legislation and regulations.[58] In effect, this means that in a country where this model is utilized, one law would apply to the protection of personal data in the financial sector and another to the educational sector. Apart from creating a situation where there are a multitude of rules and a lack of uniformity of those rules, there is

[53] Ran Zhuo, supra

[54] Ibid,

[55] Curtiss, supra; Anupam Chandler and others, 'Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (2021) World Bank Policy Research Working Paper Series <https://scholarship.law.georgetown.edu/facpub/2374/> accessed 2 March 2024

[56] Michael Pisa and Ugonma Nwankwo, 'Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development' (*Centre for Global Development*, 9 August 2021) <https://www.cgdev.org/publication/are-current-models-data-protection-fit-purpose-understanding-consequences-economic> accessed 2 March 2024

[57] Ibid

[58] Orla Lynskey, at Pp. 25, 26

also the possibility that sectors without an operational law would be without specific data protection rules.[59]

A common feature of this model is that with so many regulations, an overarching supervisory agency is absent with compliance and enforcement achieved by a range of mechanisms including administrative panels and the overseeing government institution in that sector. This is the model favoured by the US where data protection is regulated by a patchwork of federal and state laws and regulations, which govern the treatment of data across various industries and business operations.[60] In addition, states in the US have been free to set their data protection regimes, and some have done so.[61]

Generally, federal laws regulate the collection, storage and use of sensitive non-public personal information in specific industries, while state laws, in contrast, are consumer-oriented and offer differing levels of protection from one state to another.[62] For example, the information of children is protected at the federal level under the Children's Online Privacy Protection Act[63] which prohibits the collection of any information from a child under the age of 13 online and from digitally connected devices, and requires the publication of privacy notices and collection of verifiable parental consent when information from children is being collected, while the Driver's Privacy Protection Act of 1994[64] governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. Also, certain regulations ban broad categories of behaviour that, although not limited to data protection, regulate how businesses handle personal information.[65] For example, section 45 (a) of the Federal Trade Commission Act of 1914,[66] outlaws 'unfair or deceptive acts or practices,' among other things.

[59] Woodrow Hartzog and Neil Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) (61) (5) *Boston College Law Review* 1687 <https://scholarship.law.bu.edu/faculty_scholarship/3050/> accessed 2 March 2024

[60] Ola Lynskey, supra at p. 24; Boyne, supra; Robert Hasty and Trevor W Nagel and Mariam Subjally 'Data Protection Law in the USA' (2013) <https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf> accessed 2 March 2024

[61] Hartzog and Richards, supra at 1691

[62] Andy Green, 'Compete Guide to Privacy Law in the US' (*Varonis,* 2 August 2021) <https://www.varonis.com/blog/us-privacy-laws> accessed 2 March 2024

[63] 15 U.S. Code § 6501

[64] 18 U.S. Code § 2721

[65] Stephen P Mulligan and Chris D Linebaugh, 'Data Protection Law: An Overview' (2019) Congressional Research Service <https://crsreports.congress.gov/product/pdf/R/R45631> accessed 2 March 2024

[66] 15 U.S Code § 41-58

While some state laws are comprehensive, others cover areas as diverse as protecting biometric data to keeping homeowners free from drone surveillance.[67] State laws apply to all companies that collect, keep, transmit, or process data about the residents of a state irrespective of whether or not they have a physical office in a given state.[68] The state of California has led the way among states and in 2018, enacted the California Consumer Privacy Act,[69] which became effective on January 1, 2020. Section 1798.130 of the law introduced new requirements for businesses, including:

i. Requirements to disclose the categories of personal information the business collects about consumers.

ii. Requirements to specify the pieces of personal information the business collected about the consumer.

iii. Requirements to specify the categories of sources from which the personal information is collected.

iv. Requirements to specify business or commercial purpose for collecting or selling personal information.

v. Requirements to specify the categories of third parties with which the business shares personal information.

The law also introduced new rights for California residents, including the right to request access to and deletion of personal information and the right to opt out of having personal information sold to third parties.

Recently, other states across the USA have begun initiating legislative processes that will lead to the enactment of data protection laws.[70] As of 28th February 2024, thirteen of the 50 states in the USA have enacted laws to regulate data protection, while nineteen have data protection bills at different stages of the legislative process.[71] There is however worry that if

[67] Pittman, et al, supra
[68] Ibid
[69] California Consumer Privacy Act of 2018 § 1798.100-199 of the California Civil Code
[70] Andrew Folks, 'US State Privacy Legislation Tracker' (International Association of Privacy Professionals, 22 March 2024) < https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ > accessed 25 March 2024
[71] Ibid

each state adopts their data protection law, the system would end up being highly inefficient and fragmented, with companies having to comply with up to fifty different laws.[72]

The USA is without a supervisory agency serving as a data protection regulator at the federal level, however, the FTC established under the FTC Act has jurisdiction over a wide range of commercial entities under its authority to prevent and protect consumers against unfair or deceptive trade practices, including unfair privacy and data security practices.[73] The FTC uses this authority to, among other things, issue regulations and enforce certain privacy laws.[74] Some of these laws however predate the internet as well as the modern concept of privacy and therefore have little to do with data protection in the real sense. For example, the Health Insurance Portability and Accountability Act of 1996[75] (hereinafter HIPAA) covers only communication between individuals and 'covered entities,[76] which include doctors, hospitals, pharmacies, insurers, and other similar businesses. The HIPAA does not cover all health data. As such it does not extend to data collected from fitness monitors and activity trackers such as smart-watches, pedometers, and monitors for heart rate and quality of sleep. The HIPAA also does not restrict who can ask for sensitive health information such as an individual's coronavirus vaccination status.[77]

In addition to the FTC, a variety of other agencies regulate data protection through sectoral laws, these include the Office of the Comptroller of the Currency, the Department of Health and Human Services, the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau and the Department of Commerce.[78] At the state level, the recently established CPPA is the first agency focused on solely data protection in the USA.

[72] Ana Domingo and Nathalie Villar, 'Self-regulation in data protection' (2018) <https://www.bbvaresearch.com/wp-content/uploads/2018/10/Watch_Self-regulation-and-data-protection-1.pdf> accessed 25 March 2024

[73] Pittman, et al, supra; Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (2015) (83) (6) *George Washington Law Review* 2230 <https://www.gwlr.org/wp-content/uploads/2016/01/83-Geo-Wash-L-Rev-2230.pdf> accessed 25 March 2024

[74] DLA Piper, 'Data Protection Laws of the World- United States' <https://www.dlapiperdataprotection.com/?t=law&c=US > accessed 25 March 2024

[75] 42 U.S. Code § 201

[76] Ibid, at S. 1172; Hartzog and Solove, supra at p. 2252

[77] Thorin Klosowski, 'The State of Consumer Data Privacy Laws in the US (And Why It Matters)' *The New York Times* (6 September 2021) <*https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/*> accessed 28 March 2024; Sara Morrison, 'HIPAA, The Health Privacy Law That's More Limited Than You Think explained', (*Vox,* 20 April 2021) <*https://www.vox.com/recode/22363011/hipaa-not-hippa-explained-health-privacy*> accessed 28 March 2024

[78] Pittman, et al, supra

II. The Self-Regulatory Model

With the self-regulatory model, data protection is regulated by codes of practice established either by specific companies, entities or by the various industries. This typically occurs through the privacy policy of a company or other entity, or by an industry association.[79]

The European Parliament, Council and Commission have defined self-regulation as 'the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt common guidelines amongst themselves.'[80] The distinguishing factor about this model is that stakeholders and not governmental regulators develop the codes. Akindele defines self-regulation as an in-house control mechanism adopted by any data collecting body.[81] Similarly, Coglianese and Mendelson define it as 'any system of regulation in which the regulatory target … imposes commands and consequences upon itself.'[82] The regulatory target could either be an individual firm or an industry association.[83]

Historically, this model is rooted in the acceptance that in a highly technical world, laws and government regulations frequently cannot keep up with fast-changing industries, so rather than enacting proscriptive legislation, the government established a form of agreement with industries that they have to regulate themselves or the government will do it for them.[84]

In the US, the self-regulatory model has been encouraged alongside the sectoral model since the '90s when the Clinton administration promoted it as the preferred model for protecting consumer privacy online due to fears that unnecessary regulation might distort market developments by 'decreasing the supply and raising the cost of products and services,'[85] or fail to keep pace with 'the break-neck speed of change in technology.'[86] The administration also asserted that if the industry failed to address privacy concerns through self-regulation and technology, the pressure for a governmental regulatory solution would increase. From the

[79] International Association of Privacy Professionals (IAPP), 'Self-regulatory Model' <https://iapp.org/resources/article/self-regulatory-model/> accessed 25 March 2024; Organisation for Economic Co-operation and Development (OECD), *Industry Self-Regulation: Role And Use In Supporting Consumer Interests* (OECD Publishing, Paris) 11

[80] European Council, Parliament and Commission, 'Inter-Institutional Agreement on Better Law making', OJ C 2003 321/01

[81] Roland Akindele, 'Data protection in Nigeria: Addressing the multifarious challenges of a deficient legal system' (2017) (26) (4) Journal of International Technology and Information Management 110

[82] Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-regulation' in R. Baldwin, and others (ed.), *The Oxford Handbook on Regulation* (Oxford University Press 2010)

[83] Ibid

[84] Cusumano, Gawer and Yoffie, supra

[85] William J Clinton and A Gore Jr, *A Framework for Global Electronic Commerce* (White House Office 1997) 4,18

[86] Ibid

'90s till date, the self-regulatory model is still encouraged in the USA. For example, two American technological companies, Microsoft and Facebook have self-regulatory standards that they abide by. However, while Microsoft implements the GDPR[87] as its standard for self-regulation, multiple scandals involving data breaches in Facebook which until recently was heavily criticized,[88] continually cast doubts over the effectiveness of self-regulation. With the establishment of the Facebook Oversight Board in 2020, Facebook moved from an initial 'thin' self-regulatory regime towards an 'enhanced self-regulation,' in the form of an oversight board which relies on first-party and independent third-party intermediaries.[89]

There are however guiding principles on privacy regulation:

i. Efficiency. The self-regulatory principles should harness industry expertise to achieve tailored solutions at the lowest attainable costs for the government, industry, and the public.

ii. Openness and Transparency. The self-regulatory system should enable the public to participate in developing substantive rules and enforcement mechanisms. The system should require disclosure of both substantive standards and how participating firms perform against these standards.

iii. Completeness. The principles should address all aspects of the applicable standards, in the case of data protection, that would be the full set of fair information principles.

iv. Free rider problems. The principles should have strategies to minimize firms refusing to abide by or falsely claiming adherence to self-regulatory principles while their competitors institute costly, self-regulatory standards, then free ride on the sector's improved reputation for protecting privacy.[90]

v. Oversight and enforcement. The system should provide complaint resolution mechanisms, audits or other forms of verification, and impose consequences for firms that fail to comply with substantive requirements.

vi. The use of design features mainly consists of the benefits associated with formulating principles through direct negotiations among the

[87] Microsoft, 'Safeguard individual privacy with the Microsoft Cloud.' <*https://www.microsoft.com/en-us/trustcenter/Privacy/GDPR*> accessed 30 March 2024

[88] Rotem Medzini, 'Enhanced Self-Regulation: The Case of Facebook's Content Governance.' (2021) (24) (10) New Media & Society 2227

[89] ibid; David Bromell, 'Regulating Free Speech in a Digital Age: Hate, Harm and the Limits of Censorship (Springer International Publishing, 2022) 29

[90] Neil Gunningham and Darren Sinclair, 'Leaders and Laggards: Next-Generation Environmental Regulation.' (2003) (14) (1) Management of Environmental Quality 160

parties, based on information sharing, Coasian bargaining,[91] and mutual buy-in to outcomes.[92]

a. Strengths and weaknesses of the self-regulatory model

Advocates for this model state that it is cheaper to enforce and more adaptable to innovation than government regulation and that it can promote deliberate and efficient ways to deal with consumer privacy since self-regulation can foster competition between companies in achieving the best data protection laws.[93] Also, the balance it strikes between the government and industries as well as the resultant freedom it grants often leads to innovation and an ease of doing business.[94]

Although self-regulatory codes are often deficient in one or more of the normative factors highlighted by Rubinstein, a major weakness is that of enforcement. Since self-regulatory programs rely heavily on voluntary compliance, they must also include some form of enforcement, otherwise, disobedient members of an industry can not only dodge regulatory requirements but also acquire a competitive edge (for example, by saving costs that would normally go towards compliance) over those who do, thereby defeating the point of the regulation.[95] The fear or proof that competitors not abiding by self-regulatory codes may be gaining an edge can then cause other companies to not abide by the rules.[96]

Self-regulation within an industry is analogous to a private association with rules and a typical private association punishes noncompliance with expulsion. However, expulsion is only effective if the subject of the expulsion receives advantages from the association. Determining the benefits that would be lost in the event of expulsion is one of the difficulties

[91] Coasian bargaining is based on the Coase Theorem, an idea of Richard Coase, which states that under ideal economic conditions where there is a conflict of property rights, the parties involved can bargain or negotiate terms that will accurately reflect the full costs and underlying values of the property rights at issue, resulting in the most efficient outcome. In relation to self-regulation, Rubinstein is saying that a good self-regulatory code can be achieved out of a process of negotiation between the government and industries. Rubinstein (n 95)

[92] Ira S Rubinstein, 'Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes.' (2010) (6) (3) ISJLP 380

[93] Henry H Perritt Jr, 'Regulatory Models For Protecting Privacy In The Internet' <https://www.ntia.doc.gov/page/chapter-3-models-self-regulation> accessed 30 March 2024; Juan P Mendoza and Henri C Dekker and Jacco L Wielhouwer, 'Industry Self-regulation Under Government Intervention' (2020) (36) Journal of Quantitative Criminology 183 <https://doi.org/10.1007/s10940-019-09424-x> accessed 30 March 2024

[94] Cusumano, Gawer and Yoffie, supra at p. 1264

[95] Perritt, supra

[96] Cusumano, Gawer and Yoffie, supra

with self-regulation. So, if expulsion is an ineffectual consequence, noncompliance cannot be penalized, and the self-regulatory rule frequently fails in the absence of such a benefit.[97]

The self-regulatory model also comes in for criticism on the questions of mandate and accountability. The mandate is an issue because the objectives of a self-regulatory system are drawn up by an entity lacking what Arun has described as the 'democratic legitimacy'[98] that statutory or constitutional authority might possess. No matter how well drafted, a company or an industry's self-regulatory code is, it is comprised of rules and standards that did not come from a maker without democratic legitimacy.[99] The major argument, in this case, is that in issuing a statement of values, rules, standards, community guidelines, or any self-regulatory code by whatsoever name, the company or industry has already set out the rules that it will implement in a unilateral manner that undermines those rules.[100] Codes drafted in this manner may suffer from this lack of democratic legitimacy but as the Microsoft example shows, companies and industries can adopt or base their regulatory codes on legislation that has this legitimacy.

III. The Co-regulatory Model

In between traditional government regulation and unrestricted industry self-regulation, there is the co-regulatory model.[101] It is a hybrid mechanism whereby attaining the objectives laid down in a legislative Act is entrusted to parties such as economic operators, social partners, non-governmental organisations, or associations which are recognised in the field.[102] The basic legislative Act defines the framework and the extent of the co-regulation and the parties concerned are then able to conclude voluntary agreements between themselves to achieve the objectives of the law.[103] The International Association of Privacy Professionals sees co-regulation as industry development of enforceable codes or standards for privacy and data protection against the backdrop of legal requirements by the government.[104]

[97] Frank Kuitenbrouwer, 'Self-regulation: Some Dutch Experiences' <https://www.ntia.doc.gov/page/chapter-3-models-self-regulation> accessed 30 March 2024
[98] Chinmayi Arun, 'The Facebook Oversight Board: An Experiment in Self-Regulation' (*Just Security*, 6 May 2020) <https://www.justsecurity.org/70021/the-facebook-oversight-board-an-experiment-in-self-regulation/> accessed 30 March 2024
[99] Ibid
[100] Ibid
[101] Helen Cheng, 'The rise of co-regulation, from GDPR to Canada's Bill C-11' (2020) <https://iapp.org/news/a/the-rise-of-co-regulation-from-gdpr-to-canadas-bill-c-11/> accessed 30 June 2022
[102] The European Council
[103] Ibid
[104] IAPP, 'Co-regulatory Model' <*h*ttps://iapp.org/resources/article/co-regulatory-model/> accessed 30 June 2022

In operation, co-regulation aims to fuse governmental emphasis on transparency and public accountability with the effectiveness and adaptability of self-regulation. With this model, businesses are encouraged to take proactive data protection measures because it is acknowledged that the government is ultimately in charge of defending the public interest.[105] Although similar to self-regulation, co-regulation is done under the 'shadow of the State', [106] because government approval is needed for the code of conduct to come into effect and the regulated industries or entities act knowing that the government may intervene if no compromise is found or public interests are seriously threatened.[107]

a. Strengths and weaknesses of the co-regulatory model

The less adversarial nature of co-regulation encourages a relationship between regulators and industry in which the knowledge and expertise of all parties involved can be used more effectively. Where industry professionals possess a greater level of knowledge than the legislature, the co-regulatory model may be especially helpful in bringing the innovative codes of the industries in line with objectives set by the law.[108]

While comprehensive legislation may become obsolete, co-regulation may provide industry standards approved by regulators that, in addition to being more flexible, will develop and react more quickly than laws enacted through a legislative process, resulting in laws that are more likely to be inventive, practical, and targeted to consumer needs.[109] Such a benefit is especially significant in a situation like data protection, where rapid innovation may jeopardise the credibility and effectiveness of legislation if it does not adapt to changing technological, market, and social conditions.[110]

As opposed to the self-regulatory codes, codes arrived at through the co-regulatory model will receive accreditation from authorities that possess 'democratic legitimacy', so abiding by them can be made proof of compliance with the law. Consequently, the rate of compliance is

[105] Dennis D Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' *SULR* (2011) (34) (2) 441

[106] Hans J Kleinsteuber, 'The Internet between Regulation and Governance' (2004) <https://www.osce.org/files/f/documents/2/a/13844.pdf > accessed 30 March 2024

[107] Ibid

[108] Marsden, supra at p. 54; Maximilian Grafenstein, 'Co-Regulation And Competitive Advantage In The GDPR: Data Protection Certification Mechanisms, Codes Of Conduct And Data Protection-By-Design' in G González-Fuster, R van Brakel and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, (Edward Elgar Publishing, 2019) 404

[109] Cheng, supra

[110] Marsden, supra

likely to increase as data controllers and processors will want to adhere to the code of conduct to demonstrate compliance with the law.[111]

The co-regulatory model also presents an attractive option for low-income countries where it may be expensive or difficult for their governments to acquire the specialist knowledge necessary to regulate effectively. A co-regulatory regime might reduce state monitoring and enforcement responsibilities and costs without sacrificing compliance by enabling private agencies to play a role in monitoring and enforcing compliance, with the state supervising that role through audits and other monitoring mechanisms.[112]

Another appeal of the co-regulatory model is that it could reduce the proliferation of codes, as codes could be designed to have wide applicability and not necessarily be confined or limited to a specific sector.[113] For example, a code could apply to separate sectors that have a common processing activity that shares the same processing characteristics and needs.

Despite these strengths, the co-regulatory model if not properly overseen could enable corporations in the form of a cabal to restrict entry to an industry to an extent. And the standardization it promotes can inhibit competition. Cheng reiterates the risk that co-regulation poses to the independence of a regulatory authority when it becomes involved in approving codes and certification schemes because a potential or perceived conflict of interest could compromise its impartiality as a regulator of data controllers.[114]

Although the relationship between regulators and the industry could encourage compliance as an industry is more likely to commit to rules that they helped shape, codes arrived at through the co-regulatory model although having legitimacy from the government; are still voluntary regulatory tools. Therefore, if controllers and processors within an industry choose not to comply with codes of conduct, there appears to be no way to compel them to comply as they are still voluntary. And it may be a waste of resources to monitor or enforce sanctions against such controllers and processors.

The co-regulatory model may result in a situation where a private agency empowered to monitor compliance with a code of conduct turns out to lack the resources and capacity to develop and operate a high-quality scheme or may be unwilling to be transparent about its processes and outcomes. Such a situation defeats the purpose of co-regulation. If co-

[111] Grafenstein, supra
[112] Marsden, supra
[113] Grafenstein, supra at p. 425
[114] Cheng, supra

regulation is successful, there is the possibility that the government may abuse it by continually utilizing it as a means to push operational costs to private agencies.

5. Recommendation and Conclusion

It has been demonstrated the different models for data protection. Heavy reliance was placed on examples from different jurisdictions in a bid to highlight their strengths and weaknesses. It was further revealed the lack of agreement on effectiveness of any model of data protection. It is therefore recommended that it is better for jurisdictions to find ways to synthesize the available options open them in creating a hybrid model. A hybrid model can take the strength of the omnibus protection provided by the comprehensive model and fuse it with tailored solutions for specific industries typical of the sectoral model. This approach will operate to counteract the restrictive nature of the comprehensive model. This can be further fused with the industry-led initiatives of the self-regulatory model and a balance can be struck between government oversight and industry participation with the co-regulatory model.

It was also demonstrated that an effective data protection regime depends on effective monitoring and compliance. So the presence of an omnibus law within this hybrid approach can establish a well-resourced and independent authority to ensure consistent application of rules and maintain the accountability of organizations that engage in the processing of personal data.