Walking on Sunshine: Defining the Legal Parameters of Open Data in the Philippines

Patricia Anne Alarios[★]

★ '22 J.D., *with honors*, Ateneo de Manila University School of Law. The Author was a Member of the Executive Committee and the Board of Editors of the *Ateneo Law Journal*. She was the Lead Editor of the Third Issue of the 66th Volume and the Associate Lead Editor of the Second and Third Issues of the 64th Volume.

This Note is a revised and abridged version of the Author's Juris Doctor's thesis in the Ateneo de Manila University School of Law (on file with the Professional Schools Library, Ateneo de Manila University), which won the first prize at the Foundation for Liberty and Prosperity's Dissertation Writing Contest for the Academic Year 2021-2022.

Cite as 67 ATENEO L.J. 275 (2022).

I. INTRODUCTION

Open government data, more commonly known as *Open Data*, refers to data generated by the government and its agencies that is released "in a manner that is legally and technically re-usable."[1] In other words, it is "publicly available information that can be universally and readily accessed, used, and redistributed free of charge in digital form."[2]

The government's role has been recognized as a "catalyst[ ] in the development of a data ecosystem through the opening of [its] own datasets, and actively managing [the] dissemination and use" thereof.[3] While government data may not always be characterized the same way big data is (i.e., high volume, high velocity, and high variety),[4] "[g]overnments [still] generate and collect vast quantities of data through their everyday activities,

1. Frederik Zuiderveen Borgesius, et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2075 (2015).

2. Beth Simone Noveck, *Is Open Data the Death of FOIA?*, 126 YALE L.J. F. 273, 273-74 (2016).

3. Ricard Munné, *Big Data in the Public Sector*, *in* NEW HORIZONS FOR A DATA-DRIVEN ECONOMY: A ROADMAP FOR USAGE AND EXPLOITATION OF BIG DATA IN EUROPE 199 (Jose Maria Cavanillas, et al. eds., 2016) (citing World Economic Forum, Big Data, Big Impact: New Possibilities for International Development, at 6, *available at* https://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf) (last accessed July 31, 2022) [https://perma.cc/4CWP-BZYB]. *See* Gartner, Big Data, *available at* https://www.gartner.com/en/information-technology/glossary/big-data (last accessed July 31, 2022) [https://perma.cc/8WHF-XN49].

4. Edward Curry, *The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches*, *in* NEW HORIZONS FOR A DATA-DRIVEN ECONOMY: A ROADMAP FOR USAGE AND EXPLOITATION OF BIG DATA IN EUROPE 30 (Jose Maria Cavanillas, et al. eds., 2016) (citing Doug Laney, 3D Data Management: Controlling Data Volume, Velocity, and Variety (Technical Report), at 4, *available at* http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (last accessed last accessed July 31, 2022) [https://perma.cc/GU8B-GF2G]).

such as managing pensions and allowance payments, tax collection, national health systems, recording traffic data, and issuing official documents."[5]

A. Background of the Study

This Note is concerned with open data, which contemplates data in raw form, particularly data from the government. Raw data are simply "data in their original form"[6] or "data collected which has not been subjected to processing or any other manipulation beyond that necessary for its first use."[7] The actual data collected from the data subjects is the raw data.

However, datasets in an open data regime are not limited to those collected from government-funded surveys. It likewise includes administrative government data in the hands of government agencies, which are not categorized as confidential.[8]

5. Munné, *supra* note 3, at 195.

6. GENELYN MA. F. SARTE, ET AL., ELEMENTARY STATISTICS 164 (2010).

7. Krzysztof Izdebski, Transparency and Open Data Principles: Why They Are Important and How They Increase Public Participation and Tackle Corruption, at 16, *available at* http://web.archive.org/web/20220120052820/https://transparencee.org/wp-content/uploads/2015/12/open-data-principles-by-krzysztof-izdebski.pdf (citing Unleashed Open Data Competition, Glossary, *available at* https://uladl.com/glossary). Raw data is

> [d]ata collected which has not been subjected to processing or any other manipulation beyond that necessary for its first use. Raw data, i.e., unprocessed data, is a relative term; data processing commonly occurs by stages, and the 'processed data' from one stage may be considered the 'raw data' of the next.

Id.

8. Patricia Anne R. San Buenaventura, et al., Registers and Administrative Forms Review System: Assessment of the Quality and Potentials of Administrative Data in the Philippine Government (A Paper Presented at the 14th National Convention on Statistics), at 2, *available at* https://www.psa.gov.ph/sites/default/files/6.7.2%20Registers%20and%20Administrative%20Forms%20Review%20System%20Assessment%20of%20the%20Quality%20and%20Potentials%20of%20A.pdf (last accessed July 31, 2022) [https://perma.cc/QM3N-CZ68] (citing United Nations Economic Commission for Europe, *Using Administrative and Secondary Sources for Official Statistics: A Handbook of Principles and Practices*, at 4, U.N. Doc No. E/ ECE/CES/13 (2011)).

1. What Makes Open Data Valuable?

Open data's value in modern society has been proven. Objectively, government agencies and civil society organizations are able to use such data to reduce costs of and further improve public services.[9] The private sector may also rely upon this information to maximize business potential.[10] In terms of government-held data, the concept of open data was initially intended as a public accountability measure, especially in the United States (U.S.).[11] Nowadays, beyond a governmental tool and measure for improvement of transparency, accountability, and delivery of essential services, among others, open data is also advantageous for economic gain.[12] In fact, open data in Europe has an estimated worth of more than €184 billion in 2019, and this number is projected to rise even more in the years to come[13]

Other benefits that have been derived from an open data framework include:

(a) improved government accountability;[14]

(b) improved private sector accountability;[15]

(c) enhanced consumer decision-making;[16]

(d) promotion of entrepreneurship;[17]

(e) innovation and economic growth;[18]

9. *See* Lori Bowen Ayre & Jim Craner, *Open Data: What It Is and Why You Should Care*, PUB. LIB. Q., Volume No. 36, Issue No. 2, at 173.

10. *See id.*

11. Alon Peled & Nahon Karine, Towards Open Data for Public Accountability: Examining the US and the UK Models (A Conference Paper for iConference 2015), at 1-2, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546017 (last accessed July 31, 2022) [https://perma.cc/RET6-3M24].

12. *See id.* at 3.

13. EUROPEAN DATA PORTAL, THE ECONOMIC IMPACT OF OPEN DATA 17 (2020).

14. Beth Simone Noveck, *Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency*, 19 YALE HUM. RTS. & DEV. L.J. 1, 19 (2017).

15. *Id.* at 20.

16. *Id.* at 21.

17. *Id.* at 22.

18. Borgesius, et al., *supra* note 1, at 2080.

(f) proactive democratic participation;[19] and

(g) efficiency in the delivery of public services,[20] among others.

It is understandable, therefore, that open data has been adopted into the policy framework of different nations, as will be explained in detail in the succeeding parts of this Note.

2. What is Meaningful Open Data?

In 2018, the Open Data Charter initiated a strategy of "publishing with purpose."[21] However, as the open data movement's thrust initially focused on calling for governments to resort to open data by default, it appears that such a simplistic call translated into the quantitative perception of opening more datasets without much regard to the quality of what is being shared.[22] While this is not peculiar to the Philippine open data regime alone,[23] data quality must be of foremost consideration to reap the full benefits of open data.

Thus, open data frameworks should not merely be a race to publish more datasets than other government agencies or governments in the region.[24] Such a limited view of open data will not yield a harnessing of its full potential. Manifestly, a perusal of the available datasets in the country's portal reveals different datasets of varying degrees of volume and of value.[25]

This Note proffers a legal approach in finding the answer to this conundrum. As a movement, open data will only go so far until legal issues gradually arise and eventually need to be addressed within the existing legal framework of any jurisdiction. To this end, this Note attempts to determine what is meaningful — primarily in the legal sense under the Philippine Constitution, existing laws, and prevailing jurisprudence, as well as in relation

19. *Id.* at 2083.

20. *Id.* at 2085.

21. Ania Calderon, Publishing with Purpose: Introducing Our 2018 Strategy, *available at* https://opendatacharter.medium.com/publishing-with-purpose-introducing-our-2018-strategy-ddbf7ab46098 (last accessed July 31, 2022) [https://perma.cc/HD2W-KPYX].

22. *See id.*

23. *See* Peled & Karine, *supra* note 11, at 10.

24. *See id.*

25. National Government Portal, Open Data Philippines (Beta), *available at* https://data.gov.ph/?q=search/type/dataset (last accessed July 31, 2022) [https://perma.cc/2VBQ-XVSA].

to what is meaningful open data to the stakeholders. At the outset, what may be more familiar to many is the idea of open data as an adjunct to freedom of information (FOI), but there are other legal bases that may be relied upon and provide support to open data. In any case, this is quite understandable, considering the fact that the Philippines is still catching up to its more advanced counterparts in terms of an open data regime and its execution.

Notably, experts have emphasized the value of "independent corroboration,"[26] especially in light of the coronavirus pandemic, for example. This has particular ramifications on the government's pandemic response, as different datasets are made available to the public or restricted to specific private sector groups.[27] Another issue that arose involved data quality from different data drops, where analysts found erroneous data entries and several inconsistencies after cross-validation.[28] Again, these issues go into data quality, which is not usually the center of open data discussions. Therefore, one of the major thrusts of this Note is to understand how to strike a balance between the state policy of full disclosure and right to information on one hand, and protecting privacy rights on the other. Without a legal understanding of the former, data's advantages to the government and society will not be fully maximized under a strictly conservative privacy regime.

3. Open Data and Freedom of Information

Government disclosure may be classified into two: proactive and reactive disclosure.[29] Reactive disclosure is disclosure after a demand or

26. Policy Note *by* UP COVID-19 Pandemic Response Team, *Prevailing Issues in the Time of COVID-19 and the Need for Open Data*, at 7 (May 8, 2020). In any field of science, independent corroboration of research results by other experts or peers is valued greatly for "verification, refutation, or refinement" of the soundness of methodology and findings of the study. I NATIONAL ACADEMY OF SCIENCES, RESPONSIBLE SCIENCE: ENSURING THE INTEGRITY OF THE RESEARCH PROCESS 48 (1992).

27. UP COVID-19 Pandemic Response Team, *supra* note 26 at 6.

28. *Id.* at 3.

29. Helen Darbishire, Proactive Transparency: The Future of the Right to Information? (A Paper Commissioned by the Access to Information Program at the World Bank Institute), at 3, *available at* https://openknowledge.worldbank.org/bitstream/handle/10986/25031/565980WP0Box351roactiveTransparency.pdf?sequence=1&isAllowed=y (last accessed July 31, 2022) [https://perma.cc/2B9X-KJP6]. *See also* Pearl Clemente, [FOI 101] 3.7.1 Proactive and Reactive Disclosure, *available at* https://coursebank.ph/courses/course-v1:PCOO-FOIPMO+FOI101+2020_

request,[30] easily concretized by the FOI framework in the Philippines.[31] On the other hand, proactive disclosure refers to disclosure of information without the need for any request or demand.[32] Open data falls under the proactive disclosure mechanism because, in an open data regime, the government continuously publishes and updates datasets that the people may access and reuse.[33] Additionally,

> FOI is an inherently confrontational tactic focused on prying secrets out of government. Open data is not. It depends upon the institution that collects the data wanting to publish it in order to attract knowledgeable and passionate members of the public who want to use it. *Because governments in an* [*o*]*pen* [*d*]*ata regime must proactively publish their data with the intent that people will use it, the normative essence of* [*o*]*pen* [*d*]*ata is participation rather than litigation*. The role of the public has always been to scrutini[z]e and critici[z]e. The idea that the public and government can work together to augment the manpower and skills in under-resourced public institutions continues to demand a major shift of mindset.[34]

When it comes to access to information on matters of public concern, the more traditionally and generally accepted principles are reflected in a jurisdiction's legal framework on FOI. Unfortunately, such a law has yet to be enacted in the Philippines.[35] President Rodrigo R. Duterte instead issued

---

Q3/courseware/6d98647be1164a678391a642938e941e/4bffa7e2181b4bd2b0432 0595d2a80e8/1?activate_block_*id*=block-v1%3APCOO-FOIPMO%2BFOI 1012B2020_Q3%2Btype%40vertical%2Bblock%40a4884795847 94c85aedd27d3d dd77dc5 (last accessed July 31, 2021) [https://perma.cc/58DC-FA5W].

30. *Id.*

31. Pearl Clemente, Video, [FOI 101] 3.7.1 Proactive and Reactive Disclosure, *available at* https://coursebank.ph/courses/course-v1:PCOO-FOIPMO+FOI101+2020_Q3/courseware/6d98647be1164a678391a642938e94 1e/4bffa7e2181b4bd2b04320595d2a80e8/1?activate_block_*id*=block-v1%3APCOO-FOIPMO%2BFOI101%2B2020_Q3%2Btype%40vertical %2Bblock%40a4884795847 94c85aedd27d3ddd77dc5 (last accessed July 8, 2021) [https://perma.cc/58DC-FA5W].

32. Darbishire, *supra* note 29, at 3.

33. *See* Clemente, *supra* note 31.

34. Beth Simone Noveck, *Foreword* to THE STATE OF OPEN DATA: HISTORIES AND HORIZONS xii (Tim Davies, et al. eds., 2019) (emphasis supplied).

35. *See* An Act Implementing the Right of the People to Information on Matters of Public Concern and State Policies of Full Public Disclosure of All Its Transactions Involving the Public Interest and Honesty in the Public Service and for Other

an Executive Order (E.O.)[36] on FOI in the Executive Branch in fulfillment of his campaign promise to do so.[37] However, despite his claims of commitment to FOI, some believe that the E.O. remains an insufficient mechanism for full public disclosure as local government units, the Congress, and the Judiciary are not covered by the order.[38]

Nevertheless, even with an FOI law or executive order, open data is still not directly addressed. FOI laws across jurisdictions, including those proposed FOI bills currently pending in Congress, concern the release of *specifically*

Purposes, S.B. No. 1673, § 2, 18th Cong., 2d Reg. Sess. (2020); An Act Strengthening the Right of Citizens to Information Held by the Government, Institutionalizing Open Data Governance and for Other Purposes, S.B. No. 795, § 2, 18th Cong., 1st Reg. Sess. (2019); An Act Implementing the People's Right to Information and the Constitutional Policies of Full Public Disclosure and Honesty in the Public Service and for Other Purposes, S.B. No. 606, § 2, 18th Cong., 1st Reg. Sess. (2019); An Act Implementing the Right of the People to Information on Matters of Public Concern Guaranteed Under the 1987 Philippine Constitution, and for Other Purposes, S.B. No. 511, § 2, 18th Cong., 1st Reg. Sess. (2019); An Act Implementing the People's Right to Information and the Constitutional Policies of Full Public Disclosure and Honesty in the Public Service and for Other Purposes, S.B. No. 324, § 2, 18th Cong., 1st Reg. Sess. (2019); An Act Implementing the People's Right to Information and the Constitutional Policies of Full Public Disclosure and Honesty in the Public Service, and for Other Purposes, S.B. No. 265, § 2, 18th Cong., 1st Reg. Sess. (2019); & An Act Implementing the People's Right to Information and the Constitutional Policies of Full Public Disclosure and Honesty in the Public Service and for Other Purposes, S.B. No. 121, § 2, 18th Cong., 1st Reg. Sess. (2019).

36. Office of the President, Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor, Executive Order No. 2, Series of 2016 [E.O. No. 2, s. 2016] (July 23, 2016).

37. Rappler, *Duterte Bent on Pushing FOI, Even If It Takes an EO*, RAPPLER, May 11, 2016, *available at* https://www.rappler.com/nation/132693-duterte-push-freedom-of-information-eo (last accessed July 31, 2022) [https://perma.cc/T9C9-ZH84].

38. Leila B. Salaverria, *Duterte's FOI Order Leads to 'Unintended Consequences'*, PHIL. DAILY INQ., June 26, 2017, *available at* https://newsinfo.inquirer.net/908698/dutertes-foi-order-leads-to-unintended-consequences (last accessed July 31, 2022) [https://perma.cc/2A7Z-727H].

requested information.[39] In contrast, raw data and information are readily available and easily accessible, ideally through online government portals, *without need for a request* filed by natural or juridical persons in an open data framework.[40] Hence, an open data policy entails "*proactive publication* of [ ] classes of information" in their entirety, as much as practicable.[41] This proactive stance on the part of the government reflects an approach closer to accountability and transparency to the people.[42]

A law on FOI does not traditionally contemplate Open Data, which is arguably a step further in the realm of *sunshine laws* because FOI is grounded on specific requests from the people, based on its nature as a reactive disclosure mechanism.[43] More practically, in the Philippines, there may be instances of relatively slow movement in the bureaucratic process of requesting information or data from the government.[44] Theoretically, such information should have been made publicly available in the first place, even without a request under the policy of mandatory public disclosure[45] and following the intent of the framers of the Constitution regarding this provision. There is also the matter of penalties for a public official's failure to comply with accepted open data standards.

After exploring constitutional and statutory provisions that lend support to open data, this Note primarily endeavors to find the balance between *providing high quality and quantity of information that can be made available* to the public without offending the privacy rights of the data subjects.

B. Statement of the Problem

Based on the current interpretation of the right to information on matters of public concern, there arises the issue of whether there is a legal basis to recognize open data within the Philippine legal framework. In taking an in-

39. Noveck, *supra* note 2, at 274.

40. *Id.*

41. *Id.* (emphasis supplied).

42. *Id.* at 276.

43. *See* Darbishire, *supra* note 29, at 3.

44. *See* Statement *by* Cebu Citizens-Press Council, *CCPC Hails Signing of FOI Ordinance* (July 28, 2022) (*available at* https://www.cebucitizenspresscouncil.org (last accessed July 31, 2022) [https://perma.cc/DCC2-5JDL]). *But see* E.O. No. 2, s. 2016, § 9.

45. *See* PHIL. CONST. art. II, § 28.

depth look at the Philippine open data regime, it is integral to determine the legal parameters of its use vis-à-vis data privacy rights.

Building a stronger legal framework for open data will ensure that priority for transparency and government disclosure of information on matters of public concern will no longer shift as chief executives come and go. By finding strong constitutional support for open data, the Author hopes that a legal approach will pave the path to a sound and well-institutionalized open data regime in the country. Thus, a recognized obligation on the part of the government to make such data available and accessible to the people under an open data regime and a legally defensible right to the same will therefore operate to safeguard the underlying principles of a healthy democracy and maintain the benefits enjoyed by the people.

C. Significance of the Study

As briefly pointed out earlier, open data frameworks have proven to be highly advantageous to the governments and the people. Several examples are in order:

(a) A transparency initiative in Ohio released state-level financial data, including salaries of government employees, which "allow[ed] citizens to keep track of what the government is doing with their money, create[d] transparency which allow[ed] the citizens to hold their elected officials accountable, and promote[d] government efficiency by making spending information more easily accessible and open to public scrutiny."[46]

(b) In Arizona, the state compiled information on opioid prescription patterns of doctors and released such data publicly.[47] As a result of the publicly available medical information, doctors became more circumspect in their prescriptions, and the state saw a marked reduction in the prescription of opioid medication.[48]

(c) California law has incorporated a specific legal provision for improving its water database to fill in the gaps in its water data

46. Charles Roman, *Open Data*, 8 CONLAWNOW 19, 21 (2016).

47. Noveck, *supra* note 14, at 21 (citing Scott Calvert, Doctors' Individual Opioid Prescription 'Report Cards' Show Impact, *available at* https://www.wsj.com/articles/doctors-individual-opiate-prescription-report-cards-show-impact-1472856624 (last accessed July 31, 2022) [https://perma.cc/TK9X-BT58]).

48. *Id.*

> network in order to improve the government's decision-making.[49] The state had been experiencing drought and scarcity of water resources,[50] so the government took to water data in order to address issues of uniformity[51] and data integration[52] in their existing water databases.

These are only a few of the many other instances where open data resulted in a step forward towards a healthy democracy and enhanced civic participation. Public response to the information derived from the data made publicly available breaks the ground for the discussion of open data as an obligation of the government and as a right of the people, much like how the twin provisions of full public disclosure[53] and the right to information[54] are understood together in Philippine law. More than a tool traditionally used as a transparency and accountability measure, open data has evolved its potential into a collaboration between government and civil society to troubleshoot problems and find solutions.[55]

Foreign jurisdictions have begun taking steps to harness data for the benefit of society.[56] Data-driven decisions are becoming more and more important in deciding policy direction, and it is therefore only important that a jurisdiction's legal framework makes space for such developments while protecting the existing rights of individuals. The examples of meaningful use of open data show that while open data gained traction as a tool for the people to exact accountability from its government and public officials, it has also evolved into a measure that allows for collaboration between the government and the people in terms of economic, research, and other objectives.

This Note submits a legal approach to understanding open data beyond a mere policy tool for a stronger foundation of a Philippine open data regime.

---

49. Jonathan Gage Marchini, *Connecting the "Drops" of California Water Data: Chapter 506: The Open and Transparent Water Data Act*, 48 U. PAC. L. REV. 785, 793 (2017).

50. *Id.* at 786.

51. *Id.* at 794.

52. *Id.* at 795.

53. *See* PHIL. CONST. art II, § 28.

54. *See* PHIL. CONST. art III, § 7.

55. Noveck, *supra* note 34, at xii.

56. *See e.g.*, EUROPEAN DATA PORTAL, *supra* note 13, at 22–24.

D. Scope and Limitations

Considering that an open data regime introduces a new paradigm in which fields of law, as currently understood, may need to provide for new mechanisms or to adjust current legal principles, it is important to delineate the scope of this Note. As the Philippines is still comparatively young in terms of open data regimes, this Note will focus on the standards and basic principles of open data and whether existing laws and jurisprudence support the same.

Problems that may arise concerning property rights, competition law, trade law, and copyright law will no longer be discussed. These more specialized fields of law and their interplay with data, open data, and the right to information should be the subject of separate comprehensive work.

II. THE PHILIPPINE OPEN DATA REGIME

A. The Constitutional Right to Information & Policy of Full Public Disclosure

Whenever open data is being discussed, the foremost consideration as its legal basis is the *right to information*.[57] In the Philippine Constitution, this right is enshrined in Section 7 of the Bill of Rights —

> The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.[58]

This provision was not included in the 1935 Bill of Rights[59] and was only introduced and recognized in the 1973 Constitution.[60]

It bears stressing that access to information must be understood closely with the government's obligation to disclose matters of public interest. In fact, the Constitution expressly declares that "[s]ubject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public

57. *See* Katleen Janssen, Open Government Data: Right to Information 2.0 or Its Rollback Version? (A Working Paper Submitted to the Journal of Community Informatics), at 2, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_*id*=2152566 (last accessed July 31, 2022) [https://perma.cc/N97R-K4S4].

58. PHIL. CONST. art. III, § 7.

59. *See* 1935 PHIL. CONST. art. III (superseded in 1973).

60. *Compare* 1935 PHIL. CONST. art. III (superseded in 1973), *with* 1973 PHIL. CONST. art. III (superseded in 1987).

disclosure of all its transactions involving public interest."[61] This provision on disclosure "complements the right of access to information on matters of public concern found in the Bill of Rights."[62] It is the government's duty to provide information, even when there is no request or demand for such information.[63] And despite the import of the constitutional deliberations which consider this correlative duty to disclose as non-self-executory,[64] the Supreme Court arrived at a different interpretation, declaring Section 28 as a self-executing provision alongside Section 7 of Article III.[65] Thus, it is likewise a source of substantive rights of the people and the mirrored obligation of government to disclose, at its own instance, matters of public concern.[66] While ordinarily, provisions under the Declaration of Principles and State Policies are treated as non-self-executory provisions,[67] more so those sections which make particular reference to a further act of Congress, the Supreme Court concluded that what the Legislature was merely tasked to do under Section 28 is to provide for reasonable safeguards and not suspend its effectivity absent such legislation.[68]

1. Deliberations of the 1986 Constitutional Commission

Originally, in the discussions during the 1971 Constitutional Convention, the right to information was not self-executory and thereby necessitated implementing legislation.[69] It was Commissioner Victor De la Serna who suggested that "the Constitution itself should give the right but subject to statutory limitations."[70] The rest of the delegates shared the sentiment and approved the final version, which stated, "[t]he right of the people to

61. PHIL. CONST. art. II, § 28.

62. JOAQUIN G. BERNAS, S.J., THE 1987 CONSTITUTION OF THE REPUBLIC OF THE PHILIPPINES: A COMMENTARY 99 (2009).

63. *Id.*

64. *Id.* (citing 5 RECORD OF THE CONSTITUTIONAL COMMISSION, NO. 91, at 25 (1986)).

65. Province of North Cotabato v. Government of the Republic of the Philippines Peace Panel on Ancestral Domain (GRP), G.R. No. 183591, 568 SCRA 402, 470-71 (2008).

66. *Id.* at 470.

67. Kilosbayan, Incorporated v. Morato, G.R. No. 118910, 246 SCRA 540, 564 (1995).

68. *North Cotabato*, 568 SCRA at 470.

69. BERNAS, *supra* note 62, at 380.

70. *Id.*

information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, shall be afforded the citizen, subject to such limitations as may be provided by law."[71]

In *Baldoza v. Dimaano*,[72] which tackled public access to the docket records of a sitting judge,[73] the Supreme Court had the opportunity to elaborate that

> the incorporation of [the right to information] in the [1973] Constitution is a recognition of the *fundamental role of free exchange of information in a democracy. There can be no realistic perception by the public of the nation's problems, nor a meaningful democratic decision*[-]*making if they are denied access to information of general interest. Information is needed to enable the members of society to cope with the exigencies of the times*.[74]

Father Joaquin G. Bernas, S.J. explained that the significance of the provision's self-executory nature[75] finds relevance in the Supreme Court's pronouncement in the case of *Subido v. Ozaeta*.[76] In this case, the Supreme Court declared that "freedom of information or freedom to obtain information for publication is not guaranteed by the [C]onstitution."[77] Clearly, the same pronouncement would no longer hold true today. Thus, the shift in understanding the nature of the right to information brought about by the 1973 provision clarifies that "[t]he role given to the National Assembly was not to give the right[,] but simply to set limits[,]" because the Constitution already recognizes such right.[78]

The case of *Legaspi v. Civil Service Commission*,[79] which was decided after the 1987 Constitution took effect,[80] affirms the self-executory nature of this right.[81] In this case, the Supreme Court stated that Section 7 of the Bill of

71. 1973 PHIL. CONST. art. IV, § 6 (superseded in 1987).

72. Baldoza v. Dimaano, A.M. No. 1120-MJ, 71 SCRA 14 (1976).

73. *Id.* at 17.

74. *Id.* at 19 (emphasis supplied).

75. BERNAS, *supra* note 62, at 380.

76. Subido v. Ozaeta, 80 Phil. 383 (1948).

77. *Id.* at 386 (emphasis omitted).

78. BERNAS, *supra* note 62, at 380.

79. Legaspi v. Civil Service Commission, G.R. No. L-72119, 150 SCRA 530 (1987).

80. The 1987 Constitution came into force on 11 February 1987. Office of the President, Proclamation No. 58 (Feb. 11, 1987).

81. *Legaspi*, 150 SCRA at 534.

Rights "suppl[ies] the rules by means of which the right to information may be enjoyed by guaranteeing the right and mandating the duty to afford access to information. Hence, the fundamental right therein recognized ... by the people ... [is] without need for any ancillary act of the Legislature."[82] And in *Province of North Cotabato v. Government of the Republic of the Philippines Peace Panel on Ancestral Domain* (*GRP*),[83] the Court affirmed that

> [t]he complete and effective exercise of the right to information *necessitates that its complementary provision on public disclosure derive the same self-executory nature*. Since *both provisions go hand-in-hand*, it is absurd to say that the broader right to information on matters of public concern is already enforceable while the correlative duty of the State to disclose its transactions involving public interest is not enforceable until there is an enabling law.[84]

As may be seen in the wording of the provision, the 1973 version did not contemplate "government research data used as basis for policy development," as this clause was only added by the 1986 Constitutional Commission.[85] What prompted this addition was "the government practice during the martial law regime of withholding social research data from the knowledge of the public whenever such data contradicted policies which the government wanted to espouse."[86] Commissioner Wilfrido V. Villacorta introduced the amendment in the following exchange —

> MR. VILLACORTA: My point here, Mr. Presiding Officer, is that *the public should be more than just informed about official transactions*. I think they have the *right to know data that concern them especially if they themselves are the subject of surveys*. The experience during the past dispensation was that *state-sponsored research was manipulated to serve the interests of the regime, to legitimize its policies and perpetuate the power of its leaders. And since its think tanks conduct research to have an empirical basis for policy formulation, the public has the right to have access to these research findings*.
>
> ...

82. *Id*. at 535 (citing THOMAS COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 165 (1927)).

83. *North Cotabato*, 568 SCRA at 470.

84. *Id*. at 470-71 (citing Chavez v. National Housing Authority, G.R. No. 164527, 530 SCRA 235, 331 (2007)) (emphases supplied).

85. *Compare* 1973 PHIL. CONST. (superseded in 1987), *with* PHIL. CONST. art. III, § 7.

86. BERNAS, *supra* note 62, at 381.

> MR. VILLACORTA: I have in mind, for example, the research findings on nutrition which the previous government suppressed because they proved that we are among the most malnourished countries in the world. *Researchers from universities were refused access to data*, for obvious political reasons. Since the intent of this Section 6 is to adequately inform the public so that nothing vital in state affairs is kept from them, then we should add to this provision access to the results of government research.[87]

Other similar instances were brought up in the deliberations. Commissioner Vicente B. Foz narrated a situation in which a researcher interested in studying the financial operations of multinational drug companies using the financial records filed with the Securities and Exchange Commission was not given access to such data.[88] Commissioner Minda Luz M. Quesada also shared that a government agency commissioned the University of the Philippines to study primary health care and its implementation in the country.[89] The research strongly opposed the government's declaration on the matter, and the results were withheld from the public.[90] Commissioner Quesada then asked if the research group would be liable should it reveal the results, to which Fr. Bernas answered in the negative, based on the fact that it is a matter of public concern.[91]

While it can be gleaned from the delegates' discussion that they were referring to the findings of whichever study was under consideration or had been commissioned by the government, the final constitutional provision refers to government research data, and not just its results.[92] This distinction is important because the results of a study are not equivalent to the research data. Rather, the results are derived from the data, and are, more often than not, summarized and simplified to be more easily understood by the intended audience, who are most likely not well-versed with the technical know-how of analyzing data that is not yet summarized. On the other hand, research data refers to the raw form of the data, where information about each data subject

87. 1 RECORD OF THE CONSTITUTIONAL COMMISSION, NO. 32, at 709 (1986) (emphases supplied).

88. *Id.*

89. *Id.* at 710.

90. *Id.*

91. *Id.*

92. *See* PHIL. CONST. art. III, § 7.

is recorded as variables and are used by the researchers in generating analyses about the population.[93]

If the commissioners were only contemplating public access to the results of government studies, then the pillar upon which open data relies inevitably crumbles. Thus, the Author argues that the constitutional provision, as presently worded, provides express support to public access not only to results of government research but also to the research data used to arrive at those results. When Commissioner Villacorta's amendment was put to a vote, there were no objections.[94] It may thus be inferred that the Commission was in agreement that access to data was contemplated in the right to information, not just the results derived therefrom. Further inference can be made to the effect that it is only right to allow access not merely to the results of a study or research endeavor but also to the data from which such results are derived in order to verify and replicate the results, should anyone be so minded to quell any doubts by running his or her own analysis on the data.

More importantly, despite the language referring to research results instead of data during the deliberations, the common ground among the situational examples referred to and where Commissioner Villacorta was coming from, was *the intent to address the situation in which data gathered about the people using public funds were manipulated to serve the interests of the reigning administration or withheld to keep the administration's reputation intact*.[95] Keeping true to this constitutional intent requires allowing public access to the data in order that the people may have the opportunity to confirm the results fed to the public.

With respect to the state policy on full public disclosure under Section 28 of Article II, it was recognized that the "provision recognizes the duty of officialdom to give information even if nobody demands."[96] This accountability mandate under Section 28 reflects the vision of the commissioners of a Philippine government that puts prime on transparency, accountability, and integrity in public service.

93. *See* University College London, UCL Research Information and IT Services Group (RIISG), ¶ 1.1, *available at* https://www.ucl.ac.uk/isd/sites/isd/files/ucl_research_data_policy_v6.pdf (last accessed July 31, 2022) [https://perma.cc/ARC4-SSFM].

94. 1 RECORD OF THE CONSTITUTIONAL COMMISSION, NO. 33, at 760 (1986).

95. 1 RECORD, PHIL. CONST., NO. 32, at 708-09.

96. BERNAS, *supra* note 62, at 99.

Commissioner Blas F. Ople further clarified the provision's intent to write into the Constitution the concept of proactive disclosure.[97] He was strongly questioned on this point by Commissioner Hilario G. Davide, Jr., who manifested that the right to information under the Bill of Rights would no longer be needed if the provision that is now known as Section 28 of Article II was accepted.[98] In reply, Commissioner Ople emphasized the "splendid symmetry"[99] of these two provisions because the State

> cannot anticipate the millions of transactions in which citizens will be involved thereby urging the government to release information in specific cases ... [T]here is no conflict but a great complementarity ... between this obligation of the State for full public disclosure and the right of the citizens to get the information they seek from the State.[100]

The expectation was for this provision to "influence the climate of public ethics immediately[,]"[101] but Congress shall still enact a law to fully effect what the Commissioners had envisioned.[102]

The deliberations show that the State being referred to includes *all* agencies and departments of the government, instrumentalities, government-owned and controlled corporations, and the individual public officers.[103] This clarification is relevant because, regardless of the disclosure's nature (i.e., proactive or reactive), the State's policy applies to the entire government and not just to one particular branch.[104] From this view, FOI in the executive branch, while a step forward, is clearly not enough.

Additionally, the information under this envisioned proactive disclosure mechanism must be disclosed periodically.[105] In open data parlance, such periodic disclosure remains consistent with the principle of timely release of relevant datasets through the designated portals.

Quite interestingly, when all these matters were being discussed by the 1986 Constitutional Commission, open data or the mere idea of government

97. *See* 5 RECORD, PHIL. CONST., NO. 91, at 26-28.

98. *Id.* at 28-29.

99. *Id.* at 29.

100. *Id.*

101. *Id.* at 25.

102. *Id.*

103. *See* 5 RECORD, PHIL. CONST., NO. 91, at 26-28.

104. *Id.* at 25.

105. *Id.*

dataset disclosure had not yet gained traction.[106] And yet, the brilliant minds of the drafters of the fundamental law of the land had already planted the seeds for such a regime in due recognition of the democratic principles of transparency and accountability underlying open data regimes.

B. Reactive Disclosure

The government's FOI program is an example of a reactive disclosure mechanism. There have been several attempts at legislating FOI, but none have succeeded thus far, despite the priority assigned to it by the Duterte administration.[107]

1. Freedom of Information in Government

In 2016, President Duterte issued Executive Order No. 2, which operationalized FOI in the executive branch.[108] As the issuance is only an executive order, it does not cover the Legislature, Judiciary, and local government units.[109] Section 3 of the order declares that "[e]very Filipino shall have access to information, official records, public records, and documents and papers pertaining to official acts, transactions or decisions, as well as to government research data used as a basis for policy development."[110]

While this move amounts to bigger strides towards a transparent government, the same only covers the executive branch. Transparency, as well as the mechanisms or safeguards therefor, must be implemented by all branches and in all levels of government.

The FOI program envisions "a data-informed and data-empowered citizenry [that is cultivated] through FOI because when people are armed with the right information, they have the power to make informed and calculated choices about their government, participate meaningfully in public discourse,

106. Open Government Partnership, Philippines: Open Data (PH0031), *available at* https://www.opengovpartnership.org/members/philippines/commitments/PH0031 (last accessed July 31, 2022) [https://perma.cc/D5S6-XAPA].

107. Nestor Corrales, *Palace 'Optimistic' 18th Congress Will Pass FOI Bill 'Swiftly'*, PHIL. DAILY INQ., July 3, 2019, *available at* https://newsinfo.inquirer.net/1137218/palace-optimistic-18th-congress-will-pass-foi-bill-swiftly (last accessed July 31, 2022) [https://perma.cc/2ZUL-ZG3U].

108. E.O. No. 2, s. 2016.

109. *See id.* § 2.

110. *Id.* § 3.

and hold the government into account."[111] This vision echoes the traditional understanding of the right to information, which rests the foundation of the right to information upon transparency, accountability, and public participation.

Taking the next step forward with open data reflects a shift from this perspective to a more collaborative approach between the government and its citizens in creating long-lasting solutions to a variety of pressing problems. Transparency and accountability remain to be foundational principles relied upon by the right to information, but public participation in the context of working with — and not merely against — the government is further hammered upon in open data.

2. Legislating Freedom of Information

As the intended implementing legislation of the right to information, FOI bills have been passed in the Senate, but these are not successfully enacted into law because the counterpart bill is not approved by the House of Representatives.[112] A sponsor of one FOI Bill affirmed that a statute on FOI is still needed to (a) provide funding; (b) institutionalize the program; and (c) impose criminal penalties.[113] Indeed, there is a "need to institutionalize the FOI program so that it will not be removed or underfunded depending on the whims of the next president[.]"[114]

In the 18th Congress, seven bills on FOI were filed in the Senate, and none in the House of Representatives. Moreover, in the 17th Congress, only

111. Kristian Ablan, SPARTA 1.1.1. Welcome to the Course!, *available at* https://coursebank.ph/courses/course-v1:PCOO-FOIPMO+FOI101+2020_Q3/courseware/98302e3c32c54cf29ac85a798d0efeed/5469fd2a7a9e46d5a785bdc72622240c/1?activate_block_*id*=block-v1%3APCOO-FOIPMO%2BFOI101%2B2020_Q3%2Btype%40vertical%2Bblock%40f528c66b034b427887e40ba25ff05dfa (last accessed July 8, 2021) [https://perma.cc/Y8JT-MNYN].

112. KD Suarez, *Freedom of Information: What's Lacking in Duterte's EO?*, RAPPLER, July 26, 2016, *available at* https://www.rappler.com/nation/140976-lacking-duterte-freedom-information-executive-order (last accessed July 31, 2022) [https://perma.cc/6YBN-NLCR].

113. *Id.*

114. *Id.*

one bill on FOI was filed back in 2016,[115] and this only reached the committee referral stage.[116]

Despite these initiatives, it is the Author's position that even with an FOI law — especially as currently drafted in the pending bills — there must still be a separate implementing law for proactive disclosure through open data. To reiterate, open data is closely related to FOI to the extent of mandating government disclosure of public sector information. And as can be gleaned from the proposed bills, there is no clear standard for the disclosure of datasets in particular, although "Information," as defined,[117] may be argued to cover datasets already. More importantly, these FOI bills still operate under the general assumption that a citizen makes a request for information on matters of public concern, based on the provisions on access to information, which state that access to information shall be granted to Filipinos upon request. Open data's minimal mention in Senate Bill No. 795[118] and House Bill No. 1855[119] merely touches upon open data and the Open Data Task Force, but do not delve deeper into other issues beyond FOI but are related to open data. While some had provisions on digitization, these are still not enough. Under an open data regime, the data must be in machine-readable format to facilitate data integration and use.

Nonetheless, the successful enactment of a law on FOI is still welcome in order to institutionalize this program across all branches of government, the constitutional bodies, and local government units.

C. Proactive Disclosure

One particular provision in the Constitution that espouses a mandatory proactive disclosure of information from the government is Section 21 of

115. An Act to Strengthen the Right of Citizens to Information Held by the Government, H.B. No. 1855, 17th Cong., 1st Reg. Sess. (2016). This bill was introduced by Representative Sol Aragones.

116. Four bills on FOI were newly filed before the Senate of the 19th Congress and none, still, before the House of Representatives. This Note only covers the FOI bills filed during the 18th Congress.

117. "Information is stimuli that has meaning in some context for its receiver. When information is entered into and stored in a computer, it is generally referred to as data." TechTarget, Definition: Information, *available at* https://www.techtarget.com/searchdatamanagement/definition/information (last accessed July 31, 2022) [https://perma.cc/C8ZD-TJ3E].

118. *See* S.B. No. 795, §§ 25 & 27.

119. *See* H.B. No. 1855, § 25.

Article XII.[120] This provision on the government's foreign loans mandates public access to information relevant to foreign loans.[121] The records show that this provision was introduced by Commissioner Edmundo G. Garcia, and the final form of the provision was arrived at after a counterproposal from the Committee.[122] In adding such a provision, Commissioner Garcia intended to emphasize the gravity of the foreign loans contracted by the State, especially because it is the taxpaying public who will be shouldering the payment.[123]

Applying this similar line of reasoning in the context of open data, it can be argued that, beyond furthering the purposes of transparency and accountability, datasets containing data generated from the public or in the course of the performance of a public function should be made available to the people who are paying for such data collection or generation. In this sense, therefore, taxpayers should have access to information paid for by their taxes, especially if these are not covered by constitutional, statutory, and jurisprudential exemptions.

A Joint Memorandum Circular was issued in 2014 to inform government agencies about open data, but as a mere executive issuance, it did not have the same force of compliance for the legislative and judicial branches as it had for the executive agencies.[124] Nevertheless, datasets must be "searchable," "understandable," and "accessible," according to the Circular.[125]

The 2014 Joint Memorandum Circular was replicated in 2015, with further reference to the open data provision in the 2015 General Appropriations Act (GAA).[126] Openness was also established to mean that datasets must be "machine-readable, in open formats, and released with open

120. PHIL. CONST. art. XII, § 21.

121. PHIL. CONST. art. XII, § 21.

122. BERNAS, *supra* note 62, at 1236 (citing 3 RECORD, PHIL. CONST., NO. 64, at 639).

123. *Id.*

124. Department of Budget and Management (DBM), Office of the Presidential Spokesperson (OPS), & Presidential Communications Development and Strategic Planning Office (PCDSPO), Open Data Philippines, Joint Memorandum Circular 2014-01 [Jt. Memo. Circ. 2014-01], ¶ 9.

125. *Id.*

126. Department of Budget and Management, Office of the Presidential Spokesperson, & Presidential Communications Development and Strategic Planning Office, Open Data Philippines, Joint Memorandum Circular 01 of 2015 [Jt. Memo. Circ. 2015-01], ¶ 1.

licenses[,]"[127] with the added characteristics of being timely, described, and managed post-release.[128] By 2017, the Philippine Statistics Authority (PSA) also made public its statistical datasets through another portal, OpenStat.[129]

3. Statutory Provisions on Open Data

As briefly mentioned earlier, open data was specifically mentioned twice in Philippine law, once each in the General Appropriations Act (GAA) of the years 2015 and 2016 —

> SECTION 26. *Open Government Data.*
>
> Departments, bureaus, and offices of the National Government, including Constitutional Offices enjoying fiscal autonomy, SUCs, and GOCCs shall adopt a policy of openness for all datasets created, collected, processed, disseminated, or disposed through the use of public funds to the extent permitted by applicable laws and subject to individual privacy, confidentiality, national security, or other legally-mandated restrictions. Openness means that datasets published by agencies shall be machine-readable, in open formats, and released with open licenses.
>
> Implementation of this section shall be subject to guidelines to be issued by the Open Data Philippines Task Force comprised of the Office of the Presidential Spokesperson, [Department of Budget and Management], and the Presidential Communications Development and Strategic Planning Office.[130]

The 2016 counterpart of this provision only replicates the first paragraph.[131] Unfortunately, the open government data provision was not

127. *Id.* ¶ 7.

128. *Id.* ¶ 8.

129. Philippine Open Government Partnership (OGP) National Action Plan 2017-2019, at 9, *available at* https://www.opengovpartnership.org/wp-content/uploads/2018/06/Philippines_-Action-Plan_2017-2019_updated.pdf (last accessed July 31, 2022) [https://perma.cc/592Z-B826].

130. An Act Appropriating Funds for the Operation of the Government of the Republic of the Philippines from January One to December 31, Two Thousand and Fifteen, and for Other Purposes, Republic Act No. 10651, § 26 (2014) [hereinafter GAA 2015] & An Act Appropriating Funds for the Operation of the Government of the Republic of the Philippines from January One to December 31, Two Thousand and Sixteen, and for Other Purposes Approved by the President on December 21, 2015, Republic Act No. 10717, § 27 (2015) [hereinafter GAA 2016].

131. GAA 2016, § 27.

reproduced in the succeeding GAAs since 2017.[132] The plenary deliberations of the GAAs also do not provide any background as to the existence and consequent disappearance of these provisions after 2016.[133]

4. Current Policy Framework

Clearly, the government has taken steps to improving the established Open Data policy.[134] However, much like the FOI, the previously discussed executive issuances do not cover the other two branches of government, the Office of the Ombudsman, the constitutional bodies, and the local government units. Even with the statutory provisions in the 2015 and 2016 GAA which would have mandated compliance from these government offices, the effect was not long-lasting as GAAs need to be reenacted every year. Quite obviously, with the deletion of the Open Data provision from the 2017 GAA up to the present, there is now no legislative force which enforces compliance.[135]

Moreover, a perusal of the official data portal manned by the Open Data Task Force reveals that there are only 408 datasets uploaded,[136] contrary to the claim of having published 1,237 datasets back in 2015.[137] It may be the case that some datasets were deleted, but there was no explanation on this matter at all. And in 2016, after the national elections, procurement data and other

132. *Compare* GAA 2015, § 26, *with* GAA 2016, § 27.

133. A review of the congressional deliberations for GAA 2015 and GAA 2016 did not show any discussion on these open data provisions. However, the data portal makes reference to these two laws as part of the legal bases of open data, despite not being reenacted in subsequent GAAs after 2016.

134. *See* Philippine Open Government Partnership, 5th National Action Plan, at 51-52, *available at* https://www.opengovpartnership.org/wp-content/uploads/2019/12/Philippines_Action-Plan_2019-2022_Revised.pdf (last accessed July 31, 2022) [https://perma.cc/62YK-DTZV].

135. *See* An Act Appropriating Funds for the Operation of the Government of the Republic of the Philippines from January One to December 31, Two Thousand and Seventeen and for Other Purposes, Republic Act No. 10924 (2016).

136. *See* National Government Portal, *supra* note 25. This figure reflects the number of datasets available when this work was first written. It appears that the count fluctuates severely.

137. Philippine Open Government Partnership, National Action Plan 2015-2017, at 16, *available at* https://www.opengovpartnership.org/wp-content/uploads/2019/06/PHILIPPINE-OPEN-GOVERNMENT-PARTNERSHIP-NATIONAL-ACTION-PLAN-2015-2017.pdf (last accessed July 31, 2022) [https://perma.cc/XUC2-PWYP].

information readily available before were allegedly no longer made available without sufficient explanation.[138]

Here lies another trouble that is sought to be addressed — there must be a stronger legal basis for Open Data, anchoring upon and implementing the public's right to information and the state policy of full public disclosure in order to prevent similar instances of "disappearing" data. Institutionalizing the same will assure continuity in operations, non-reliance upon the present administration's priorities, and coverage of national and local governments.

5. House Bill on Open Data

In 2020, a bill on open data was introduced in the House of Representatives, recognizing the wealth of information that may be derived from data and the advantages of the ever-evolving technologies that the people are relying upon.[139] Under this bill, all government offices[140] are mandated to publish machine-readable datasets and publish the same for public access.[141]

Section 13 establishes the same guiding principles laid out by the Joint Memorandum Circular issued back in 2015.[142] For a dataset to be considered open, it must be "publicly available and accessible by default[,]"[143] "[t]imely and [c]omprehensive[,]"[144] "[a]ccessible and [u]sable[,]"[145] and "[c]omparable and [i]nteroperable."[146] The particular datasets that must be uploaded are laid down in Section 17.[147]

In essence, these standards reflect the same standards set forth by the Open Data Task Force since its establishment, as provided for under the 2014 and

138. Michael Canares, *South, East, & Southeast Asia*, *in* THE STATE OF OPEN DATA: HISTORIES AND HORIZONS 542 (Walker, et al. eds., 2019).

139. An Act Strengthening the Open Data Initiative of the Government, H.B. No. 7786, 18th Cong. 2d Reg. Sess. (2020). In the explanatory note, Representative Pablo John F. Garcia cites Section 7 of the Bill of Rights and Section 10 of Article XVI of the Constitution. PHIL. CONST. art. III, § 7 & art. XVI, § 10.

140. H.B. No. 7786, § 4.

141. *Id.* § 2.

142. *Id.* § 13.

143. *Id.* § 14 (a).

144. *Id.* § 14 (b).

145. *Id.* § 14 (c).

146. H.B. No. 7786, § 14 (d).

147. *Id.* § 17.

2015 executive issuances. There is likewise a provision on open licensing, which refers to the absence of restrictions as to the reuse of the dataset as long as the corresponding government agency is properly attributed.[148]

While it is commendable that such standards were set under the proposed bill, one problem remains unaddressed — the quality of the data. The value of an open data regime is always explained as one that is hinged upon the public's participation through the use of published data. This is why governments that have adopted policies of openness concretized by open data regimes are bent on releasing as many datasets, following the standards previously mentioned. However, open data is not just about opening any sort of data that is on hand; its essence lies in the quality of the datasets being released.[149]

The value of a strong open data regime depends on the quality of the datasets being made available. Unfortunately, this is not fully reflected in a lot of the open data work being done. Other than the fact that datasets uploaded before 2016 seem to have gone missing, the kinds of datasets uploaded in the online data portal are not all of high quality.

6. The Barrier of Form

The right to access information on matters of public concern has always been understood as subject to limitations imposed by law.[150] In *Valmonte v. Belmonte, Jr.*,[151] the Supreme Court categorically pronounced that a request for access to public records does not contemplate compelling the government to produce records in certain forms, such as "lists, abstracts, summaries, and the like[.]"[152] This ruling was affirmed in *Belgica v. Ochoa*,[153] where the petitioners requested for the list of lawmakers who made use of their Prior Development Assistance Funds, for whom and for what purpose those funds were spent, and all other related data thereto.[154] In denying this request, the Supreme Court clarified that

> *the denial* [ ] *only cover*[*s*] *petitioner's plea to be furnished with such schedule/list and report and not in any way deny them, or the general public, access to official documents*

148. *Id.* §15.

149. *See* Canares, *supra* note 138, at 538.

150. PHIL. CONST. art. III, § 7.

151. Valmonte v. Belmonte, Jr., G.R. No. 74930, 170 SCRA 256 (1989).

152. *Id.* at 272.

153. Belgica v. Ochoa, G.R. No. 208566, 710 SCRA 1 (2013).

154. *Id.* at 152.

> *which are already existing and of public record*. Subject to reasonable regulation and absent any valid statutory prohibition, access to these documents should not be proscribed.[155]

In light of this ruling, it appears that absent a clear mandate to release datasets of the government — or "government research data" in the words of the constitutional provision — in a particular prescribed form (i.e., machine-readable or processable), even an FOI request for the same may be denied. Such an interpretation is clearly contrary to the open data principle of accessibility, which requires datasets to be in a machine-readable format. A very important consideration of open data is quality data, which is affected by the handling of the data and the manner by which data is organized in the dataset.[156] If the government is not mandated to release, by law or by any legal force, public datasets in a certain form and format, the open data framework will not be the effective mechanism which it was originally intended to be.

D. Open Data and Research

One of the major moving forces in the rise of open data relates to research and development.[157] With more easily accessible and quality data, researchers are able to freely make use of public sector information and conduct their own analyses on the available data.[158] Again, while open data was originally intended for transparency and accountability, the more advanced open data regimes now expect economic growth and innovative developments to result from such disclosure.[159]

Using a similar perspective, it can be seen that in the Philippine Constitution, there are several provisions that make mention of the value of research and which are argued to provide support, albeit indirectly, for a stronger framework for open data beyond the right to information[160] and the

155. *Id.* at 153.

156. *See* Canares, *supra* note 138, at 538.

157. *See* Mohammad Alamgir Hossain, et al., *State-of-the-Art in Open Data Research: Insights from Existing Literature and a Research Agenda*, 26 J. ORGANIZATIONAL COMPUTING & ELECTRONIC COM. 14 (2016).

158. *See id.* at 14-15.

159. In the European Union, for example, the market derives significant value from Open Data. *See* Hossain, et al., *supra* note 157, at 23 (citing Stefan Kulk & Bastiaan van Loenen, *Brave New Open Data World?*, 7 INT'L. J. SPATIAL DATA INFRASTRUCTURES RES. 196, 203 (2012)).

160. PHIL. CONST. art. III, § 7.

State's policy on full public disclosure.[161] These include Article XII, Sections 5, 7, and 12,[162] and Article XIV, Sections 9, 10, 11, and 18 (2).[163]

Additionally, these provisions that mention "research" find more significance in the fact that in both the 1935 and 1973 Constitutions, "research" only appeared once.[164] In contrast, the 1987 Constitution references the term a total of 10 times.[165] From this, it can be inferred that the constitutional commissioners truly valued research when drafting the provisions relating to the different sectors. There is even a provision for fiscal incentives in support of research.[166]

When this understanding is coupled with the intent of the constitutional commissioners in including "government research data" in Section 7 of the Bill of Rights, i.e., to guard against the dangers similar to that present during martial law, the value of verification and replication of results cannot be denied.[167] This purpose is addressed by open data as an additional consideration beyond the usual transparency, accountability, innovation, and economic growth objectives.

III. OPEN DATA BEYOND PHILIPPINE BORDERS

A. International Covenant for Civil and Political Rights

The International Covenant for Civil and Political Rights (ICCPR) protects the right to information as a fundamental human right[168] under Article 19 (2), which states that "[e]veryone shall have the right to freedom of expression; *this right shall include freedom to seek, receive*[,] *and impart information* and ideas of

161. PHIL. CONST. art. II, § 28.

162. PHIL. CONST. art. XII, §§ 5, 7, & 12.

163. PHIL. CONST. art. XIV, §§ 9, 10, 11, & 18 (2).

164. *Compare* 1935 PHIL. CONST. art. XIII, § 4 (superseded in 1973), *with* 1973 PHIL. CONST. art. XV, § 9 (superseded in 1987).

165. *See* PHIL. CONST. art. III, § 7; art. XIII, §§ 5, 7, 12, 18 (5); & art. XIV, §§ 9, 10, 11, 18 (2).

166. *See* PHIL. CONST. art. XIV, § 11.

167. *See* BERNAS, *supra* note 62, at 381 (citing PHIL. CONST. art. III, § 7).

168. International Covenant on Civil and Political Rights art. 19 (2), *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171.

all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[169]

The Human Rights Committee (HRC) under the ICCPR clarified, "[t]o give effect to the right of access to information, States [P]arties should *proactively put in the public domain* [*g*]*overnment information of public interest*. States [P]arties should make every effort to *ensure easy, prompt, effective*[,] *and practical access to such information*."[170] This particular comment from the HRC clearly covers FOI. Of special import is its emphasis on FOI legislation as one of the means to provide access to information to the public and that it is the State as a whole, and not just any one branch of government that has the responsibility to disclose information on matters of public concern.[171] Significantly, the Committee recognizes the State's obligation to proactively disclose such information, which, as discussed previously, does not equate to the reactive disclosure of the usual FOI mechanisms.[172]

B. International Open Data Charter

The International Open Data Charter (ODC) is "a collaboration between over 150 governments and organi[z]ations working to open up data based on a shared set of principles."[173] The Philippines adopted the International ODC and sought to implement its principles under the third Open Government Partnership (OGP) National Action Plan.[174] The principles under the ODC are:

(a) "Open by Default"[175]

169. *Id.* (emphasis supplied).

170. Human Rights Committee, *General Comment No. 34*, ¶ 19, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011) (emphases supplied).

171. *See id.*

172. *Id.*

173. Open Data Charter, Who We Are, *available at* https://opendatacharter.net/who-we-are (last accessed July 31, 2022) [https://perma.cc/GMJ4-VH87].

174. Statement *by* Edwin Lacierda, Presidential Spokesperson, *On the Adoption of the Open Data Charter* (Oct. 19, 2015) (*available at* https://www.officialgazette.gov.ph/2015/10/27/statement-presidential-spokesperson-open-data-charter (last accessed July 31, 2022) [https://perma.cc/XVN8-XJP2].

175. Open Data Charter, Principles, pmbl. ¶ 10, *available at* https://opendatacharter.net/principles (last accessed July 31, 2022) [https://perma.cc/B2MV-E8C9].

(b) "Timely and Comprehensive"[176]

(c) "Accessible and Usable"[177]

(d) "Comparative and Interoperable"[178]

(e) "For Improved Governance & Citizen Engagement"[179]

(f) "For Inclusive Development and Innovation"[180]

Noticeably, the first four principles may sound very familiar, as these are the same standards used in defining Open Datasets under the 2014 and 2015 Joint Memorandum Circulars[181] and House Bill No. 7786.[182] However, it must be noted that the ODC is not a legal document from which obligations can be enforced.[183]

The principle "*Open by Default*" shifts the paradigm from reactive disclosure to a proactive disclosure mechanism, which operates under the "presumption of publication for all."[184] "*Timeliness and Comprehensiveness*" emphasizes the idea that much of Open Data's value is founded upon its relevance in relation to the time of its publication.[185] Otherwise, outdated data will not be very helpful, especially when decisions need to be made immediately. The comprehensive character of open data appears to encapsulate the original "*primary*" principle because "[a]s much as possible[,] governments should provide data in its original, unmodified form."[186] "*Accessibility and usability*" refer to the machine-readable format and licensing required to make data open.[187] "*Comparable and interoperable*" datasets are also important in order to derive more value and information, and this can be achieved through the establishment of uniform data standards with which

176. *Id.*

177. *Id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. *See* Jt. Memo. Circ. 2014-01, ¶¶ 14.1-14.3 & Jt. Memo. Circ. 2015-01, ¶¶ 5.1-5.4.

182. *See* H.B. No. 7786, § 2.

183. Open Data Charter, *supra* note 173.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

government agencies must comply.[188] The last two guiding principles direct that datasets must be used for improved governance, citizen engagement, inclusive development, and innovation,[189] which becomes even more manifest in the next subsections of this Note.

C. United States of America and the European Union

In 2009, President Barack H. Obama II issued two memoranda on his first day in office,[190] one of which promoted open government that is transparent, participatory, and collaborative.[191] The second memorandum concerned the Freedom of Information Act (FOIA).[192] By his second term beginning in 2013, machine-readable and open government information had already been made the default for government resources.[193] Thereafter, an OPEN Government Data Act founded upon the 2013 policy of President Obama was passed by the U.S. Congress.[194] This particular law set the standards for compliance with government datasets intended to be shared with the public.[195]

Turning the attention towards the European Union (E.U.) interestingly reveals through its issuances the high value they place upon opening data and allowing public access to government information. To the E.U., there must be minimum standards set for access regimes with which all Member States

188. *Id.*

189. Open Data Charter, *supra* note 173.

190. Wendy R. Ginsberg, The Obama Administration's Open Government Initiative: Issues for Congress (Congressional Report for Congress), at 1, *available at* https://sgp.fas.org/crs/secrecy/R41361.pdf (last accessed July 31, 2022) [https://perma.cc/6VRY-U4RA].

191. Transparency and Open Government, Memorandum of January 21, 2009, 74 Fed. Reg. 4685 (Jan. 21, 2009) (U.S.).

192. Ginsberg, *supra* note 190, at 1. *See also* Freedom of Information Act, Memorandum of January 21, 2009, 74 Fed. Reg. 4683 (Jan. 21, 2009) (U.S.).

193. Office of the President, Making Open and Machine Readable the New Default for Government Information, Executive Order No. 13642, Series of 2013 [E.O. 13642, s. 2013] (May 9, 2013) (U.S.).

194. Data Coalition, OPEN Government Data Act, *available at* http://web.archive.org/web/20220528185120/https://www.datacoalition.org/policy-issues/open-data/open-government-data-act.

195. Committee on Homeland Security and Governmental Affairs, S. Comm. Rep. No. 115-134, 115th Cong., 1st Sess., ¶ I (U.S.).

comply to support economic growth in the region.[196] Innovative services that are heavily reliant upon public sector information are of such importance that the Council of the E.U. found it necessary to harmonize the laws across the Union, in order to provide nondiscriminatory and efficient access. Data-driven services and projects are regarded highly, and the E.U. wanted to stimulate this market.[197] The 2019 Open Data Directive emphasized high-value datasets and dynamic data, provided transparency safeguards, and laid down limitations to exclusive data-sharing agreements with private entities.[198]

While the U.S. adopted open data from the viewpoint of transparency and accountability purposes,[199] the E.U. took to open data for economic gain.[200] This is clearly reflected by the policy and legal bases of the different documents issued for the implementation of Open Data. E.U.'s approach resulted in the steadily growing open data market size, with a forecast of €1.138 to €1.229 billion by 2020.[201] However, open data in E.U. is not without its own challenges, as national laws and policies in each E.U. Member State may vary, thereby affecting cross-border usage, in addition to technical issues on format and interoperability.[202]

Like its U.S. counterpart, the Directive "respects the fundamental rights and observes the principles recogni[z]ed in particular by the Charter [of Fundamental Rights of the European Union], including the right to privacy, the protection of personal data, the right to property[,] and the integration of persons with disabilities."[203]

196. Directive 2013/37 of the European Parliament and of the Council of 26 June 2013 on Amending Directive 2009/98/EC on the Re-Use of Public Sector Information, whereas cl. ¶ 2, 2013 O.J. (L 175) 1.

197. *See id.* whereas cl. ¶ 3.

198. *Id.*

199. *See* Transparency and Open Government, *supra* note 191.

200. *See generally* EUROPEAN DATA PORTAL, *supra* note 13.

201. EUROPEAN DATA PORTAL, ANALYTICAL REPORT 9: BENEFITS OF OPEN DATA 15 (2020).

202. MANUEL STAGARS, OPEN DATA IN SOUTHEAST ASIA: TOWARDS ECONOMIC PROSPERITY, GOVERNMENT TRANSPARENCY, AND CITIZEN PARTICIPATION IN THE ASEAN 47 (2016).

203. Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information, whereas cl. ¶ 71, 20139 O.J. (L 172) 56.

D. ASEAN

In 2012, there were barely any open data initiatives in Southeast Asian countries, such that when Indonesia and the Philippines began establishing their own open data regimes, the implementation was more focused on "data dumping," and not really on the publication of high-quality datasets.[204] And despite E.U.'s influence on the statistical framework of the Association of Southeast Asian Nations (ASEAN) Member States, there still exists a gap in relation to open data regimes because of historical differences and regional motivations.[205] Where E.U. nations decided to come together after many years of war, ASEAN States "band[ed] together more informally" because of the importance placed upon non-interference policies despite integration.[206] It has been observed that

> [*c*]*ommon laws for FOI or the reuse of PSI are missing in the ASEAN*, but several international initiatives outline rules for FOI. ... *However, the plan gives governments wide-ranging discretion and includes no binding obligations. Even though the principle of non-interference in domestic issues in the ASEAN has slightly softened since the beginning of the union, a legal framework for the entire union is difficult to install and monitor.*[207]

While the Philippines was one of the two pioneers of the Open Government Partnership in the region,[208] it is recognized that without a strong legal framework for open data, it will be difficult to prevent refusal to proactively disclose public sector information. In fact, democratic spaces play an important role in supporting open data and vice versa, because suppression of basic freedoms likewise suppresses the benefits that may be derived from open data.[209]

Clearly, compliance with the state policy of full public disclosure must not be left to the whims of whoever is seated in power. In the case of the Philippines, the Constitution itself has already declared the adoption of the state policy of full public disclosure of matters of public interest nature.[210] Clear standards must be set and complied with in order to prevent similar

204. Canares, *supra* note 138, at 536. *See also* Hossain, et al., *supra* note 157, at 21 (2016).

205. STAGARS, *supra* note 202, at 49.

206. *Id*. at 128.

207. *Id*. at 49 (emphases supplied).

208. Canares, *supra* note 138, at 542.

209. *Id*.

210. *See* PHIL. CONST. art. II, § 28.

instances of missing public datasets and to impose upon the government the duty to collect and make use of high-quality data for its own policymaking.

IV. OPEN DATA AND PRIVACY

As previously mentioned, this Note advocates for opening high-quality government data, which are granular in nature. However, in doing so, the government also runs the risk of "releas[ing] data [that] can reveal information about individuals that would otherwise not be public knowledge."[211] In fact, it is recognized that data utility and the privacy risk thereof

> are often in conflict because *less granular data protects privacy but is less valuable as an asset to promote transparency, enable innovation, and aid research.* Just as [*o*]*pen* [*d*]*ata is not valuable unless it is detailed, opening data will not be effective if it necessarily involves risks to individual privacy.*[212]

A. The Right to Privacy

Under the 1987 Constitution, the provisions that protect the right to privacy are found in Sections 2 and 3 of the Bill of Rights.[213] Section 3 expressly declares the right to privacy, which, more specifically, protects against unreasonable searches of communication and correspondences.[214] However, the landmark case of *Morfe v. Mutuc*[215] clarifies that the privacy protected in Section 3 is not limited to confidentiality of communications and correspondences.[216] Interestingly, this 1968 case already recognized the potential of modern technology to intrude upon privacy.[217]

In *Vivares v. St. Theresa's College*,[218] the Supreme Court explained that the right to privacy has three strands: (a) locational or situational privacy, (b) informational privacy, and (c) decisional privacy.[219] In this Note, resolving

211. Ben Green, et al., Open Data Privacy (Harvard Public Law Working Paper No. 17-07), at 4, *available at* http://nrs.harvard.edu/urn-3:HUL.InstRepos:30340010 (last accessed July 31, 2022) [https://perma.cc/6MTC-9S2P] [hereinafter Harvard Open Data Privacy Playbook].

212. *Id.* (emphases supplied).

213. PHIL. CONST. art. III, §§ 2-3.

214. BERNAS, *supra* note 62, at 217.

215. Morfe v. Mutuc, G.R. No. L-20387, 22 SCRA 424 (1968).

216. *See id.* at 444.

217. *Id.* at 445.

218. Vivares v. St. Theresa's College, G.R. No. 202666, 737 SCRA 92 (2014).

219. *Id.* at 111.

informational privacy concerns is the challenge because information pertaining to individuals that are generated or collected by the government will be made public when covered by Open Data. The right to control such information, particularly the details (or variables, in the case of a dataset) that lead to the identification of individuals, should be taken into account.

Previously, the Supreme Court ruled upon the constitutionality of the Anti-Graft and Corrupt Practices Act[220] and upheld the compelling interest of "promot[ing] morality in public administration by curtailing and minimizing the opportunities for official corruption and maintaining a standard of honesty in the public service."[221] In the same vein, this Note argues that Open Data, whether as a mere administrative policy, regulation, or statute, promotes transparency and accountability, drives innovation and economic growth, and advances the research landscape in the country. Such interests arguably mirror the compelling interest accepted by the Court in *Morfe*[222] and other jurisprudentially recognized interests. Open data is the tool by which these interests can be achieved, and provisions on the same subject must be narrowly drawn in order to successfully hurdle privacy questions.

When *Ople v. Torres*[223] was decided in 1998, no other laws could be referred to as providing sufficient protection or guidelines that would warrant upholding the administrative order.[224] Another important consideration is the absence of a penal provision, which could have possibly served as a deterrent to and punishment for the commission of acts that intrude upon privacy rights.[225] Notably, the President, in signing an executive issuance, is not capacitated to include such a penal provision in the administrative order, as Congress is the body that is empowered to penalize certain acts.[226]

The enactment of the Data Privacy Act, [227] almost a decade ago and several years after *Ople*'s promulgation, was intended to ensure the

220. Anti-Graft and Corrupt Practices Act, Republic Act No. 3019 (1960).

221. Ople v. Torres, G.R. No. 127685, 293 SCRA 141 (1998).

222. *Morfe*, 22 SCRA at 428.

223. *Ople,* 293 SCRA 141.

224. *Id.* at 165.

225. *Id.*

226. *Id.*

227. An Act Protecting Individual Personal Information in Information and Communications Systems in Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

confidentiality of data being collected in increasing volume as data breaches become more and more rampant.[228] The express affirmation of the state policy in Section 2 already recognizes that privacy must be protected without hampering innovation and growth, thereby acknowledging that information sharing produces value in society.[229]

The law covers the "processing of all types of personal information and [applies] to any natural and juridical person involved in personal information processing[.]"[230] To clarify, personal information is "any information ... from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[231] This means that any information that (a) directly identifies an individual or (b) makes such individual identifiable constitutes personal information.

It may be the case that for some datasets, the direct identifiers of their data subjects (e.g., name) have already been removed, but the information contained in the dataset may still be considered personal information because the data subjects remain identifiable, which calls into operation the application of the Data Privacy Act. Mere de-identification does not always operate to remove the personal information nature of the dataset.[232]

Contrast this with the privacy framework in the U.S. with respect to the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[233]

228. S. JOURNAL NO. 22, at 360-61, 15th Cong., 2d Reg. Sess. (Sept. 21, 2011).

229. Data Privacy Act of 2012, § 2.

230. *Id.* § 4.

231. *Id.* § 3 (g).

232. De-identification may be understood as "the process of removing or altering information, [e.g.,] deleting information that directly identifies individuals, such as names and addresses or dates of birth. Alternatively, it can mean reaching a state where individuals can no longer be 'reasonably identified' from the information." Office of the Victorian Information Commissioner, An Introduction to De-Identification, *available at* https://ovic.vic.gov.au/privacy/resources-for-organisations/an-introduction-to-de-identification (last accessed July 31, 2022).

233. An Act to Amend the Internal Revenue Code of 1996 to Improve Portability and Continuity of Health Insurance Coverage in the Group and Individual markets, to Combat Waste, Fraud, and Abuse in Health Insurance and Health Care Delivery, to Promote the Use of Medical Savings Accounts, to Improve

which is the basis of creating the HIPAA Privacy Rule on de-identification.[234] While HIPAA covers health information specifically,[235] the different standards imposed under HIPAA show an alternative approach to treating de-identified data.

Under HIPAA, protected health information is no longer included in the statute's scope after de-identification.[236] De-identification occurs in two instances: first, upon an expert determination that "the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information[ ]"[237] along with proper documentation of the analysis conducted;[238] and second, upon removal of the 18 identifiers listed[239] in the law so long as "[t]he covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify [the data subject.]"[240] These nuances in HIPAA differ from the privacy regime in the Philippines, in that once de-identified according to the standards set by law, data is no longer treated as personal information.

An evaluation of the prohibited acts under the Data Privacy Act of 2012 reveals that the acts contemplated pertain to instances where the data controller holds personal information or sensitive personal information.[241]

Access to Long-term Care Services and Coverage, to Simplify the Administration of Health Insurance, and for Other Purposes [Health Insurance Portability and Accountability Act of 1996], 110 Stat. 1936 (1996) (U.S.).

234. *See id.* §§ 261-262.

235. Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.514 (a) (as amended by Health Insurance Portability and Accountability Act of 1996) (U.S.).

236. *Id.*

237. *Id.* §164.514 (b) (1) (i).

238. *Id.* §164.514 (b) (1) (ii).

239. *Id.* §164.514 (b) (2) (i).

240. *Id.* § 164.514 (b) (2) (ii).

241. *See* Data Privacy Act of 2012, §§ 25-33. "Sensitive personal information," on the other hand, refers to personal information —

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to

Section 28, in particular, applies to any person, not just the known personal information controller or personal information processor,[242] who shall process personal data beyond the purposes made known to the data subject or that which is allowed by law.[243]

When government-held data is therefore made public with no restrictions as to reuse (as is the point of open data), what is really allowed is further processing in accordance with the principles of open data. Nevertheless, open data should not be used for nefarious purposes — such as the deliberate re-identification of the data subjects in an already de-identified dataset — which clearly and directly violates the privacy rights of individuals. Thus, while there may be privacy fears about releasing granular datasets such as the sample Department of Health (DOH) data drop, deliberate re-identification of the data subjects is what constitutes processing for unauthorized purposes.

B. The Re-Identification Problem

Mosaic effect "occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other

---

have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

Id. § 3 (l).

242. Data Privacy Act of 2012, § 3 (i) & (j).

> Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
>
> Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure[,] or destruction of data.

Id.

243. *Id.* § 28.

available information, could pose such risk."[244] While not yet a widespread phenomenon, there have been a number of instances of mosaicking in which privacy rights were involved.

The problem arises because the variables in a dataset can be used to identify the data subject with different levels of difficulty.[245] Some variables are direct identifiers[246] and some are indirect identifiers.[247] Publicly available datasets cannot contain direct identifiers, as this would be a clear violation of privacy. What is allowed in some States, however, is the publication of datasets after the removal (or use of other de-identifying techniques) of such variables.[248] The mosaic effect thus contemplates the re-identification of data subjects after de-identification.

In one instance, longitudinal[249] health data was published by the Australian federal health department for policy research purposes in 2016.[250] The dataset was already de-identified, but some researchers were able to show that the unencrypted parts of the data can be matched to an individual using other known information based on mundane facts.[251]

Notably, the data release in these scenarios was intended to satisfy economic and academic purposes, among others, which are in themselves not driven by malicious purposes. However, in the course of pursuing noble objectives, it is clear that the manner in which privacy rights are protected

244. Office of Management and Budget, Open Data Policy — Managing Information as an Asset, at 4, Memorandum No. 13 [M-13-13], at 4 (May 9, 2013) (U.S.).

245. Boris Lubarsky, *Re-Identification of "Anonymized Data"*, 1 GEO. L. TECH. REV. 202, 203 (2017).

246. Harvard Open Data Privacy Playbook, *supra* note 211, at 19-20.

247. *Id.* & Lubarksy, *supra* note 245, at 203. Indirect identifiers are sometimes referred to as quasi-identifiers. Harvard Open Data Privacy Playbook, *supra* note 211, at 20.

248. *See* Privacy of Individually Identifiable Health Information, § 164.514 (b) (2) (i).

249. "A dataset is longitudinal if it tracks the same type of information on the same subjects at multiple points in time." National Center for Analysis of Longitudinal Data in Education Research, What are Longitudinal Data?, *available at* https://caldercenter.org/what-are-longitudinal-data (last accessed July 31, 2022) [https://perma.cc/86R3-SK2H].

250. Vanessa Teague et al., Research Reveals De-Identified Patient Data Can Be Reidentified, *available at* https://phys.org/news/2017-12-reveals-de-identified-patient-re-identified.html (last accessed July 31, 2022) [https://perma.cc/4Y6C-L3K5].

251. *Id.*

must likewise evolve. The threat to privacy is real, but the value of open data should not be discounted outright because these risks exist. Otherwise, privacy concerns will always take the helm, and a conservative approach to this framework might just hinder society from benefitting from open data.

1. Preventive Measures

There are a number of tools available in order to de-identify data.[252] For direct identifiers, redaction and replacement are the main techniques used,[253] and for indirect identifiers, statistical noise and aggregation.[254] Unlike the first two techniques mentioned, statistical noise and aggregation can considerably weaken data utility because of the loss of information from the data.[255]

More advanced techniques other than the four mentioned exist.[256] Experts are continuously developing increasingly complex methods to prevent or lower the risk of the mosaic effect.[257] De-identification is not merely a matter of choosing which technique to apply; more often than not, the best possible approach is to use a combination of techniques in de-identifying the data while still preserving the quality of information.[258]

It is important to note that anonymized information is not covered by the Data Privacy Act.[259] However, it is easy to mistake anonymization for de-identification, which are actually different concepts. In de-identification, the identifying variables in the dataset are removed (e.g., name, social security number, and any other unique identifier of the data subject).

When one looks at the data alone, it would not be possible to identify particular individuals because the direct identifiers and indirect identifiers with outlying or unique values have been redacted. As for anonymization, the National Privacy Commission (NPC) follows the definition of anonymization adopted by the E.U. General Data Protection Regulation,[260] which requires

252. Lubarsky, *supra* note 245, at 205.

253. *Id.*

254. *Id.*

255. *See id.* at 207.

256. Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party of the European Commission, at 3 (Apr. 10, 2014).

257. *See id.* annex.

258. *Id.* at 23-25.

259. *See* Privacy Policy Office, Advisory Opinion No. 2017-27, at 1 (June 23, 2017).

260. *Id.*

that "data should be such as not to allow the data subject to be identified via 'all' 'likely' and 'reasonable' means."[261] Anonymization, therefore, partakes of a nature that is irreversible, both on the side of the third-party researcher and the original data holder.[262] In the country, the common way that this is made possible is through aggregation.[263]

Thus, when holders of data release de-identified datasets to the public, the security that privacy rights are protected is not actually at the same level as in the case of truly anonymized data. It is, therefore, not surprising for government agencies and public officials to be extremely wary of releasing datasets through the Open Data portal. To address this tension, datasets made available are usually aggregated. This method, in itself, is recognized as an acceptable way to secure irreversible anonymization; however, data utility takes a hit. This highlights the importance of striking a balance between the interests of privacy and the interest of disclosing information to the public for transparency, accountability, research, policymaking, and economic purposes.

Of course, the implementation aspect of balancing open data with the concomitant re-identification issue is a major concern for government, and the two are different but not altogether separate matters. The Harvard Playbook's practical recommendations[264] mirror the role played by Privacy Impact Assessments,[265] the establishment of Privacy Management

261. *Id.* (citing Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party of the European Commission, at 5.).

262. *Id. See also* Department of Health & National Privacy Commission, Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002 [Jt. Memo. Circ. 2020-0002], pt. IV (1) (Apr. 24, 2020). In this issuance, NPC first defined anonymization as "a process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party." Jt. Memo. Circ. No. 2020-0002, pt. IV (1).

263. *See* National Government Portal, *supra* note 25.

264. *See* Harvard Open Data Privacy Playbook, *supra* note 211.

265. *See* NPC Privacy Toolkit: A Guide for Management and Data Processing Officers, at 45-58, *available at* https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/3rdToolkit_0618.pdf (last accessed July 31, 2022) [https://perma.cc/P3TT-DUJD].

Programs,[266] and the strengthening of existing security measures[267] in the Philippine jurisdiction.[268]

Nevertheless, there must be a corresponding legal framework that addresses the issue of the mosaic effect after the fact. This is not to discount the significance of preventive measures in the execution; rather, on the legal front, data officers of the different government agencies must have a clear understanding of the existing framework for handling the mosaic effect.

2. Clarifying Prohibited Acts and the Penalty Provisions

In the U.K., there is an express provision prohibiting re-identification of data subjects.[269] One of the new offenses relating to personal data penalizes "a person [who] knowingly or recklessly [ ] re-identif[ies] information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data."[270] Defenses to such a charge are likewise provided for.[271] Further processing of the re-identified data is also not allowed "without the consent of the controller responsible for de-identifying the personal data, and (b) in circumstances in which the re-identification was an offence[.]"[272]

From this example, it can be seen that one way of addressing this issue is to criminalize the act of re-identification and use such re-identified datasets. However, the Author is of the view that the existing Data Privacy Act already covers re-identification under Section 28, which penalizes the processing of personal data for unauthorized purposes.[273] In the context of Open Data, datasets are made available for reuse without restriction; nonetheless, it should be understood that the re-identification of data subjects remains to be an

266. *Id.* at 59-61.

267. *Id.* at 97.

268. These are three of the five pillars of compliance according to the National Privacy Commission. *See id.* ch. 2, 23-141.

269. An Act to Make Provision for the Regulation of the Processing of Information Relating to Individuals; to Make Provision in Connection with the Information Commissioner's Functions Under Certain Regulations Relating to Information; to Make Provision for a Direct Marketing Code of Practice; and for Connected Purposes [Data Protection Act 2018], § 171 (2018) (U.K.).

270. *Id.* § 171 (1).

271. *Id.*

272. *Id.* § 171 (5).

273. Data Privacy Act of 2012, § 28.

unauthorized purpose. It is also recognized that re-identification can just be a preparatory step before further action is taken upon or further processing is applied to the re-identified data. In the Philippine framework, this will still fall under processing for unauthorized purposes.[274]

However, unlike its U.K. counterpart, the Data Privacy Act provides no defenses similar to those indicated in the U.K. Data Protection Act.[275] The only way to escape liability is to prove that the processing aligns with the purpose declared to the data subject or with some statutory provision allowing it.

Some experts warn of the chilling effect that criminalization brings.[276] In Australia, specifically, there had been talks in parliament about expressly criminalizing re-identification, but the proposed bill on the matter was perceived to be detrimental to research on cybersecurity.[277]

These are, indeed, valid concerns, but the solution is to declare the purpose of the re-identification attempt to the proper authorities and to the stakeholders. Of course, this presupposes that the government agency involved followed security protocols prior to releasing the dataset in order that no administrative liability attaches. It is necessary to make accommodations for public interest research on this matter because re-identification techniques can only grow increasingly more complex with the development of technology. Thus, it is just as important for experts and researchers to freely test datasets and de-identification techniques in order to respond to such advancements accordingly.

Risk management must guide the data throughout its life cycle, from collection of information from the data subject up to the disclosure of the dataset as open data. The Data Privacy Act of the Philippines is not inadequate in addressing the mosaic effect. However, the law must not also be used as a shield against releasing primary data in fear of violating the privacy statute. This delicate balancing act will not be addressed by legislating an express prohibition on re-identification but by the *proper handling of data in all stages*.

---

274. *See id.*

275. *See* Data Protection Act 2018, § 171.

276. Teague, et al., *supra* note 250.

277. Jessica Clarence, Anonymous No More? Make It a Crime to Re-Identify Personal Data, *available at* https://www.aspistrategist.org.au/anonymous-no-more-make-it-a-crime-to-re-identify-personal-data (last accessed July 31, 2022) [https://perma.cc/87E5-MGUE].

From the open data perspective, government agencies should likewise take caution not to fall into the trap of being too conservative. Just because aggregation satisfies the true anonymization standard and ensures no liability, this does not mean that all datasets must be aggregated for supposed full compliance with open data and privacy standards. The inverse relationship between data utility and privacy risk has already been established and cannot be contradicted. Finding the middle ground in this spectrum requires careful evaluation of risks and keeping in mind the purpose for which publication is being done.

3. Duty to Report

Under the Data Privacy Act, there is an obligation to notify the National Privacy Commission of any breach of personal data.[278] However, consider the situation of an innocent data user who makes use of available open data from several agencies or other data sources and, after linking them together, inadvertently re-identifies any of the data subjects. In such a case, there was no intent to re-identify at all. Should this already be categorized as penalized re-identification?

In the view of the Author, inadvertent or unintentional discoveries of re-identification should not be penalized as a "breach" under or a violation of the Data Privacy Act. While the Data Privacy Act is a special law, in which case, violations are treated as *mala prohibita* and therefore do not account for criminal intent in theory,[279] the better approach is to instead impose on the individual the duty to report this finding. It is not a "breach" as understood in the context of the provisions of the Data Privacy Act, but the infringement partakes of the same nature. In imposing the duty to report, the authorities will be alerted accordingly, and remedial measures may be taken to address the privacy risk as soon as possible.

Should the discoverer be immediately treated as a malicious re-identifier, it is highly likely that no inadvertent discovery will be reported, and the danger to privacy remains unaddressed. What should be penalized instead is the concealment of such discovery. Thus, in a scenario where an individual interested in studying multiple datasets combines such datasets and discovers a risk of re-identification, there must be a compelling legal mechanism to report the matter.

278. Data Privacy Act of 2012, § 20 (f).

279. LUIS B. REYES, THE REVISED PENAL CODE: BOOK ONE 52 (2017).

4. The Principles of Transparency, Legitimate Purpose, and Proportionality

Recall that Section 11 of the Data Privacy Act mentions three valuable principles to be adhered to when personal information is being processed.[280] These same principles are just as crucial in handling open data and are similar to the recommended actions found in the Harvard Open Data Playbook.[281]

As to *transparency*, government agencies must always be transparent about the data that will be made available to the public. It matters to the people how personally identifiable information was deleted, anonymized, or pseudonymized. Other measures adopted to secure data privacy throughout the life cycle of the data will be informative to the public and can help increase awareness of the people as to the value of open data that does not set aside privacy concerns.

With regard to *legitimate purpose*, it has been previously mentioned that open data is not merely publishing any and all de-identified data in the hands of the government. Such action will be meaningless and will unnecessarily shift the focus away from the publication of high-value datasets (from which the most utility can be derived) to a race to publish the greatest number of datasets (without accounting for the dataset's potential to be useful). For the Open Data Institute (ODI), this translates to the call for government agencies to "publish with purpose," which was the 2018 strategy adopted by the Open Data Charter.[282]

Finally, *proportionality* in the sense of open data can translate to government agencies figuring out which variables are necessary for the purpose for which the data is being published. A more proactive approach is to decide on priority concerns in various sectors in order that datasets are intentionally curated and data purposefully collected in proportion to what is necessary to address these priority concerns.

These three principles were primarily understood from the perspective of processing personal information, but they likewise provide guidance in terms of open data management.

280. Data Privacy Act of 2012, § 11.

281. *See* Harvard Open Data Privacy Playbook, *supra* note 211.

282. Calderon, *supra* note 21.

V. LIBERTY OF PRIVACY, PROSPERITY IN INFORMATION, & THE RULE OF LAW

A. Legal Foundations of Open Data

In legal theory, open data is closely understood with FOI, but a deeper understanding of government disclosure reveals certain nuances.[283] In the Philippines, FOI has been operationalized in the executive branch, but there is yet a law on the subject as FOI bills continue to languish in Congress.[284]

FOI is grounded upon Section 7 of the Bill of Rights[285] and has since been affirmed by the Supreme Court as a self-executory provision in several cases.[286] Analysis of jurisprudence reveals the Supreme Court's view on the symmetrical relationship between the right to information and the policy of full public disclosure pronounced in Section 28 of Article 2.[287] In fact, the deliberations of the framers of the Constitution reveal their intent to adopt a proactive disclosure mechanism, which is incidentally similar to open data as regards some of its principles, despite the fact that the concept of open data as understood today had not yet been fully comprehended at that time.[288]

The point of taking this perspective in law finds significance in the fact that FOI has its own limitations.[289] While the Supreme Court will uphold the right when properly invoked, the same cannot be used to require a particular form for the requested information, contrary to the concept of open data.[290]

The deliberations of the Constitutional Commission also support the view that the framers had contemplated two ideas: *first*, to make government datasets available to the people as a check on the government's decision-making,[291] and *second*, to force the government to make disclosures

283. This was discussed in detail in Chapter II of this Note.

284. *See* S.B. No. 324; S.B. No. 1673; S.B. No. 511; S.B. No. 795; S.B. No. 265; S.B. No. 121; S.B. No. 606; & H.B. No. 7786.

285. PHIL. CONST. art. III, § 7.

286. *Legaspi*, 150 SCRA at 534.

287. PHIL. CONST. art. II, § 28.

288. 5 RECORD, PHIL. CONST., NO. 91, at 26-28.

289. *See* E.O. No. 2, s. 2016, § 4 & Office of the President, Inventory of Exceptions to Executive Order No. 2, series of 2016 [E.O. No. 2, s. 2016], Memorandum from the Executive Secretary (Nov. 24, 2016).

290. *Valmonte*, 170 SCRA at 272.

291. *Id.* at 24.

proactively, without need for request unlike in the reactive disclosure mechanism of the right to information as presently implemented.[292] These intentions are well-supported by open data. Conversely, they are argued to give rise to a different legal basis for open data. The principles of transparency and accountability underlying Section 28, Article II are unarguably cornerstones of a healthy democracy, both of which are fully supported by open data.

Another approach that is well-taken is understanding the constitutional provisions that make mention of research and its value in community development as further support for open data.[293] This is not a logical leap to make because open data was conceptualized in the context of scientific research in the first place.[294] Thus, a contemporary appreciation of these lesser-known provisions that refer to research is argued to add support for the legal foundation of open data. In fact, a comparison of the provisions in the current and previous versions of the Constitution reveals that from just one express mention of "research" under the 1935[295] and 1973[296] Constitutions, the 1987 Constitution uses it a total of 10 times.[297] It can be inferred that this change indicates the framers' understanding of the true value of research in society's way forward. Open data is one way to give effect to these provisions.

This Note offers a novel and deeper understanding of open data with the hope that a legal perspective on the matter will pave the way to achieve the vision of the framers of the Constitution in regard to transparency and accountability in public service. The Author endeavored to establish a legal basis to argue in favor of an open data regime beyond what is being implemented in the Philippines now. When viewed as a matter that furthers the constitutional mandate regarding the state policy of full public disclosure, open data finds support beyond policy considerations, which would otherwise be subject to the whims or policy priorities of the reigning administration

292. *See id.* at 27.

293. *See* PHIL. CONST. art. XII, § 5; art. XII, § 7; art. XII, § 12; art. XIV, § 9; art. XIV, § 10; art. XIV, § 11; & art. XIV, § 18 (2).

294. Harlan Yu & David G. Robinson, The New Ambiguity of Open Government, 59 UCLA L. REV. DISC. 178, 189 (2012).

295. 1935 PHIL. CONST. art. III (superseded in 1973).

296. 1973 PHIL. CONST. art. III (superseded in 1987).

297. PHIL. CONST. art. XII, § 5; art. XII, § 7; art. XII, § 12; art. XIV, § 9; art. XIV, § 10; art. XIV, § 11; & art. XIV, § 18 (2).

absent a clear understanding that it likewise finds legal basis in the fundamental law of the land.

B. Open Data in the Philippine Legal Framework

Central to this Note is understanding open data not merely as a policy of full disclosure[298] from which society can benefit but also as an extension of the right to information, which is protected by the Constitution.[299] In the first place, established open data regimes began with FOI legislation, and privacy and open data frameworks followed.

The right to access information on matters of public concern has always been subject to limitations set forth by law.[300] In *Valmonte v. Belmonte, Jr.*, the Supreme Court categorically pronounced that a request for access to public records does not contemplate compelling the government to produce records in certain forms.[301] In this light, government datasets may not be required to follow a specific form as well. Such an interpretation is clearly contrary to the open data principle of accessibility, which requires datasets to be in a machine-readable format. A very important consideration of open data is quality data, which is affected by the handling of the data and the manner in which data is organized in the dataset. If the government is not mandated to release public datasets in a certain form and format, the open data framework will not be the strong and effective proactive disclosure mechanism it was originally intended to be.

Thus, legislation affecting open data principles is but a timely response to solidify the open data framework in the Philippines and resolve the challenges on form and format which arise from the Court's interpretation in *Valmonte*.

Privacy is another major concern in opening government data, especially for datasets involving information on individual persons. However, this Note has clarified that a balancing act must be done in order to uphold both the right to privacy and the right to information. At present, there may be many fears to be allayed about opening data that could possibly and unknowingly be violative of the Data Privacy Act; but this is where the legal understanding of open data enters the picture. As against an underlying purpose of promoting transparency and accountability in government, which is founded upon a

298. PHIL. CONST. art. II, § 28.

299. PHIL. CONST. art. III, § 7.

300. PHIL. CONST. art. III, § 7.

301. *Valmonte*, 170 SCRA at 272.

proclaimed state policy on full disclosure, open data can no longer be set aside nor merely substantially complied with so easily.

One such concern that heightens privacy risks to people is the matter of re-identification of already de-identified open datasets.[302] While other jurisdictions have contemplated and enacted statutes expressly criminalizing this act of violation of privacy,[303] a review of the Philippines' Data Privacy Act shows no need for another penal prohibition. Section 28, which penalizes processing for unauthorized purposes,[304] is broad enough to cover the re-identification concern as further processing that is not allowed under the law. The only nuance that needs further interpretation by the NPC, if not an additional statutory provision, is the matter of an inadvertent discovery of re-identification from the combination of two or more datasets. In this sense, the status quo understanding of the penal provision arguably affects unintentional acts, which ordinarily would not matter in special penal laws of a *mala prohibita* character.[305] Instead, what is recommended is an imposition of a statutory duty to report such discovery within a reasonable time to prevent the dangers that the privacy law protects against.[306]

Ultimately, this balancing act presupposes that proper de-identification techniques have been applied prior to the release of the dataset. An open data regime, which is characterized by the release of what has been referred to in this Note as meaningful open data, has the potential to infringe upon informational privacy rights without the proper safeguards. What this Note seeks to establish is an approach that strikes a balance. Otherwise, proactive disclosure through open data will not be realized should a privacy regime be interpreted so conservatively. In this light, lessons can be learned from other jurisdictions that have more advanced legal frameworks in dealing with open data and data privacy, especially with respect to the techniques that may be applied, the acceptable level of risks for different datasets, and how liability attaches.

Thus, in legislating on open data, several modifications to the currently pending House Bill No. 7786 are proposed in accordance with the discussions

302. *See e.g.*, Teague, et al., *supra* note 250.

303. *See e.g.* Data Protection Act 2018, § 171 (U.K.).

304. Data Privacy Act of 2012, § 28.

305. REYES, *supra* note 279, at 52.

306. In one article, it was observed that "[t]here is no duty to report if data has been re-identified." Lubarsky, *supra* note 245, at 213. This observation was the springboard for the recommendation on the duty to report, mirroring the notification requirements under the Data Privacy Act of 2012.

of this Note.[307] It is likewise recommended that the NPC and the PSA coordinate with each other in issuing a memorandum providing guidance to all government agencies on the proper de-identification techniques for open data. PSA's expertise on matters of handling voluminous and granular data will aid government agencies in applying similar treatment to their own datasets, with due respect to the *primary* requisite and without offending privacy rights.

C. Recommendations

1. Institutionalizing Open Data via Legislation

i. Criteria for Open Data

The recently filed bill on open data presents a way to institutionalize it in government.[308] However, the principles of open data provided in Section 14 prove to be lacking.[309] The provision is reproduced below —

> Section 14. Criteria for a Dataset to be Considered Open — For a government dataset to be considered open, it must possess the following:
>
> (1) Publicly available and accessible by default. If the dataset qualifies for publication to the extent permitted by applicable laws and subject to individual privacy, confidentiality, national security, or other legally-mandated restrictions, it should be available through the national government portal and the agency's website by default and obtainable through download[;]
>
> (2) Timely and Comprehensive. Each dataset shall be updated to ensure its quality and to preserve its value. All datasets must be updated at least once every quarter of the year, or whenever possible or permissible;
>
> (3) Accessible and Usable. Each dataset must be platform-independent, machine-readable, and free of restrictions that would impede the re-use, modification, or processing of the information it contains. Datasets in machine-readable formats shall have data that can be extracted and processed by computer programs easily; and
>
> (4) Comparable and Interoperable. Each dataset shall be easy to compare within and between sectors, across geographic locations, and over time. All datasets must be presented in structured and standardized formats to support interoperability, traceability, and effective reuse.

307. *See* Annex.

308. H.B. No. 7786.

309. *See id.* § 14.

> It shall be understood that a government dataset uploaded in the government Open Data portal is to be used for improved governance and citizen engagement as well as for inclusive development and innovation.[310]

Comparing this provision with the applied open data principles in the U.S. shows that it lacks the principles that open data must be complete, described, and managed post-release.[311]

Completeness appears to be dismissed quite easily from a data privacy lens because this principle requires that the datasets are "published in primary forms (i.e., as collected at the source), with the finest possible level of granularity that is practicable and permitted by law and other requirements."[312] Additionally, when aggregated data is released instead of primary data, the released dataset "must reference primary data."[313] This principle is one of the pillars of open data. As reiterated in this Note, the level of granularity of the datasets affects the value and volume of information derived from it.[314] While there is value in presenting summary statistics to the public for ease of understanding, primary data must not be discounted and should instead be the foremost consideration from the perspective of government under open data regimes; thereafter, other legal restrictions, e.g., privacy, may be addressed through the application of proper techniques.

The spectrum in which open data and data privacy lie needs a fulcrum that government must take pains to keep balanced. Privacy must not stifle full disclosure of public sector information, but open data should also not dismiss valid privacy issues. The scales can only be stabilized if both ends are treated not as directly opposing or competing rights and policies but as important considerations in improving transparency, accountability, and even economic growth.

A *described* open data simply refers to the requirement of providing metadata or data about the data.[315] In most cases, datasets are coded or codenamed for convenience, and without this metadata providing a clear description of what the data contains, potential users of the data will not understand, if not misunderstand, the data. Finally, *managing datasets post-release* can be executed through a complaint resolution mechanism for open

310. H.B. No. 7786, § 14.

311. *See* Jt. Memo. Circ. No. 2015-01, ¶ 8. *See also* M-13-13, at 5 (U.S.).

312. M-13-13, at 5 (U.S.).

313. *Id.*

314. Harvard Open Data Privacy Playbook, *supra* note 211, at 9.

315. Jt. Memo. Circ. 2015-01, ¶¶ 8 & 9.2.

datasets[316] or, further, an opportunity to manage the privacy risk of re-identification as more and more datasets are released over time.

Despite the government's ongoing efforts on open data, there is still merit in a legislative enactment on open data in order to strengthen the principles of transparency and accountability in government. At best, policies, including the priority accorded to such policies, may be changed from administration to administration.[317] Therefore, having a statute that protects against these occurrences and further recognizing the research provisions in the Constitution as support or basis for open data apart from the right to information on matters of public concern will firmly establish and further solidify open data in government.

Thus, the Author recommends the incorporation of these principles in an Open Data law. The provisions may be drafted as follows —

> Section XX. Criteria for Open Data. Government-held datasets made available through Open Data shall adhere to the following requirements:
>
> (1) Open by Default. When not otherwise prohibited by law, and to the extent practicable, public data assets maintained by the government shall be platform independent, machine-readable, and available under an open license.
>
> (2) Primary and Complete. Datasets must be published in primary forms, with the finest possible level of granularity that is practicable and permitted by law. Whenever necessary, aggregate data may also be published but shall reference the primary data.
>
> (3) Accessible and Usable. Each dataset shall be made available in convenient, modifiable, and open formats that can be retrieved, downloaded, indexed, and searched. Formats should be machine-readable. Open data structures shall not discriminate against any person or group of persons and should be made available to the widest range of users for the widest range of purposes by providing the data in multiple formats for consumption. To the extent permitted by law, these formats should be non-proprietary, publicly available, and no restrictions should be placed upon their use.
>
> (4) Timely and Comprehensive. Each dataset shall be updated as quickly as necessary to ensure its quality and to preserve its value. The frequency of release should account for the needs of the stakeholders.

316. *Id.* ¶ 8.3 & M-13-13, at 5 (U.S.).

317. *See* Alana Maurushat, et al., *Open Data: Turning Data into Information, and Information into Insights that Allow for Evidence-Based Policy*, 12 NEWCASTLE L. REV. 104, 123 & 125 (2017).

> (5) Comparable and Interoperable. Each dataset shall be easy to compare within and between sectors, across geographic locations, and over time. All datasets must be presented in structured and standardized formats to support interoperability, traceability, and effective reuse.

In the pending House Bill on open data, the primary requirements for datasets to be opened are the following: (a) "Publicly available and accessible by default[;]"[318] (b) "Timely and Comprehensive[;]"[319] (c) "Accessible and Usable[;]"[320] and (d) "Comparable and Interoperable."[321] Under the proposal, an added requirement is that the dataset must be Primary and Complete as well. Following the recognized principles under the Open Data Charter, it appears that the House Bill is already compliant with requirements (a) to (d). However, as discussed in this Note, *meaningful open data* cannot sacrifice the quality of the data, which inevitably brings to the discussion the quality and types of data being made available to the public. Hence, the addition of the principle under the proposal that "[d]atasets must be published in primary forms, with the finest possible level of granularity that is practicable and permitted by law. Whenever necessary, aggregate data may also be published but shall reference the primary data."[322] The rest of the principles are substantively similar to those proposed in the House Bill, but the description of each follows instead the explanations provided in the 2013 Memorandum on the Open Data Policy of the U.S. (2013 Memorandum on Open Data), which tackled how the Federal Government endeavored to manage information as an asset.[323] Notably, the Memorandum is merely an executive issuance, but the details of its contents and the technical knowledge required to come up with the same reveal how advanced of an understanding of open data already persisted years ago in the U.S. In fact, the Memorandum was issued jointly by the Director of the Office of Management and Budget, the Federal Chief Information Officer, the U.S. Chief Technology Officer, and the Acting Administrator of the Office of Information and Regulatory Affairs.[324] Thus, the Memorandum still provides ample guidance to proposed legislation on open data, especially with respect to open data principles.

318. H.B. No. 7786, § 14 (a).

319. *Id.* § 14 (b).

320. *Id.* § 14 (c).

321. *Id.* § 14 (d).

322. M-13-13, at 5 (U.S.).

323. *Id.* at 1.

324. *Id.*

ii. Metadata

> Section XX. Metadata. Each dataset shall have a corresponding metadata that provides contextual information on the dataset, in compliance with best practices on Open Data.

The basis for this second proposal on metadata is found in Joint Memorandum Circular No. 2015-01, which provided the guidelines for the Implementation of the Open Government Data General Provision in the 2015 General Appropriations Act.[325] In the Philippines, metadata was already viewed as an important consideration in an open data regime by then, that the Open Data Task Force even recognized that "[e]ach dataset shall have corresponding metadata[,]"[326] and prescribed specific metadata standards.[327] Two years earlier, the 2013 Memorandum on Open Data of the U.S. already provided a policy requiring the —

> [u]se [of] common core and extensible metadata — Agencies must describe information using common core metadata, in consultation with the best practices found in Project Open Data, as it is collected and created. Metadata should also include information about origin, linked data, geographic location, time series continuations, data quality, and other relevant indices that reveal relationships between datasets and allow the public to determine the fitness of the data source. Agencies may expand upon the basic common metadata based on standards, specifications, or formats developed within different communities (e.g., financial, health, geospatial, law enforcement). Groups that develop and promulgate these metadata specifications must review them for compliance with the common core metadata standard, specifications, and formats.[328]

The specific metadata standards may be fully threshed out in the Implementing Rules and Regulations instead, but the above-cited provision can serve as guidance.

iii. Data Management and Release

> Section XX. Data Management and Release. To ensure that data assets are managed and maintained throughout their life cycle, government agencies

325. Jt. Memo. Circ. 2015-01, ¶¶ 8.2 & 9.2.

326. *Id.* ¶ 9.2.

327. *Id.* ("Agencies that have not yet adopted any metadata standard shall adopt the JavaScript Object Notation (JSON) schema unless particular datasets require another standard. However, metadata of datasets published through data.gov.ph shall use the JSON schema.").

328. M-13-13, at 7 (U.S.).

> shall adopt effective data asset portfolio management approaches. Within six months from the date of effectivity of this law, agencies must review and where appropriate, revise existing policies and procedure to strengthen data management and release practices which include but are not limited to the following —
>
> (1) Creating and maintaining an enterprise data inventory;
>
> (2) Creating and maintaining a public data listing;
>
> (3) Establishing a process to facilitate and prioritize data release; and
>
> (4) Clarifying roles and responsibilities for efficient and effective data release practices.

Next is a provision on data management and release, which also finds basis in the 2013 Memorandum on Open Data.[329] This provision requires full maintenance of datasets from collection or generation up to their use, archiving, or destruction, if necessary.[330] There is likewise a time limit adopted, which provides a deadline for government offices to strengthen their respective data management and release practices. An enterprise data inventory refers to an inventory "that accounts for datasets used in the agency's information systems[,]"[331] which

> will be built [ ] over time, with the ultimate goal of including all agency datasets, to the extent practicable. The inventory will indicate, as appropriate, if the agency has determined that the individual datasets may be made publicly available (i.e., release is permitted by law, subject to all privacy, confidentiality, security, and other valid requirements) and whether they are currently available to the public.[332]

In building this inventory, there is already a determination of which datasets are to be opened by the government. Thus, the public officer or officers must be capacitated with the legal, technical, and technological knowledge necessary to handle the inventory. The public data listing is the list of datasets that can be made public. [333] Of course, improving efficiency in engaging with the public and with

---

329. *Id.* at 8-9.

330. *See id.*

331. *Id.* at 8.

332. *Id.*

333. *Id.* This should include datasets that can be made publicly available but have not yet been released. This public data listing should also include, to the extent permitted by law and existing terms and conditions, datasets that were produced through agency-funded grants, contracts, and cooperative agreements (excluding

other government agencies must also be given attention, hence the items listed as (c) and (d) in the proposed provision.[334]

iv. Post-release Management

> Section XX. Post-release Management. The government agency in charge of maintaining the dataset shall designate a point of contact to assist with the data use and to respond to complaints about adherence to the [o]pen [d]ata requirements.

And as a final addition, the above provision makes reference to managing the datasets post-release.[335] Datasets must be given ample attention in every stage of its life cycle. Open data does not end with the fact of releasing data but must be geared towards continuous improvement. This can be done by engaging the public and responding to clarifications, inquiries, or complaints to better the services based on user and stakeholder feedback. Building and strengthening open data regimes cannot be done by the government alone; the public must participate to be empowered by this democratic system. In response, the State must be capable of addressing issues and feedback provided.

v. Imposition of Administrative Liabilities

Instead of a blanket criminal provision as provided in the bill,[336] the Author recommends the provision for administrative liabilities for public officers who do not comply with the prevailing open data standards. As the bill currently stands, the applicable penalty provision is Section 21 on violations, which imposes a penalty of "imprisonment ranging from six (6) months to three (3) years and a fine of not less than Two hundred thousand (₱200,000.00) but not more than One million pesos (₱1,000,000.00)."[337] In removing the criminal liabilities, it is hoped that public officers take a more proactive and less conservative approach to opening data instead of hiding behind the curtain of the Data Privacy Act to defeat a claim for disclosure.

> any data submitted primarily for the purpose of contract monitoring and administration), and, where feasible, be accompanied by standard citation information, preferably in the form of a persistent identifier.
>
> M-13-13, at 8 (U.S.).

334. M-13-13, at 9 (U.S.).

335. *See id.* at 5.

336. H.B. No. 7786, § 21.

337. *Id.*

vi. Duty to Report

Furthermore, after concluding that the Data Privacy Act sufficiently covers re-identification under its penal provisions,[338] the law on open data can instead carve out the exception of inadvertent or unintentional re-identification and provide for the duty to report the same to the corresponding government agency. Thus —

> Section XX. Duty to Report. Any person who discovers or becomes aware of any re-identification of individuals in a dataset shall make a report thereof to the government office which released the data within seventy-two (72) hours upon knowledge thereof.

The time frame indicated in the proposed provision was patterned after the breach notification procedure under the Data Privacy Act,[339] which is considered by the Author as a reasonable time to notify the corresponding government agency that released the dataset.

As previously discussed, there is no need to amend the Data Privacy Act of 2012 because the coverage of the law's penal provisions encompasses the data privacy violations that can happen in the case of reidentification.

2. NPC Circular on De-Identification

As the central statistics authority in the country,[340] the PSA is armed with the technical expertise to deal with anonymization and screening of identifiers, among other techniques. Thus, PSA should coordinate with the NPC in issuing a memorandum providing guidance to all government agencies on the proper de-identification techniques for open data. It is acknowledged that the expertise of PSA on matters of handling voluminous and granular data will aid government agencies in applying similar treatment to their own datasets, with due respect to the primary requisite and without offending privacy rights.

In one memorandum circular issued jointly with the Department of Health, the NPC stated that "[o]nly aggregate health information or pseudonymized or anonymized detailed health information shall be shared by public health authorities to stakeholders for the purpose of business

338. *See* Data Privacy Act of 2012, § 28.

339. Rules and Regulations Implementing the Data Privacy Act of 2012, rule IX, § 38.

340. An Act Reorganizing the Philippine Statistical System, Repealing for the Purpose Executive Order Numbered One Hundred Twenty-One, Entitled "Reorganizing and Strengthening the Philippine Statistical System and for Other Purposes" [Philippine Statistical Act of 2013], Republic Act No. 10625, § 5 (2013).

intelligence and policy and biomedical researches."[341] This is the only circular of the NPC that acknowledges the de-identification techniques of pseudonymization and anonymization in order that health information may be released for research purposes. In the same manner, it is recommended for NPC to confer with PSA in releasing a similar circular to provide guidelines for other acceptable de-identification techniques such as noise addition, permutation, differential privacy, k-anonymity, l-diversity or t-closeness, among others.[342] Even authorities in the E.U. already recognize that residual risk will always be present,[343] and what data privacy authorities must monitor is the management of such risk.

While the HIPAA rule on the deletion of the 18 identifiers provided in the law for purposes of arriving at a de-identified dataset is sufficient compliance under U.S. Law,[344] the second option of getting expert determination that the privacy risk is minimal[345] is the more well-taken approach in this jurisdiction. PSA's expertise in data handling, management, and analysis will be instrumental in such determination, which may be case-by-case, and in the future, may be extended to other professionals who may contribute to such a determination.

An additional standard that the NPC may consider is the Motivated Intruder Test. In the U.K., the appeals relating to FOI and data privacy issues are tested against this standard.[346]

> The 'motivated intruder' is taken to be *a person who starts without any prior knowledge but who wishes to identify the individual from whose personal data the anonymi[z]ed data has been derived*. This test is meant to assess whether the motivated intruder would be successful.
>
> The approach assumes that the 'motivated intruder' is *reasonably competent, has access to resources such as the internet, libraries, and all public documents, and would employ investigative techniques such* as making enquiries of people who may have additional knowledge of the identity of the data subject or advertising for anyone with information to come forward. The 'motivated

341. Jt. Memo. Circ. 2020-0002, pt. VI (F) (1).

342. Opinion 05/2014 on Anonymisation Techniques, *supra* note 256, at 3.

343. *Id.* at 3-4.

344. Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.514 (b) (2) (i).

345. *Id.* §164.514 (b) (1).

346. Information Commissioner's Office, Anonymisation: Managing Data Protection Risk Code of Practice, at 22, *available at* https://ico.org.uk/media/1061/anonymisation-code.pdf (last accessed July 31, 2022) [https://perma.cc/TSU5-2LT7].

> intruder' is *not assumed to have any specialist knowledge such as computer hacking skills*[,] *or to have access to specialist equipment, or to resort to criminality*[,] such as burglary, to gain access to data that is kept securely.
>
> ...
>
> The 'motivated intruder' test is useful because it sets the bar for the risk of identification higher than considering whether a 'relatively inexpert' member of the public can achieve re-identification, but lower than considering whether someone with access to a great deal of specialist expertise, analytical power or prior knowledge could do so.[347]

It is submitted that this standard can be used for government agencies and public officials assigned or required to prepare government datasets for public release. Complying with this standard, therefore, becomes a clearer threshold for determining administrative liability. In other words, due diligence in de-identification shall make reference to a potential attack by an individual with reasonable knowledge, not one who is highly skilled in hacking or using computer systems and techniques. This standard may likewise be taken into consideration should a case reach the courts.

3. Final Note

Ultimately, there must be a balance between the protection of data privacy rights and the proactive disclosure of government data through preventive measures, coordination between technical agencies, and close collaboration between the government and the people. As technology continues to evolve, more data will also be available. Privacy fears and risks are real, but these must not be allowed to prevent society from accessing, using, and benefitting from the data, so long as proper safeguards are set.

As a final note, it must be understood that open data is but one aspect of the government's disclosure regime. In modern society, information is both a weapon and a shield against abuse. Legislating on open data does not render a law on FOI useless; rather, all of these measures contribute to a disclosure environment for public offices that strengthens transparency and accountability through the enactment of sunshine laws. With the increasing developments in technology, good governance practices must keep up by evolving legal frameworks accordingly in order that rights remain upheld and protected in all instances.

347. *Id.* at 22–23 (emphases supplied).

ANNEX
PROPOSED AMENDMENTS TO HOUSE BILL NO. 7786 [348]

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. _____
Introduced by _____

AN ACT STRENGTHENING THE OPEN DATA INITIATIVE OF THE GOVERNMENT

Be it enacted by the Senate and the House of Representatives of the Philippines in the Congress assembled:

CHAPTER I
GENERAL PROVISIONS

Section 1. *Short Title*. — This Act shall be known as the "Open Data Act of 2020".

Section 2. *Declaration of Policy* — It is the policy of the State to make all published government data accessible to the public. It will use an open data strategy to adopt openness for all datasets created, collected, processed, disseminated, or disposed through the use of public funds to the extent permitted by applicable laws and subject to individual privacy, confidentiality, national security, or other legally-mandated restrictions. Openness means that datasets published by agencies shall be machine-readable, in open formats, and released with open licenses.

In line with this, the State shall mandate all government offices to adopt the Open Data strategy to enforce the digitization of government

348. The Annex reproduces House Bill No. 7786 introduced by Representative Pablo John F. Garcia, incorporating the recommendations put forth by this Note. This amended version is likewise recommended for filing in the Senate for the passage of the counterpart bill in the Upper House. Other modifications or minor corrections are underlined.

datasets to make them available in a machine-readable format and publish these datasets in a shared repository in an internet domain. The State shall:

(a) Make government data searchable and reusable;
(b) Democratize data by cultivating a culture of information-sharing among government institutions;
(c) Strengthen evidence-based policymaking and decision-making;
(d) Form a systematic approach to use open data as a tool to support government and private sector initiatives;
(e) Enhance the participation of citizens in good governance by making the government more transparent, responsive, accountable, and effective;
(f) Use real-time government data for disaster risk reduction and mitigation initiatives, food security, economic and financial matters, as well as in public procurement, among others, and
(g) Promotion of innovation by encouraging and incentivizing research undertakings and scientific engagements using government data.

Section 3. *Definition of Terms*. — As used in this Act, the following terms shall be defined as follows:

(a) "Agency Information Inventory" refers to the comprehensive listing of all information and datasets that an agency currently holds.
(b) "Data" refers to recorded information, regardless of the form or the media on which the data is recorded.
(c) "Dataset" refers to information comprising a collection of information held in electronic form where all or most of the information in the collections —
    (i.) has been obtained or recorded for the purposes of providing a public authority with information,
    (ii.) is factual information which is not the product of analysis or interpretation other than calculation, and
    (iii.) remains presented in a way that (except for the purpose of forming part of the collection) has not been organized, adapted, or otherwise materially altered since it was obtained or recorded.
(d) "Machine-readable" refers to the form in which data or text can be easily processed by a computer. It excludes the picture format (scanned or photographed) of documents.

(e) "Metadata" refers to the description of a data or dataset. It provides information that describes its content.
(f) "Open access" refers to the provision of free access to the general public.
(g) "Open Data Philippines" refers to the core government program that addresses the constitutional right of Filipinos to information on matters of public concern by making government data accessible, searchable, and understandable.
(h) "Open Data Portal" refers to the public domain website that serves as the central repository for all government datasets.
(i) "Open license" refers to a legal condition that allows content to be free and reusable in any way under a few conditions, attribution being the usual requirement.

Section 4. *Coverage* — This Act shall cover all agencies and instrumentalities of the government, including State Universities and Colleges (SUCs), Government-Owned and -Controlled Corporations (GOCCs), and Government Financial Institutions (GFIs); Local Government Units (LGUs); and constitutional offices enjoying fiscal autonomy.

Section 5. *Exceptions* — This Act shall not apply to government datasets pertaining to the following:

(a) Personal and sensitive personal information collected pursuant to Republic Act No. 10173 or the Data Privacy Act of 2012;
(b) National security matters, including military, diplomatic, and other State secrets;
(c) Trade or industrial secrets pursuant to Republic Act No. 8293 or the Intellectual Property Code of the Philippines;
(d) Banking information and transactions covered by Republic Act No. 1405 or the Secrecy of Bank Deposits;
(e) Classified law enforcement matters, such as those relating to the apprehension, prosecution, and detention of criminals; and to
(f) Other situations involving other known legal limitations including, but are not limited to, contractual pledges of confidentiality.

CHAPTER II
OPEN DATA PHILIPPINES

Section 6. *Open Data Policy Board*. An independent inter-agency body to be known as the Open Data Policy Board (ODPB) is hereby established to develop policies and oversee the proper implementation of Open Data

Philippines based on domestic and international standards on open data. It shall ensure the alignment of its policies to government data disclosure initiatives such as the Data Privacy Act, the Intellectual Property Code, and other pertinent laws and regulations.

The ODPB shall be composed of the Secretary of the Department of Information and Communication Technology as Chairperson, the National Statistician as the Vice Chairperson, with the following members:

(a) Secretary of the Department of Science and Technology;
(b) Secretary of the Department of Education;
(c) Secretary of the Department of Interior and Local Government;
(d) Secretary of the Department of Budget and Management;
(e) Secretary of the Presidential Communication Operations Office;
(f) Director-General of the National Archives of the Philippines;
(g) Chairperson of the National Privacy Commission;
(h) Director-General of the Intellectual Property Office;
(i) Chairperson of the Commission on Higher Education;
(j) President of the University of the Philippines; and the
(k) Director-General of the Technical Education and Skills Development Authority;

or their duly authorized representatives. A representative from the private sector shall be appointed by the President of the Philippines upon the recommendation of the ODPB. The ODPB may invite resource persons to their meetings.

Section 7. *Powers and Functions of the Open Data Policy Board*. — The Open Data Policy Board shall have the following powers and functions:

(a) Establish government-wide policies and best practices for the use, protection, dissemination, and generation of data;
(b) Promote and encourage data sharing agreements between government agencies and instrumentalities;
(c) Identify ways in which government agencies and instrumentalities can improve upon the production of data for use in policymaking;
(d) Identify and evaluate new technology solutions for improving the collection and use of data; and
(e) Consult with the public and engage with private users of government data and other stakeholders on how to improve access to and usability of data assets of the government.

The ODPB shall be supported by the Open Data Bureau.

Section 8. *Open Data Bureau* — There shall be a body to be known as the "Open Data Bureau" under the supervision and control of the Open Data Policy Board specifically dedicated to the administration, promotion, development, and implementation of the Open Data Initiative of the Philippine government as provided in this Act, which shall have the following functions:

(a) Strengthen the existing Open Data Philippines initiative to foster openness and increase government transparency and citizen engagement;
(b) Strengthen the existing Open Data Portal to serve as the central repository of all open government datasets;
(c) Create, issue, and implement an Open Data Action Plan (ODAP), which shall outline a three-year roadmap to a complete and integrated Open Data system and demonstrate the potential uses of open data in public service delivery, among others;
(d) Institutionalize data management practices and standards set by the Philippine eGovernment Interoperability Framework (PeGIF) for Open Data, such as a naming and tagging convention, metadata schema, and data dictionary, among others;
(e) Maintain an accessible open data inventory and catalogue;
(f) Promote civic participation by consulting with civil society organizations in formulating plans and policies for the implementation of open data;
(g) Monitor and evaluate the compliance of government agencies with the guidelines on open data;
(h) Issue specific guidelines in accordance with the policies laid down by the ODPB;
(i) Conduct capacity-building activities such as trainings, workshops, and seminars to train government agencies and instrumentalities on integration with the ODPH and use of the portal;
(j) Render opinions on issues raised and referred by government agencies about the implementation of this Act;
(k) Consult with the public and engage with private users of government data and other stakeholders on how to improve access to data assets of the government; and
(l) Assume other duties and functions as may be deemed necessary by the ODPB for the successful operation of the Bureau.

In addition to the powers granted under this Act, the Open Data Bureau shall absorb all the powers, functions, and responsibilities of the Open

Data Philippines Task Force created under Joint Memorandum Circular No. 2015-01.

Section 9. *Organizational Structure of the Bureau*. — The Bureau shall be headed by an Executive Director. The Executive Director shall be assisted by two (2) Deputy Directors, one to be responsible for Data Processing Systems and one to be responsible for Policy and Planning. The Executive Director and the two Deputy Directors shall be appointed by the President of the Philippines for a term of three (3) years and may be reappointed for another term of three (3) years. Vacancies in the Bureau shall be filled in the same manner in which the original appointment was made.

Section 10. *Qualification of the Executive Director and Deputy Directors*. — The Executive Director and Deputy Directors must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of open data, statistics, data privacy, or computer and information technology.

The Executive Director shall enjoy the benefits, privileges, and emoluments equivalent to the rank of an Undersecretary. The Deputy Directors shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Assistant Secretary.

Section 11. *Open Data Officer* — Each government agency covered by this Act shall appoint or designate an Open Data Officer. The Open Data Officer shall be responsible for the following:

(a) Promote the increased use and re-use of official government data within the agency and by the public;
(b) Coordinate with the Open Data Bureau for the proper implementation of its issuances and other concerns;
(c) Maintain an Agency Information Inventory;
(d) Improv and enhance data management practices of the agency;
(e) Consult with the public and engage with private users of agency data and other stakeholders on how to improve access to data assets of the government; and
(f) Respond to feedback from the public regarding open data.

The government agency may create an Agency Open Data Team to assist the Open Data Officer in fulfilling the functions listed above.

Appointed or designated officers shall enjoy additional emoluments as may be determined by the head of the government agency. In no case shall the Open Data Officer be the same as the Data Privacy Officer.

Section 12. *League of Open Data Officers*. — There shall be an organization of all Open Data officers to be known as the League of Open Data Officers for the primary purpose of ventilating, articulating, and crystallizing issues affecting Open Data administration and securing, through proper and legal means, solutions thereto.

CHAPTER III
OPEN DATA OPERATIONALIZATION

Section 13. *General Open Data Principles*. — The Open Data initiative shall be guided by the following principles:

(a) *Access to public sector information*. Open Data Philippines is one of the core government programs that guarantee the constitutional right of the people to information on matters of public concern and the state policy of full public disclosure thereof. The Open Data portal is intended to be the primary platform by which government data is published.
(b) *Data Driven Governance*. The program seeks to drive government decision-making based on available and sound data. Equally important, the program recognizes that government does not have a monopoly on good governance, as a citizenry empowered with open government data can help improve the government's service delivery.
(c) *Public engagement*. The program adheres to the idea that opening government data goes beyond providing data; it needs the public's participation to move it forward. Hence, the program establishes linkages outside of government, especially with civil society organizations (CSOs), the private sector, academe, and other stakeholders.
(d) *Practical Innovation*. The program aspires to create opportunities for innovation that tremendously benefit both government and the public. The program recognizes that open government data goes beyond the fundamental purpose of transparency but also aims to improve the delivery of public services, translate them into economic or commercial opportunities, and find relevance in the everyday lives of citizens.

Section 14. *Criteria for Open Data.* Government-held datasets made available through open data shall adhere to the following requirements:

(a) *Open by Default.* When not otherwise prohibited by law and to the extent practicable, public data assets maintained by the government shall be platform-independent, machine-readable, and available under an open license.
(b) *Primary and Complete.* Datasets must be published in primary forms, with the finest possible level of granularity that is practicable and permitted by law. Whenever necessary, aggregate data may also be published but shall reference the primary data.
(c) *Accessible and Usable.* Each dataset shall be made available in convenient, modifiable, and open formats that can be retrieved, downloaded, indexed, and searched. Formats should be machine-readable. Open data structures shall not discriminate against any person or group of persons and should be made available to the widest range of users for the widest range of purposes by providing the data in multiple formats for consumption. To the extent permitted by law, these formats should be non-proprietary, publicly available, and no restrictions should be placed upon their use.
(d) *Timely and Comprehensive.* Each dataset shall be updated as quickly as necessary to ensure its quality and to preserve its value. The frequency of release should account for the needs of the stakeholders.
(e) *Comparable and Interoperable.* Each dataset shall be easy to compare within and between sectors, across geographic locations, and over time. All datasets must be presented in structured and standardized formats to support interoperability, traceability, and effective reuse.

It shall be understood that a government dataset uploaded in the government Open Data portal is to be used for improved governance and citizen engagement as well as for inclusive development and innovation.

Section 15. *Open License.* — Government data uploaded in the Open Data Portal shall be considered as public content and can be used for public consumption. This means that the dataset is offered for free and without restriction, subject only to proper attribution to the publishing government agency or instrumentality.

Section 16. *Metadata.* — Each dataset shall have corresponding metadata that provides contextual information on the dataset, in compliance with best practices on open data.

Section 17. *Data Management and Release*. To ensure that data assets are managed and maintained throughout their life cycle, government agencies shall adopt effective data asset portfolio management approaches. Within six months from the date of effectivity of this law, agencies must review and, where appropriate, revise existing policies and procedures to strengthen data management and release practices which include but are not limited to the following:

(a) Creating and maintaining an enterprise data inventory;
(b) Creating and maintaining a public data listing;
(c) Establishing a process to facilitate and prioritize data release; and
(d) Clarifying roles and responsibilities for efficient and effective data release practices.

Section 18. *Uploading of Datasets*. — All datasets to be uploaded by the agencies shall be coursed through their respective Open Data Officers before uploading. These shall include datasets that are:

(a) Necessary to espouse transparency and accountability in public governance;
(b) Relevant for the public to know through the use of statistics;
(c) Requested by other government agencies and other institutions and entities; and
(d) Required by the Open Data Policy Bureau to be uploaded.

Section 19. *Post-release Management*. — The government agency in charge of maintaining the dataset shall designate a point of contact to assist with the data use and to respond to complaints about adherence to the open data requirements.

Section 20. *Agency Implementation*. — All agencies, through their respective Open Data Officers, shall comply with the Open Data guidelines, which will be set by the Open Data Bureau. To fulfill their commitment to the Open Data initiative, they shall:

(a) Adopt an Agency Open Data Policy;
(b) Foster an open, transparent, and accessible government through open data;
(c) Promote the increased use and re-use of official government data within the Department and by the public;
(d) Improve and enhance data management practices;
(e) Respond to feedback from the public regarding open data; and

(f) Work with civil society, the private sector, and the citizens to prioritize open datasets for release.

Section 21. *Civic Engagement*. — Civic participation and engagement shall be promoted by consulting with civil society organizations in formulating plans and policies for the implementation of open data. It is recommended that each data category has a CSO counterpart that shall build on the data.

Section 22. *Incentive for Open Data Utilization*. — All Filipino citizens are encouraged to create usable applications out of the datasets that will be uploaded to the government portal. An incentive program shall be created for this purpose.

Section 23. *Duty to Report*. Any person who discovers or becomes aware of any re-identification of individuals in a dataset shall make a report thereof to the government office, which released the data within seventy-two (72) hours upon knowledge thereof.

CHAPTER IV
PENALTIES

Section 24. *Responsibility of Heads of Agencies*. — All open data maintained by the government, its agencies, and instrumentalities shall be published, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry and as recommended by the Open Data Policy Board. The head of each government agency or instrumentality shall be responsible for complying with the disclosure requirements mentioned herein, while the Bureau shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

Section 25. *Violations*. — Any act of intentional misuse, misrepresentation, tampering, hacking, or other analogous acts, committed in the Philippines or abroad by Filipinos or foreigners, shall be penalized by imprisonment ranging from six (6) months to three (3) years and a fine not less than Two hundred thousand (₱200,000.00) but not more than One million pesos (₱1,000,000.00).

Any combination or series of acts listed above shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not

less than One million pesos (₱1,000,000.00) but not more than Five million pesos (₱5,000,000.00).

Undue or malicious refusal to disclose datasets that should have been disclosed or published by the government agency shall subject the public officer to administrative sanctions only.

CHAPTER V
MISCELLANEOUS PROVISIONS

Section 26. *Interpretation*. — Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the right of the people to information on matters of public concern and access to government research data used as bases for policy development.

Section 27. *Implementing Rules and Regulations*. — The ODPB shall convene within fifteen (15) days from the effectivity of this Act to formulate the Implementing Rules and Regulations (IRR) of this Act within ninety (90) days from convening.

Section 28. *Congressional Oversight Committee*. — There is hereby created a Joint Congressional Oversight Committee to oversee the implementation of this Act for a period not exceeding five (5) years from the effectivity of this Act. The Committee shall be composed of the Chairperson of the Senate Committee on Public Information and Mass Media and two (2) members thereof appointed by the Senate President, the Chairperson of the House Committee on Information and Communications Technology, and two (2) members thereof to be appointed by the Speaker of the House of Representatives.

Section 29. *Reportorial Requirements*. — The Open Data Bureau shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Bureau shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public on open data, data ethics, data privacy, data protection, and fair information rights and responsibilities.

Section 30. *Transitory Provision*. — Government agencies and instrumentalities affected by this Act shall be given one (1) year transitory period from the effectivity of the IRR or such other period as may be determined by the ODPB to comply with the requirements of this Act.

Section 31. *Appropriations Clause*. — The Bureau shall be provided with an initial appropriation of Twenty million pesos (₱20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (₱10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government.

Section 32. *Separability Clause*. — If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid and subsisting.

Section 33. *Repealing Clause*. — Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations, and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

Section 34. *Effectivity Clause*. — This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

APPROVED, _____